

## **Chapter 1: Introduction to the System Safety Handbook**

<b>1.1 INTRODUCTION .....</b>	<b>2</b>
<b>1.2 PURPOSE .....</b>	<b>3</b>
<b>1.3 SCOPE.....</b>	<b>3</b>
<b>1.4 ORGANIZATION OF THE HANDBOOK.....</b>	<b>3</b>
<b>1.5 RELATIONSHIP OF THE SSH TO THE AMS .....</b>	<b>4</b>
<b>1.6 SYSTEM SAFETY OBJECTIVES .....</b>	<b>7</b>
<b>1.7 GLOSSARY .....</b>	<b>7</b>

## 1.1 Introduction

The System Safety Handbook (SSH) was developed for the use of Federal Aviation Administration (FAA) employees, supporting contractors and any other entities that are involved in applying system safety policies and procedures throughout FAA. As the Federal agency with primary responsibility for civil aviation safety, the FAA develops and applies safety techniques and procedures in a wide range of activities from NAS modernization, to air traffic control, and aircraft certification. On June 28, 1998, the FAA Administrator issued Order 8040.4 to establish FAA safety risk management policy. This policy requires all the Lines of Business (LOB) of the FAA to establish and implement a formal risk management program consistent with the LOB's role in the FAA. The policy reads in part: "The FAA shall use a formal, disciplined, and documented decision making process to address safety risks in relation to high-consequence decisions impacting the complete life cycle."

In addition, the Order established the FAA Safety Risk Management Committee (SRMC) consisting of safety and risk management professionals representing Associate/Assistant Administrators and the offices of the Chief Counsel, Civil Rights, Government and Industry Affairs, and Public Affairs. The SRMC provides advice and guidance, upon request from the responsible program offices to help the program offices fulfill their authority and responsibility for implementing Order 8040.4.

This System Safety Handbook provides guidance to the program offices. It is intended to describe "how" to set up and implement the safety risk management process. The SSH establishes a set of consistent and standardized procedures and analytical tools that will enable each LOB or program office in the FAA to comply with Order 8040.4.

In FAA, the Acquisition Management System (AMS) provides agency-wide policy and guidance that applies to all phases of the acquisition life cycle. Consistent with Order 8040.4, AMS policy is that System Safety Management shall be conducted throughout the acquisition life cycle (section 2.9.13) of the AMS. The SSH is designed to support this AMS system safety management policy. It is included in the FAA Acquisition System Toolset (FAST), and is referenced in several of the FAST process documents. It is also designed to support safety risk management activities in FAA not covered by AMS policy and guidance.

This SSH is intended for use in support of specific system safety program plans. While the SSH provides guidance on "how" to perform safety risk management, other questions concerning "when, who, and why" should be addressed through the three types of plans discussed in this document: System Safety Management Plan (SSMP), and a System Safety Program Plan (SSPP), and an Integrated System Safety Program Plan (ISSPP). The SSH focuses on "how" to perform safety risk management, while these planning documents describe, in Chapter 5, the organization's processes and procedures for implementing system safety.

FAA System Safety Handbook, Chapter 1: Introduction  
December 30, 2000

High-level SSMPs describe general organizational processes and procedures for the implementation of system safety programs, while more specific SSPPs are developed for individual programs and projects. The ISSPP is intended for large complex systems with multiple subcontractors. The SRMC is responsible for developing an overall FAA SSMP, while the System Engineering Council develops the SSMP for AMS processes, such as Mission Analysis, Investment Analysis, and Solution Implementation. Integrated Product Team (IPT) leaders, program managers, project managers and other team leaders develop SSPPs appropriate to their activities. Chapter 4 of the SSH provides guidance for the development of a SSPP.

## **1.2 Purpose**

The purpose of this handbook is to provide instructions on how to perform system safety engineering and management for FAA personnel involved in system safety activities, including FAA contractor management, engineering, safety specialists, team members on Integrated Product Development System (IPDS) teams, analysts and personnel throughout FAA regions, centers, facilities, and any other entities involved in aviation operations.

## **1.3 Scope**

This handbook is intended to support system safety and safety risk management throughout the FAA. It does not supersede regulations, or other procedures or policies; however, this handbook provides best practices in system safety engineering and management. When these regulations or procedures exist, this handbook will indicate the reference and direct the reader to that document. If a conflict exists between the SSH and FAA policies and regulations, the policies and regulations supersede this document. However, if results of analysis using the tools and techniques in this SSH identify policy or regulatory issues that conflict with existing FAA policies and regulations, the issues should be brought to the attention of the Office of System Safety (ASY), and consideration should be given to changing the policy or regulation. This handbook is also intended to provide guidance to FAA contractors who support the FAA by providing systems and/or analyses. This handbook does not supersede the specific contract, but can be referenced in the statement of work or other documents as a guide.

## **1.4 Organization of the Handbook**

The SSH is organized from general to specific instructions. The first three chapters provide a brief overview of system safety policy, system safety processes, definition of what system safety is as practiced in FAA, and some common principles of the safety discipline. Chapters 4-6 explain how to establish a system safety program, how to prepare the required system safety plans, and how to perform system safety integration and safety Comparative Safety Assessment. Chapter 7 describes how to perform integrated system hazard analysis. Chapters 8 and 9 discuss hazard analysis tasks and some of the analytical techniques used in system safety analysis. Chapter 10 discusses how to perform system software safety. Chapter 11 explains test and evaluation safety guidance. Chapter 12 is focused on facilities and is directed to Occupational Health and Safety aspects of FAA

FAA System Safety Handbook, Chapter 1: Introduction  
December 30, 2000

facilities and equipment operation. Chapter 13 is a special discussion of the commercial launch vehicle safety and certification process. Chapter 14 addresses training, Chapter 15 discusses operational risk management, Chapter 16 treats Organizational Systems in Aviation, and Chapter 17 concludes with Human Factors Safety Principles.

### 1.5 Relationship of the SSH to the AMS

The AMS contains guidance to the acquisition engineers in the FAA Acquisition System Toolset (FAST). The SSH is a tool within the FAST toolset. AMS Section 2 refers to the following process documents that contain further detailed guidance on implementation of the system safety management process.

Mission Analysis Process (MAP)
Investment Analysis Process (IAP)
Integrated Program Plan (IPP)
Acquisition Strategy Paper (ASP)

In addition, the following eight appendices to the Investment Analysis Plan (IAP) contain guidance related to system safety:

Appendix A Investment Analysis Plan
Appendix B Requirements Document
Appendix C Investment Analysis Process Flow Discussion
Appendix D Candidate Solution Identification & Analysis Discussion
Appendix F Acquisition Program Baseline
Appendix G Investment Analysis Report
Appendix H Investment Analysis Briefing
Appendix J Definitions and Acronyms

Where these FAST documents indicate a requirement for including system safety activities, or results of safety analyses in documentation or briefings, they generally reference the appropriate chapter in the SSH for a discussion of how to comply with the requirement. Figure 1-1 shows the flowdown of system safety relationships from the AMS Section 2 the other FAST documents listed above. Section 2.9.13 System Safety Management is the primary policy statement in Section 2. It states as a requirement that each line of business shall implement a system safety program in

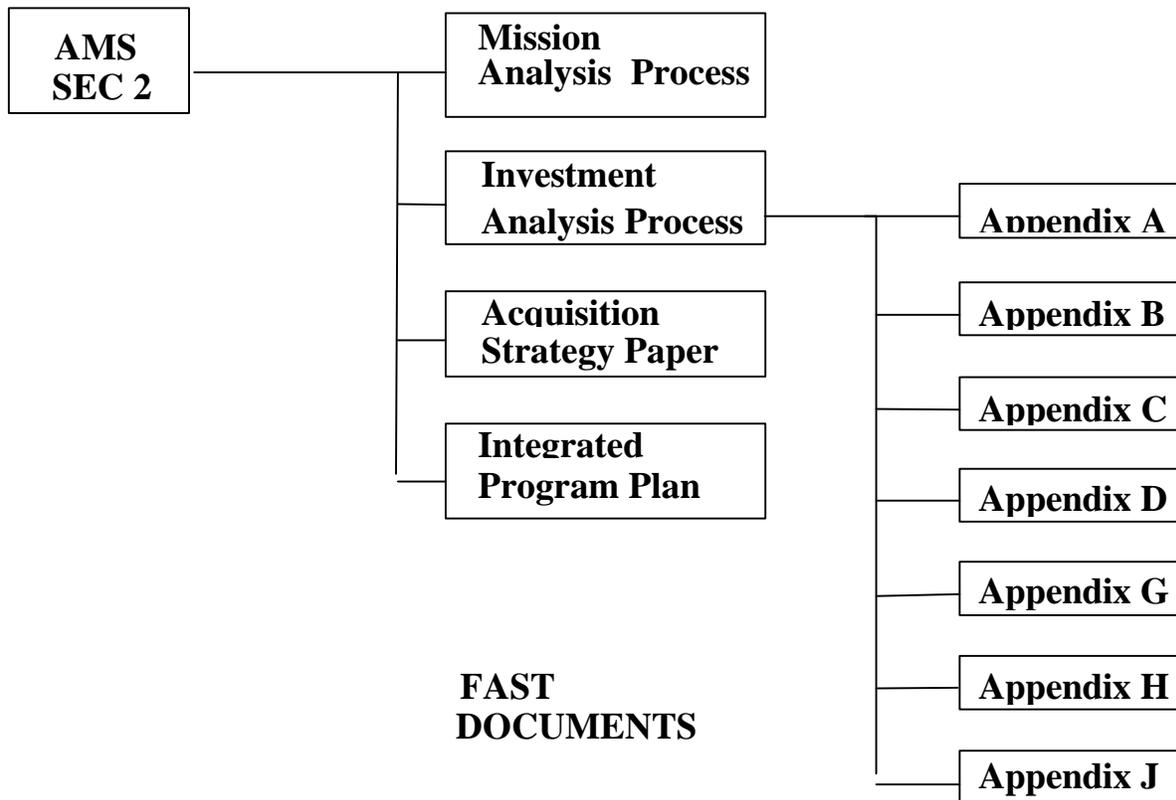
FAA System Safety Handbook, Chapter 1: Introduction  
December 30, 2000

accordance with FAA Order 8040.4. The second tier of documents provide further guidance on how to implement the order, and the Appendices to the Investment Analysis Process document provide templates and formats for documentation that will be taken to the JRC.

Table 1-1 shows the applicability of each chapter in this handbook to the applicable AMS segment.

Table 1-1: System Safety Handbook vs. AMS Segment

AMS Segment	All	Mission Analysis	Investment Analysis	Solution Implementation	In Service Management	Service Life Extension
Applicable Handbook Chapters	2,3,6,7,8,12,13,17	4	5	9,10,11	9,10,11,15,16	9,10,11,15,16
Applicable Appendices	A, C, D, E, G, H		B	J	F, J	J
Launch Unique	13					



**Figure 1-1: Documents Affected by the System Safety Policy Changes to the Acquisition Management System (AMS)**

## 1.6 System Safety Objectives

This handbook supports the achievement of the following system safety objectives:

- Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- Hazards associated with the system (and its component subsystems) are identified, tracked, evaluated, and eliminated, or the associated risk is reduced to a level acceptable to FAA management throughout the entire life cycle of a system. Risk is described in Comparative Safety Assessment terms. See Chapter 3.
- The safety design order of precedence is applied and FAA management accepts the residual risk.
- Safety analyses and assessments are performed in support of the FAA safety risk management efforts and are in accordance with the best safety engineering practices.
- Historical safety data, including lessons learned from other systems, are considered and used in safety assessments and analyses.
- Minimum risk is sought in accepting and using new technology, materials, or designs: and new production, test and operational techniques in the NAS.
- Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during research, technology development, and acquisition of a system.
- Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to FAA management.
- Consideration is given early in the life cycle to system safety through the end of the life cycle which includes system decommissioning.
- Significant safety data are documented as “lessons learned” and are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

## 1.7 Glossary

Appendix A contains a glossary of terms that are used throughout the handbook. It is important to understand the difference between a hazard and a risk, for example, and how these terms relate to the system safety methods. The glossary also provides discussion on different definitions associated with specific system safety terminology. It is important to understand the different definitions. The glossary can be used as a reference, i.e., as a dictionary. Many terms and definitions associated with system safety are included. The glossary can be used for training and

FAA System Safety Handbook, Chapter 1: Introduction  
December 30, 2000

educational purposes. Depending on the need, these terms and definitions can be used when discussing methodology or when conducting presentations. There are terms referenced that are not specifically addressed in the handbook. These additional terms are important, however, as reference material.

## **Chapter 2: System Safety Policy and Process**

<b>2.1 FAA POLICIES.....</b>	<b>2</b>
<b>2.2 THE FAA SAFETY RISK MANAGEMENT PROCESS.....</b>	<b>3</b>

FAA System Safety Handbook, Chapter 2: System Safety Policy and Process  
December 30, 2000

## 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.

FAA System Safety Handbook, Chapter 2: System Safety Policy and Process  
December 30, 2000

## 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).

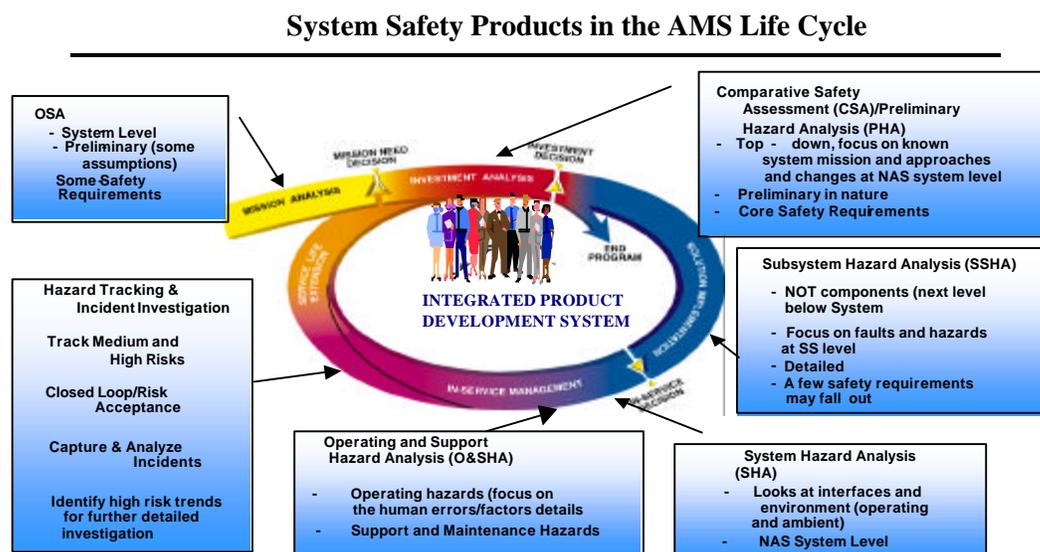


Figure 2-1: Integrated Product Development System

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)

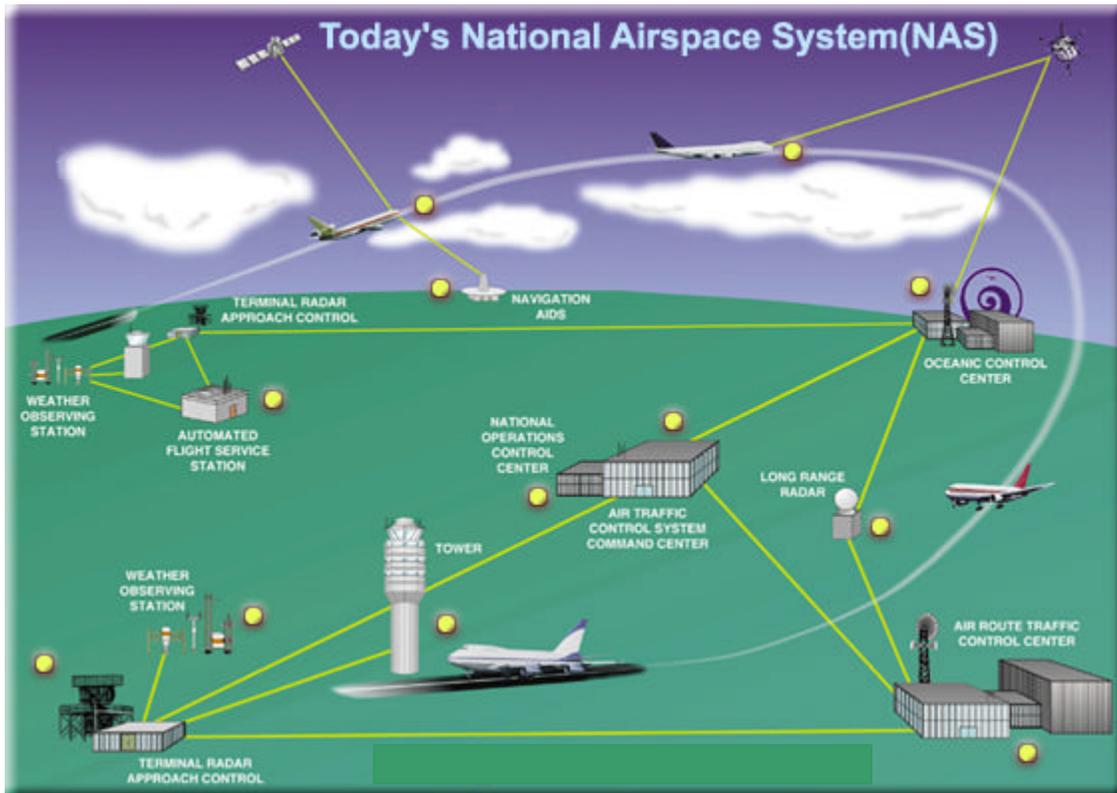


Figure 2-2: Elements of the National Airspace System

### 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

FAA System Safety Handbook, Chapter 2: System Safety Policy and Process  
December 30, 2000

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.

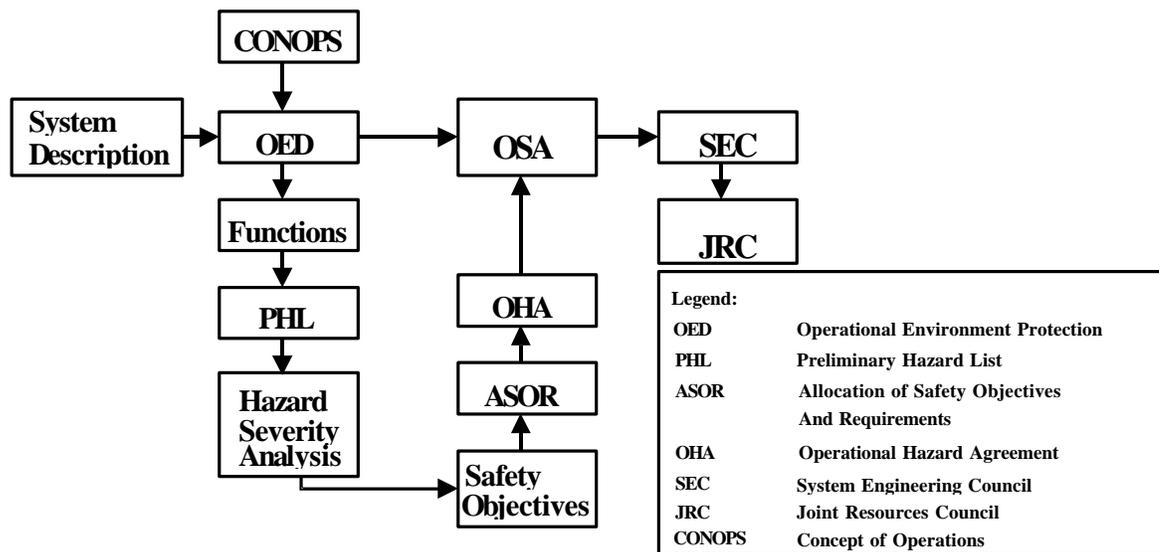


Figure 2-3: Operational Safety Assessment Process

FAA System Safety Handbook, Chapter 2: System Safety Policy and Process  
December 30, 2000

### 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.

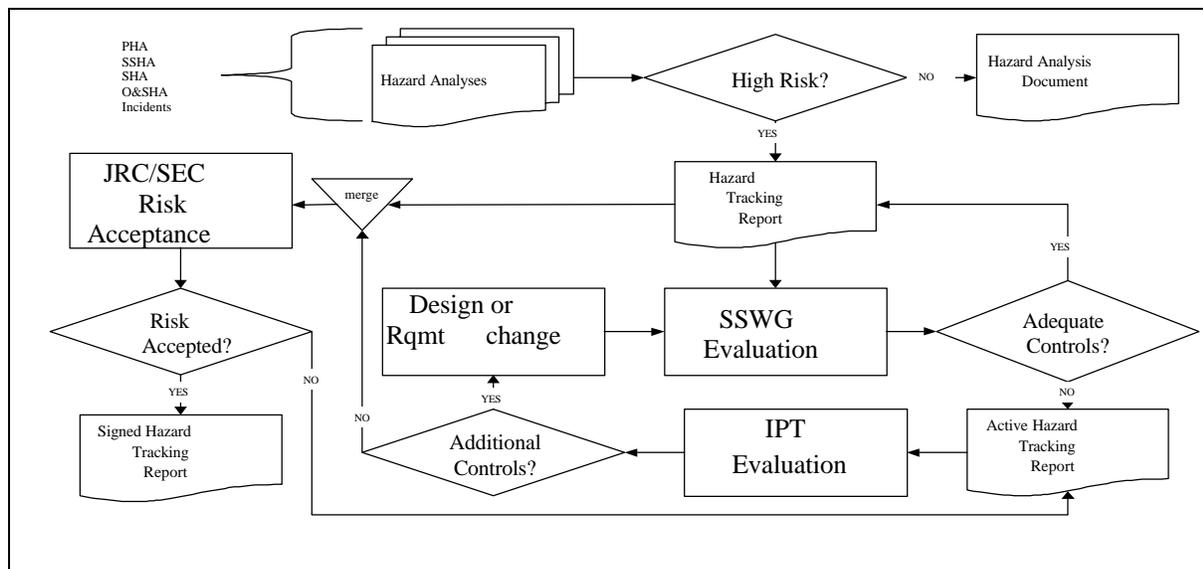
*References* - Appropriate references associated with the specific SAR are indicated, Analysis, Configuration Items, Software Units, Procedures, Tests, and Documents.

*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."

## **Chapter 3: Principles of System Safety**

<b>3.1 DEFINITION OF SYSTEM SAFETY .....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>3.2 PLANNING PRINCIPLES .....</b>	<b>2</b>
<b>3.3 HAZARD ANALYSIS .....</b>	<b>3</b>
<b>3.4 COMPARATIVE SAFETY ASSESSMENT .....</b>	<b>9</b>
<b>3.5 RISK MANAGEMENT DECISION MAKING .....</b>	<b>12</b>
<b>3.6 SAFETY ORDER OF PRECEDENCE.....</b>	<b>12</b>
<b>3.7 BEHAVIORAL-BASED SAFETY .....</b>	<b>15</b>
<b>3.8 MODELS USED BY SYSTEM SAFETY FOR ANALYSIS .....</b>	<b>15</b>

## **3.0 Principles of System Safety**

### **3.1 Definition of System Safety**

System safety is a specialty within system engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety. The goal of System Safety is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence. As discussed in Chapter 2, the FAA AMS identifies System Safety Management as a Critical Functional Discipline to be applied during all phases of the life cycle of an acquisition. FAA Order 8040.4 establishes a five step approach to safety risk management as: Planning, Hazard Identification, Analysis, Assessment, and Decision. The system safety principles involved in each of these steps are discussed in the following paragraphs.

### **3.2 Planning Principles**

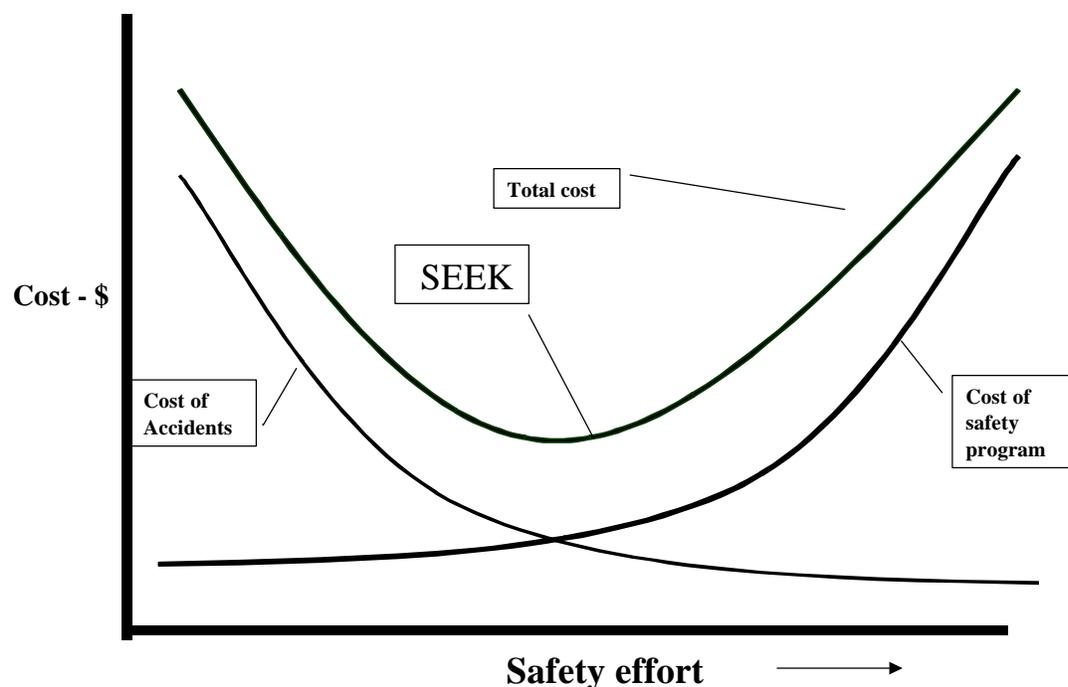
System safety must be planned. It is an integrated and comprehensive engineering effort that requires a trained staff experienced in the application of safety engineering principles. The effort is interrelated, sequential and continuing throughout all program phases. The plan must influence facilities, equipment, procedures and personnel. Planning should include transportation, logistics support, storage, packing, and handling, and should address Commercial Off-the-Shelf (COTS) and Non-developmental Items (NDI). For the FAA AMS applications of system safety, a System Safety Management Plan is needed in the Pre-investment Decision phases to address the management objectives, responsibilities, program requirements, and schedule (who?, what?, when?, where?, and why?). After the Investment Decision is made and a program is approved for implementation, a System Safety Program Plan is needed. See Chapter 5, for details on the preparation of a SSPP.

#### **3.2.1 Managing Authority (MA) Role**

Throughout this document, the term Managing Authority (MA) is used to identify the responsible entity for managing the system safety effort. In all cases, the MA is a FAA organization that has responsibility for the program, project or activity. Managerial and technical procedures to be used must be approved by the MA. The MA resolves conflicts between safety requirements and other design requirements, and resolves conflicts between associate contractors when applicable. See Chapter 5 for a discussion on Integrated System Safety Program Plans.

#### **3.2.2 Defining System Safety Requirements**

System safety requirements must be consistent with other program requirements. A balanced program attempts to optimize safety, performance and cost. System safety program balance is the product of the interplay between system safety and the other three familiar program elements of cost, schedule, and performance as shown in Figure 3-1. Programs cannot afford accidents that will prevent the achievement of the primary mission goals. However, neither can we afford systems that cannot perform due to unreasonable and unnecessary safety requirements. Safety must be placed in its proper perspective. A correct safety balance cannot be achieved unless acceptable and unacceptable conditions are established early enough in the program to allow for the selection of the optimum design solution and/or operational alternatives. Defining acceptable and unacceptable risk is as important for cost-effective accident prevention as is defining cost and performance parameters.



**Figure 3-1: Cost vs. Safety Effort (Seeking Balance)**

### 3.3 Hazard Analysis

Both elements of risk (hazard severity and likelihood of occurrence) must be characterized. The inability to quantify and/or lack of historical data on a particular hazard does not exclude the hazard from this requirement<sup>1</sup>. The term "hazard" is used generically in the early chapters of this handbook. Beginning with Chapter 7, hazards are subdivided into sub-categories related to environment such as system states, environmental conditions or "initiating" and "contributing" hazards.

Realistically, a certain degree of safety risk must be accepted. Determining the acceptable level of risk is generally the responsibility of management. Any management decisions, including those related to safety, must consider other essential program elements. The marginal costs of implementing hazard control requirements in a system must be weighed against the expected costs of not implementing such controls. The cost of not implementing hazard controls is often difficult to quantify before the fact. In order to quantify expected accident costs before the fact, two factors must be considered. These are related to risk and are the potential consequences of an accident and the probability of its occurrence. The more severe the consequences of an accident (in terms of dollars, injury, or national prestige, etc.) the lower the probability of its occurrence must be for the risk to be acceptable. In this case, it will be worthwhile to spend money to reduce the probability by implementing hazard controls. Conversely, accidents whose consequences are less severe may be acceptable risks at higher probabilities of occurrence and will consequently justify a lesser expenditure to further reduce the frequency of occurrence. Using this concept as a baseline, design limits must be defined.

<sup>1</sup> FAA Order 8040.4 Paragraph 5.c.

### 3.3.1 Accident Scenario Relationships

In conducting hazard analysis, an accident scenario as shown in Figure 3-2 is a useful model for analyzing risk of harm due to hazards. Throughout this System Safety Handbook, the term hazard will be used to describe scenarios that may cause harm. It is defined in FAA Order 8040.4 as a "Condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event." Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes termed initiating and contributory hazards. As shown in Figure 3-2, contributory hazards involve consideration of the system state (e.g., operating environment) as well as failures or malfunctions. In chapter 7 there is an in-depth discussion of this methodology.

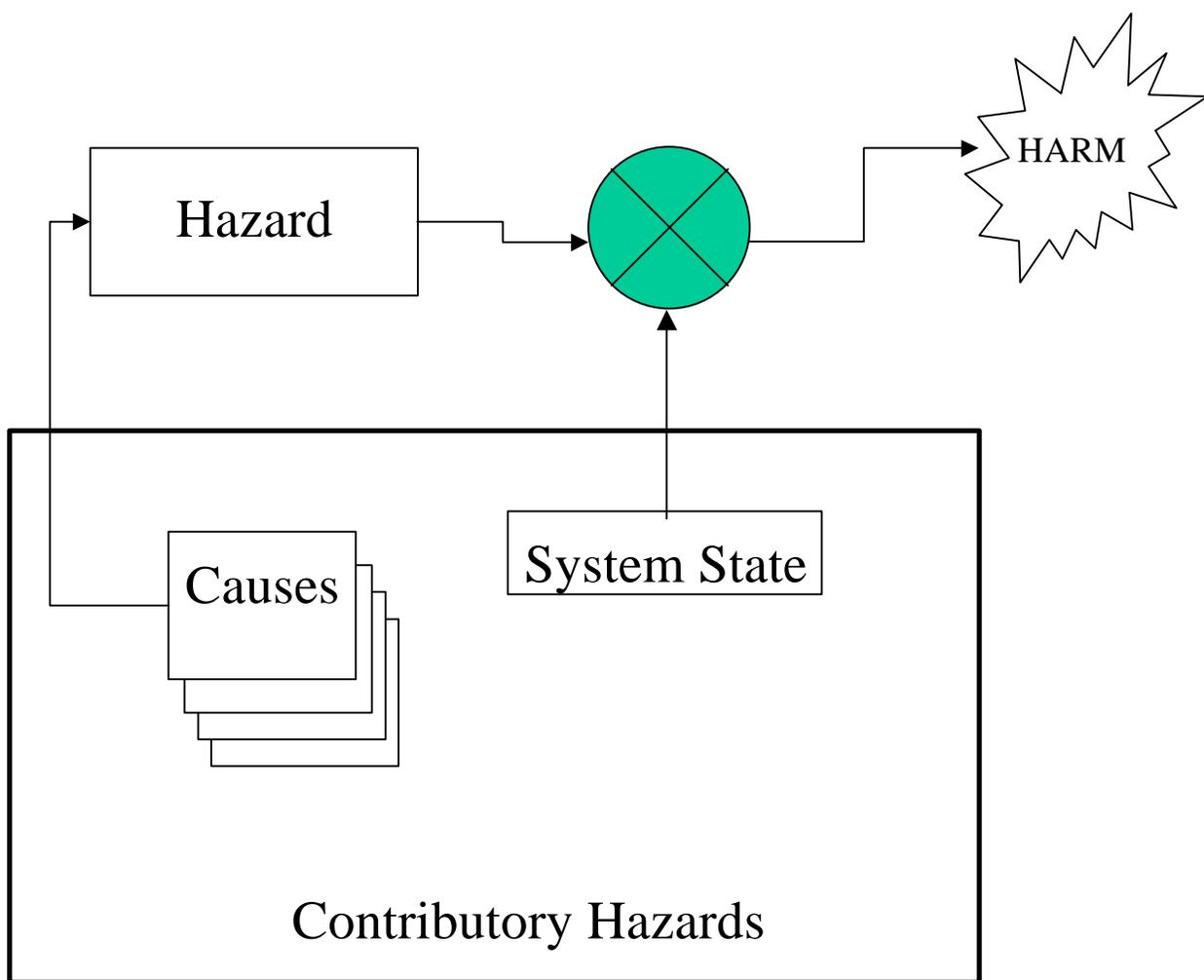


Figure 3-2: Hazard Scenario Model

### 3.3.2 Definitions for Use in the FAA Acquisition Process

The FAA System Engineering Council (SEC) has approved specific definitions for Severity and Likelihood to be used during all phases of the acquisition life cycle. These are shown in Table 3-2 and Table 3-3.

**Table 3-2: Severity Definitions for FAA AMS Process**

<b>Catastrophic</b>	<b>Results in multiple fatalities and/or loss of the system</b>
<b>Hazardous</b>	<b>Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: Large reduction in safety margin or functional capability Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (1) Serious or fatal injury to small number of occupants of aircraft (except operators) Fatal injury to ground personnel and/or general public</b>
<b>Major</b>	<b>Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – Significant reduction in safety margin or functional capability Significant increase in operator workload Conditions impairing operator efficiency or creating significant discomfort Physical distress to occupants of aircraft (except operator) including injuries Major occupational illness and/or major environmental damage, and/or major property damage</b>
<b>Minor</b>	<b>Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include Slight reduction in safety margin or functional capabilities Slight increase in workload such as routine flight plan changes Some physical discomfort to occupants or aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage</b>
<b>No Safety Effect</b>	<b>Has no effect on safety</b>

**Table 3-3: Likelihood of Occurrence Definitions**

<b>Probable</b>	<b>Qualitative:</b> Anticipated to occur one or more times during the entire system/operational life of an item. <b>Quantitative:</b> Probability of occurrence per operational hour is greater than $1 \times 10^{-5}$
<b>Remote</b>	<b>Qualitative:</b> Unlikely to occur to each item during its total life. May occur several times in the life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-5}$ , but greater than $1 \times 10^{-7}$
<b>Extremely Remote</b>	<b>Qualitative:</b> Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-7}$ but greater than $1 \times 10^{-9}$
<b>Extremely Improbable</b>	<b>Qualitative:</b> So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. <b>Quantitative:</b> Probability of occurrence per operational hour is less than $1 \times 10^{-9}$

**MIL-STD-882 Definitions of Severity and Likelihood**

An example taken from MIL-STD-882C of the definitions used to define Severity of Consequence and Event Likelihood are in Tables 3-4 and 3-5, respectively.

**Table 3-4: Severity of Consequence**

<i>Description</i>	<i>Category</i>	<i>Definition</i>
<b>Catastrophic</b>	<b>I</b>	Death, and/or system loss, and/or severe environmental damage.
<b>Critical</b>	<b>II</b>	Severe injury, severe occupational illness, major system and/or environmental damage.
<b>Marginal</b>	<b>III</b>	Minor injury, minor occupational illness, and/or minor system damage, and/or environmental damage.
<b>Negligible</b>	<b>IV</b>	Less than minor injury, occupational illness, or less than minor system or environmental damage.

**Table 3-5: Event Likelihood (Probability)**

<i>Description</i>	<i>Level</i>	<i>Specific Event</i>
<b>Frequent</b>	A	Likely to occur frequently
<b>Probable</b>	B	Will occur several times in the life of system.
<b>Occasional</b>	C	Likely to occur some time in the life of the system.
<b>Remote</b>	D	Unlikely but possible to occur in the life of the system.
<b>Inprobable</b>	E	So unlikely, it can be assumed that occurrence may not be experienced.

### 3.3.3 Comparison of FAR and JAR Severity Classifications

Other studies have been conducted to define severity and event likelihood for use by the FAA. A comparison of the severity classifications for the FARs and JARs from one such study<sup>2</sup> is contained in Table 3-6. JARs are the Joint Aviation Regulations with European countries.

<sup>2</sup> Aircraft Performance Comparative Safety Assessment Model (APRAM), Rannoch Corporation, February 28, 2000

**Table 3-6 Most Severe Consequence Used for Classification**

Probability (Quantitative)	1.0		$10^{-3}$	$10^{-5}$	$10^{-7}$		$10^{-9}$
Probability (Descriptive)	FAR	Probable		Improbable			Extremely Improbable
	JAR	Frequent	Reasonably Probable	Remote	Extremely Remote		Extremely Improbable
Failure condition severity classification	FAR	Minor		Major			Catastrophic
	JAR	Minor		Major	Hazardous		Catastrophic
Effect on aircraft occupants	FAR	<ul style="list-style-type: none"> <li>Does not significantly reduce airplane safety (Slight decrease in safety margins)</li> <li>Crew actions well within capabilities (Slight increase in crew workload)</li> <li>Some inconvenience to occupants</li> </ul>		<ul style="list-style-type: none"> <li>Reduce capability of airplane or crew to cope with adverse operating conditions</li> <li>Significant reduction in safety margins</li> <li>Significant increase in crew workload</li> </ul> <p><b>Severe Cases:</b></p> <ul style="list-style-type: none"> <li>Large reduction in safety margins</li> <li>Higher workload or physical distress on crew - can't be relied upon to perform tasks accurately</li> <li>Adverse effects on occupants</li> </ul>			<ul style="list-style-type: none"> <li>Conditions which prevent continued safe flight and landing</li> </ul>
	JAR	<ul style="list-style-type: none"> <li>Nuisance</li> </ul>	<ul style="list-style-type: none"> <li>Operating limitations</li> <li>Emergency procedures</li> </ul>	<ul style="list-style-type: none"> <li>Significant reduction in safety margins</li> <li>Difficulty for crew to cope with adverse conditions</li> <li>Passenger injuries</li> </ul>	<ul style="list-style-type: none"> <li>Large reduction in safety margins</li> <li>Crew extended because of workload or environmental conditions</li> <li>Serious or fatal injury to small number of occupants</li> </ul>	<ul style="list-style-type: none"> <li>Multiple deaths, usually with loss of aircraft</li> </ul>	

### 3.4 Comparative Safety Assessment

Selection of some alternate design elements, e.g., operational parameters and/or architecture components or configuration in lieu of others implies recognition on the part of management that one set of alternatives will result in either more or less risk of an accident. The risk management concept emphasizes the identification of the change in risk with a change in alternative solutions. Safety Comparative Safety Assessment is made more complicated considering that a lesser safety risk may not be the optimum choice from a mission assurance standpoint. Recognition of this is the keystone of safety risk management. These factors make system safety a decision making tool. It must be recognized, however, that selection of the greater safety risk alternative carries with it the responsibility of assuring inclusion of adequate warnings, personnel protective systems, and procedural controls. Safety Comparative Safety Assessment is also a planning tool. It requires planning for the development of safety operating procedures and test programs to resolve uncertainty when safety risk cannot be completely controlled by design. It provides a control system to track and measure progress towards the resolution of uncertainty and to measure the reduction of safety risk.

Assessment of risk is made by combining the severity of consequence with the likelihood of occurrence in a matrix. Risk acceptance criteria to be used in the FAA AMS process are shown in Figure 3-3 and Figure 3-4.

<i>Severity Likelihood</i>	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A					
Remote B					
Extremely Remote C					
Extremely Improbable D					

High Risk
Medium Risk
Low Risk

**Figure 3-3: Risk Acceptability Matrix**

	<b>High Risk --Unacceptable. Tracking in the FAA Hazard Tracking System is required until the risk is reduced and accepted.</b>
	<b>Medium -- Acceptable with review by the appropriate management authority. Tracking in the FAA Hazard Tracking System is required until the risk is accepted.</b>
	<b>Low -- Low risk is acceptable without review. No further tracking of the hazard is required.</b>

**Figure 3-4: Risk Acceptance Criteria**

An example based on MIL-STD-882C is shown in Figure 3-5. The matrix may be referred to as a Hazard Risk Index (HRI), a Risk Rating Factor (RRF), or other terminology, but in all cases, it is the criteria used by management to determine acceptability of risk.

The Comparative Safety Assessment Matrix of Figure 3-5 illustrates an acceptance criteria methodology. Region R1 on the matrix is an area of high risk and may be considered unacceptable by the managing authority. Region R2 may be acceptable with management review of controls and/or mitigations, and R3 may be acceptable with management review. R4 is a low risk region that is usually acceptable without review.

FREQUENCY OF OCCURENCE	HAZARD CATEGORIES			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	IA	IIA	IIIA	IVA
(B) Probable	<b>R1</b> IB	IIB	IIIB	IVB
(C) Occasional	IC	IIC	IIIC	IVC <b>R4</b>
(D) Remote	<b>R2</b> ID	IID	IIID	IVD
(E) Improbable	<b>R3</b> IE	IIE	IIIEP	IVE
Hazard Risk Index (HRI)		Suggested Criteria		
R1		Unacceptable		
R2		Must control or mitigate (MA review)		
R3		Acceptable with MA review		
R4		Acceptable without review		

**Figure 3-5: Example of a Comparative Safety Assessment Matrix**

FAA System Safety Handbook, Chapter 3: Principles of System Safety  
December 30, 2000

Early in a development phase, performance objectives may tend to overshadow efforts to reduce safety risk. This is because sometimes safety represents a constraint on a design. For this reason, safety risk reduction is often ignored or overlooked. In other cases, safety risk may be appraised, but not fully enough to serve as a significant input to the decision making process. As a result, the sudden identification of a significant safety risk, or the occurrence of an actual incident, late in the program can provide an overpowering impact on schedule, cost, and sometimes performance. To avoid this situation, methods to reduce safety risk must be applied commensurate with the task being performed in each program phase.

In the early development phase (investment analysis and the early part of solution implementation), the system safety activities are usually directed toward: 1) establishing risk acceptability parameters; 2) practical tradeoffs between engineering design and defined safety risk parameters; 3) avoidance of alternative approaches with high safety risk potential; 4) defining system test requirements to demonstrate safety characteristics; and, 5) safety planning for follow-on phases. The culmination of this effort is the safety Comparative Safety Assessment that is a summary of the work done toward minimization of unresolved safety concerns and a calculated appraisal of the risk. Properly done, it allows intelligent management decisions concerning acceptability of the risk.

The general principles of safety risk management are:

All system operations represent some degree of risk.

Recognize that human interaction with elements of the system entails some element of risk.

Keep hazards in proper perspective.

Do not overreact to each identified risk, but make a conscious decision on how to deal with it.

Weigh the risks and make judgments according to your own knowledge, inputs from subject matter experts, experience, and program need.

It is more important to establish clear objectives and parameters for Comparative Safety Assessment related to a specific program than to use generic approaches and procedures.

There may be no "single solution" to a safety problem. There are usually a variety of directions to pursue. Each of these directions may produce varying degrees of risk reduction. A combination of approaches may provide the best solution.

Point out to designers the safety goals and how they can be achieved rather than tell him his approach will not work.

There are no "safety problems" in system planning or design. There are only engineering or management problems that, if left unresolved, may lead to accidents.

The determination of severity is made on a "worst credible case/condition" in accordance with MIL-STD-882, and AMJ 25.1309.

- Many hazards may be associated with a single risk. In predictive analysis, risks are hypothesized accidents, and are therefore potential in nature. Severity assessment is made regarding the potential of the hazards to do harm.

### **3.5 Risk Management Decision Making**

For any system safety effort to succeed there must be a commitment on the part of management. There must be mutual confidence between program managers and system safety management. Program managers need to have confidence that safety decisions are made with professional competence. System safety management and engineering must know that their actions will receive full program management attention and support. Safety personnel need to have a clear understanding of the system safety task along with the authority and resources to accomplish the task. Decision-makers need to be fully aware of the risk they are taking when they make their decisions. They have to manage program safety risk. For effective safety risk management, program managers should:

Ensure that competent, responsible, and qualified engineers be assigned in program offices and contractor organizations to manage the system safety program.

Ensure that system safety managers are placed within the organizational structure so that they have the authority and organizational flexibility to perform effectively.

Ensure that all known hazards and their associated risks are defined, documented, and tracked as a program policy so that the decision-makers are made aware of the risks being assumed when the system becomes operational.

Require that an assessment of safety risk be presented as a part of program reviews and at decision milestones. Make decisions on risk acceptability for the program and accept responsibility for that decision.

### **3.6 Safety Order of Precedence**

One of the fundamental principles of system safety is the Safety Order of Precedence in eliminating, controlling or mitigating a hazard. The Safety Order of Precedence is shown in Table 3-7. It will be referred to several times throughout the remaining chapters of this handbook.

**Table 3-7: Safety Order of Precedence**

<b>Description</b>	<b>Priority</b>	<b>Definition</b>
<b>Design for minimum risk.</b>	<b>1</b>	<b>Design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.</b>
<b>Incorporate safety devices.</b>	<b>2</b>	<b>If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.</b>
<b>Provide warning devices.</b>	<b>3</b>	<b>When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response. Warning signs and placards shall be provided to alert operational and support personnel of such risks as exposure to high voltage and heavy objects.</b>
<b>Develop procedures and training.</b>	<b>4</b>	<b>Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.</b>

**Examples:**

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

FAA System Safety Handbook, Chapter 3: Principles of System Safety  
December 30, 2000

### **opening high voltage panels**

### 3.7 Behavioral-Based Safety

Safety management must be based on the behavior of people and the organizational culture. Everyone has a responsibility for safety and should participate in safety management efforts. Modern organization safety strategy has progressed from “safety by compliance” to more of an appropriate concept of “prevention by planning”. Reliance on compliance could translate to after-the-fact hazard detection, which does not identify organizational errors, that are often times, the contributors to accidents.

Modern safety management, i.e.--“system safety management”-- adopts techniques of system theory, statistical analysis, behavioral sciences and the continuous improvement concept. Two elements critical to this modern approach are a good organizational safety culture and people involvement.

The establishment of system safety working groups, analysis teams, and product teams accomplishes a positive cultural involvement when there are consensus efforts to conduct hazard analysis and manage system safety programs.

Real-time safety analysis is conducted when operational personnel are involved in the identification of hazards and risks, which is the key to behavioral-based safety. The concept consists of a “train-the-trainer” format. See chapter 14 for a detailed discussion of how a selected safety team is provided the necessary tools and is taught how to:

- Identify hazards, unsafe acts or conditions;
- Identify “at risk” behaviors;
- Collect the information in a readily available format for providing immediate feedback;
- Train front-line people to implement and take responsibility for day-to-day operation of the program.

The behavioral-based safety process allows an organization to create and maintain a positive safety culture that continually reinforces safe behaviors over unsafe behaviors. This will ultimately result in a reduction of risk. For further information concerning behavioral-based safety contact the FAA’s Office of System Safety.

### 3.8 Models Used by System Safety for Analysis

The AMS system safety program uses models to describe a system under study. These models are known as the 5M model and the SHELL model. While there are many other models available, these two recognize the interrelationships and integration of the hardware, software, human, environment and procedures inherent in FAA systems. FAA policy and the system safety approach is to identify and control the risks associated with each element of a system on a individual, interface and system level.

The first step in performing safety risk management is describing the system under consideration. This description should include at a minimum, the functions, general physical characteristics, and operations of the system. Normally, detailed physical descriptions are not required unless the safety analysis is focused on this area.

Keep in mind that the reason for performing safety analyses is to identify hazards and risks and to communicate that information to the audience. At a minimum, the safety assessment should describe the system in sufficient detail that the projected audience can understand the safety risks.

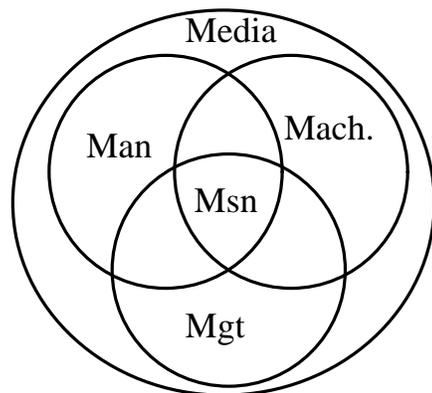
A system description has both breadth and depth. The breadth of a system description refers to the system boundaries. Bounding means limiting the system to those elements of the system model that affect or interact with each other to accomplish the central mission(s) or function. Depth refers to the level of detail in the description. In general, the level of detail in the description varies inversely with the breadth of the system. For a system as broad as the National Airspace System (NAS) our description would be very general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, could include a lot of detail to support the assessment.

First, a definition of “system” is needed. This handbook and MIL-STD-882<sup>1</sup> (System Safety Program Requirements) define a system as:

*A composite at any level of complexity, of personnel, procedures, material, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operation or support environment to perform a given task or achieve a specific production, support, or mission requirement.*

Graphically, this is represented by the 5M and SHELL models, which depict, in general, the types of elements that should be considered within most systems.

## 5M model of System Engineering



- Msn - Mission: central purpose or functions
- Man - Human element
- Mach - Machine: hardware and software
- Media - Environment: ambient and operational environment
- Mgt- Management: procedures, policies, and regulations

### **Figure 3-6: The Five-M Model**

**Mission.** The mission is the purpose or central function of the system. This is the reason that all the other elements are brought together.

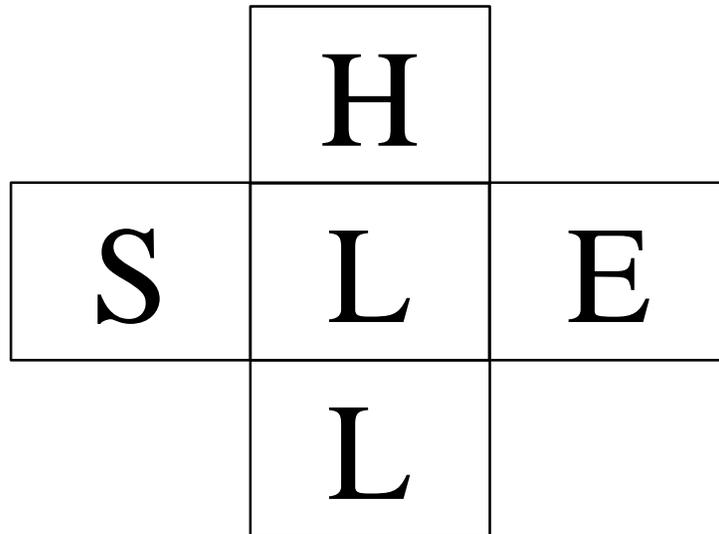
**Man.** This is the human element of a system. If a system requires humans for operation, maintenance, or installation this element must be considered in the system description.

**Machine.** This is the hardware and software (including firmware) element of a system.

**Management.** Management includes the procedures, policy, and regulations involved in operating, maintaining, installing, and decommissioning a system.

(1) **Media.** Media is the environment in which a system will be operated, maintained, and installed. This environment includes operational and ambient conditions. Operational environment means the conditions in which the mission or function is planned and executed. Operational conditions are those involving things such as air traffic density, communication congestion, workload, etc. Part of the operational environment could be described by the type of operation (air traffic control, air carrier, general aviation, etc.) and phase (ground taxiing, takeoff, approach, enroute, transoceanic, landing, etc.). Ambient conditions are those involving temperature, humidity, lightning, electromagnetic effects, radiation, precipitation, vibration, etc.

## SHELL Model of a system



S= Software (procedures, symbology, etc.)  
H= Hardware (machine)  
E= Environment (operational and ambient)  
L= Liveware (human element)

**Figure 3-6: The SHELL Model**

In the SHELL model, the match or mismatch of the blocks (interface) is just as important as the characteristics described by the blocks themselves. These blocks may be re-arranged as required to describe the system. A connection between blocks indicates an interface between the two elements.

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

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

**Functional description:** A functional description should describe what the system is intended to do, and should include subsystem functions as they relate to and support the system function. Review the FAA System Engineering Manual (SEM) for details on functional analysis.

**Physical characteristics:** A physical description provides the audience with information on the real composition and organization of the tangible system elements. As before, the level of detail varies with the size and complexity of the system, with the end objective being adequate audience understanding of the safety risk.

**Both models describe interfaces.** These interfaces come in many forms. The table below is a list of interface types that the system engineer may encounter.

Interface Type	Examples
Mechanical	Transmission of torque via a driveshaft. Rocket motor in an ejection seat.
Control	A control signal sent from a flight control computer to an actuator. A human operator selecting a flight management system mode.
Data	A position transducer reporting an actuator movement to a computer. A cockpit visual display to a pilot.
Physical	An avionics rack retaining several electronic boxes and modules. A computer sitting on a desk. A brace for an air cooling vent. A flapping hinge on a rotor.
Electrical	A DC power bus supplying energy to an anti-collision light. A fan plugged into an AC outlet for current. An electrical circuit closing a solenoid.
Aerodynamic	A stall indicator on a wing. A fairing designed to prevent vortices from impacting a control surface on an aircraft.
Hydraulic	Pressurized fluid supplying power to an flight control actuator. A fuel system pulling fuel from a tank to the engine.
Pneumatic	An adiabatic expansion cooling unit supplying cold air to an avionics bay. An air compressor supplying pressurized air to an engine air turbine starter.
Electromagnetic	RF signals from a VOR . A radar transmission.

<sup>i</sup> MIL-STD-882. (1984). Military standard system safety program requirements. Department of Defense.

## **Chapter 4: Safety Assessments Before Investment Decision**

<b>4.0 SAFETY ASSESSMENTS BEFORE INVESTMENT DECISION.....</b>	<b>2</b>
<b>4.1 OPERATIONAL SAFETY ASSESSMENT .....</b>	<b>3</b>
<b>4.2 COMPARATIVE SAFETY ASSESSMENT (CSA) .....</b>	<b>10</b>

#### 4.0 Safety Assessments Before Investment Decision

Before the investment decision at JRC 2, there are two phases of the acquisition life cycle: Mission Analysis and Investment Analysis. The Pre-Investment phase of a program encompasses the Mission Analysis and Investment Analysis phases of the Acquisition cycle illustrated in Figure 4-1. System safety's purpose during these phases is twofold. The first purpose is to develop early safety requirements that form the foundation of the safety and system engineering efforts. The second purpose is to provide objective safety data to the management activity when making decisions. The early assessment of alternatives saves time and money, and permits the "decision makers" to make informed, data driven decisions when considering alternatives. This section describes the System Safety assessments typically performed prior to the decision to approve a Mission Need at JRC-1, and prior to the decision to go forward with the program at JRC-2. The pre-investment safety assessments are: (1) Operational Safety Assessment (OSA) and (2) Comparative Safety Assessment (CSA).

#### System Safety Products in the AMS Life Cycle

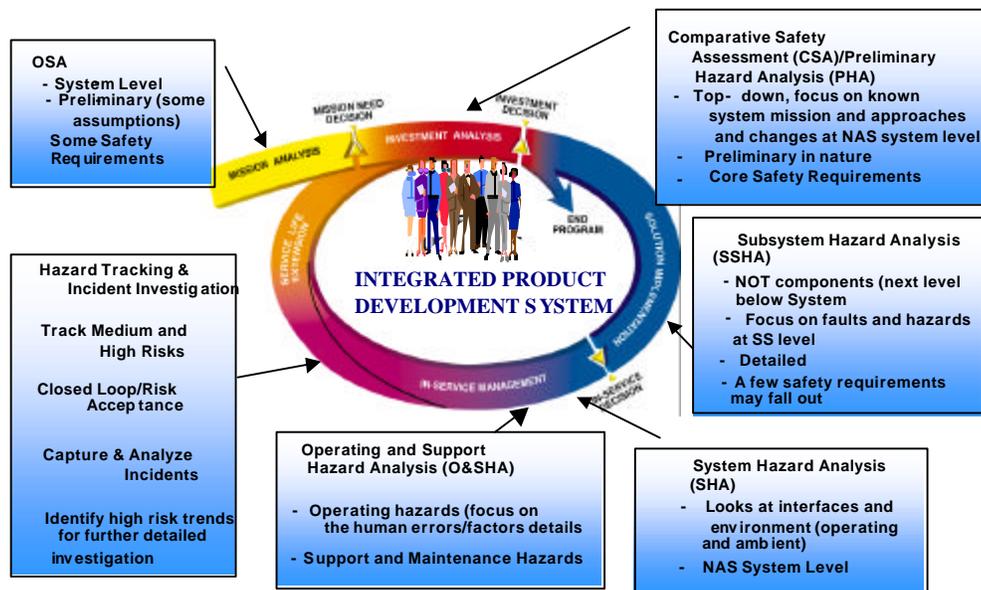


Figure 4-1: Safety Products in AMS Life Cycle

An Operational Safety Assessment (OSA) has been designed to provide a disciplined, and internationally developed (RTCA SC189) method of objectively assessing the safety requirements of aerospace systems. In the FAA, the OSA is used to evaluate Communication, Navigation, Surveillance (CNS) and Air Traffic Management (ATM) systems. The OSA identifies and provides an assessment of the hazards in a system,

defines safety requirements, and builds a foundation for follow-on institutional safety analyses related to Investment Analysis, Solution Implementation, In-Service Management, and Service Life Extension.

The OSA is composed of two fundamental elements: (1) the Operational Services & Environment Description (OSED), and (2) an Operational Hazard Assessment (OHA). The OSED is a description of the system physical and functional characteristics, the environment's physical and functional characteristics, air traffic services, and operational procedures. This description includes both the ground and air elements of the system to be analyzed. The OHA is a qualitative safety assessment of the operational hazards associated with the OSED. Each hazard is classified according to its potential severity. Each classified hazard is then mapped to a safety objective based on probability of occurrence. In general, as severity increases, the safety objective is to decrease probability of occurrence.

The information contained in the OSA supports the early definition of system level requirements. It is not a risk assessment in a classical sense. Instead, the OSA's function is to determine the system's requirements early in the life cycle. The early identification and documentation of these requirements may improve system integration, lower developmental costs, and increase system performance and probability of program success. While the OSA itself is not a risk assessment, it does support further safety risk assessments that are required by FAA Order 8040.4. The follow-on safety assessments may build on the OSA's OSED and OHA, by using the hazard list, system descriptions, and severity codes identified in the OSA. The OSA also provides an essential input into CSA safety assessments that support trade studies and decision making in the operational and acquisition processes.

The CSA is a safety assessment performed by system safety to assess the hazards and relative risks associated with alternatives in a change proposal. The alternatives can be design changes, procedure changes, or program changes. It is useful in trade studies and in decision-making activities where one or more options are being compared in a system or alternative evaluation. This type of risk assessment can be used by management to compare and rank risk reduction alternatives. More details on how to perform a CSA are included in section 4.2.

## **4.1 Operational Safety Assessment**

The OSA is intended to provide system level safety requirements assessment of aerospace CNS/ATM systems. As described above it is composed of two elements: (1) The Operational Environment Definition (OSED) and (2) the Operational Hazard Assessment (OHA). The OSA is based on an RTCA/SC-189 framework.

### **4.1.1 Operational Environment Definition (OED)**

The OED is basically a system description that may include all the elements of the 5M model. See chapter 3 for instructions on developing a system description.

### **4.1.2 OSA Tasks**

The steps within this task are:

- Define the boundaries of the system under consideration. Determine, separate, and document what elements of the system you will describe/analyze from those that you will not

describe/analyze. The result of this process is a model of the system under analysis that will be used to analyze hazards.

- Using models such as those described in chapter 3, describe the system physical and functional characteristics, the environment physical and functional characteristics, air traffic services, human elements (e.g. pilots and controllers, etc.) and operational procedures.
- From this description, determine and list the system functions. For example, the primary function of a precision navigation system is to provide CSA and flight crews with vertical and horizontal guidance to the desired landing area. These functions could be split if desired into vertical and horizontal guidance. Supporting functions would be those functions that provide the system the capability to perform the primary function. For instance a supporting function of the precision navigation system would be transmission of the RF energy for horizontal guidance. It is up to the system engineering team to determine how to group these functions and to what level to take the analysis. Detailed analyses would go into the lower level functions. Typically the OSA functional analysis is limited to the top-level functions. See FAA System Engineering Manual for more detailed guidance on functional analysis.

#### 4.1.3 Operational Hazard Assessment

The Operational Hazard Assessment (OHA) is the second part of the OSA. The OHA is a qualitative assessment of the hazards associated with the system described in the OSED.

##### Determining functions and hazards

Once the system has been bounded, described, and the functions determined in the OSED, the analyst is ready to determine the hazards associated with the system. For these types of assessments the best method is to assess scenarios containing a set of hazardous conditions. Therefore, the following definition can be used to define the hazards in a Preliminary Hazard List (PHL):

Hazard	<p>The potential for harm. Unsafe acts or unsafe conditions that could result in an accident. (A hazard is not an accident).</p> <p><u>Hazard or hazardous condition.</u> Anything, real or potential, that could make possible, or contribute to making possible, an accident.</p> <p><u>Hazard.</u> A condition that is prerequisite to an accident</p>
--------	---

Since the work has already been done in defining the system operational environment, it is often best to relate the functions of the system to hazards. For example, in analyzing the NAS, one would find the following functions of the NAS (listed in Table 4.1-1). These functions are then translated into hazards that would be included in the preliminary hazard list. For many of the listed hazards other conditions must be present before an accident could occur. These are detailed in the detailed description of the risk assessment. The purpose here is to develop a concise, clear, and understandable PHL.

**Table 4-1: Examples of NAS System Functions and Their Associated Hazards**

NAS System function	NAS System hazard
Provide air – ground voice communications.	Loss of air – ground voice communication.
Provide CSA precision approach instrument guidance to runways.	Loss of precision instrument guidance to the runway.
Provide En Route Flight Advisories of severe weather.	Lack EFAS warning of severe weather in flight path to CSA flight crew.

In addition to the functional analysis, the following tools can be used to identify the foreseeable hazards to the system operation. These tools are listed in Table 4-2.

#### Determining Severity of Consequence

The severity of each hazard is determined by the worst credible outcome, or effect of the hazard on the CSA or system. This is done in accordance with MIL-STD-882 and FAR/AMJ 25.1309. Both documents state that the severity should consider all relevant stages of operation/flight and worst case conditions. See the risk determination Table 3-2 to define the severity levels of a hazard.

**Table 4-2: Safety Analysis Tools**

<b>OPERATIONS ANALYSIS</b>	<i>Purpose:</i> To understand the flow of events. <i>Method:</i> List events in sequence. May use time checks.
<b>PRELIMINARY HAZARD ANALYSIS (PHA)</b>	<i>Purpose:</i> To get a quick hazard survey of all phases of an operation. In low hazard situations the PHA may be the final Hazard ID tool. <i>Method:</i> Tie it to the operations analysis. Quickly assess hazards using scenario thinking, brainstorming, experts, accident data, and regulations. Considers all phases of operations and provides early identification of highest risk areas. Helps prioritize area for further analysis.
<b>“WHAT IF” TOOL</b>	<i>Purpose:</i> To capture the input of operational personnel in a brainstorming-like environment. <i>Method:</i> Choose an area (not the entire operation), get a group and generate as many “what ifs” as possible.
<b>SCENARIO PROCESS TOOL</b>	<i>Purpose:</i> To use imagination and visualizations to capture unusual hazards. <i>Method:</i> Using the operations analysis as a guide, visualize the flow of events.
<b>LOGIC DIAGRAM</b>	<i>Purpose:</i> To add detail and rigor to the process through the use of graphic trees. <i>Method:</i> Three types of diagrams- positive, negative, and risk event.

<b>CHANGE ANALYSIS</b>	<i>Purpose:</i> To detect the hazard implications of both planned and unplanned change. <i>Method:</i> Compare the current situation to a previous situation.
<b>CAUSE &amp; EFFECT TOOL -- CHANGE ANALYSIS</b>	<i>Purpose:</i> To add depth and increased structure to the Hazard ID process through the use of graphic trees. <i>Method:</i> Draw the basic cause and effect diagram on a worksheet. Use a team knowledgeable of the operation to develop causal factors for each branch. Can be used as a positive or negative diagram. <i>Purpose:</i> To detect the hazard implications of both planned and unplanned change. <i>Method:</i> Compare the current situation to a previous situation.
<b>CAUSE &amp; EFFECT TOOL</b>	<i>Purpose:</i> To add depth and increased structure to the Hazard ID process through the use of graphic trees. <i>Method:</i> Draw the basic cause and effect diagram on a worksheet. Use a team knowledgeable of the operation to develop causal factors for each branch. Can be used as a positive or negative diagram.

**OHA Tasks**

The tasks to be accomplished in this phase are:

- From the function list (or tools listed in Table 4-2) develop the list of hazards potentially existing in the system under study
- Determine the potential severity of each hazard in the hazard list by referring to the risk determination section of Chapter 3.

**4.1.4 Allocation of Safety Objectives and Requirements (ASOR)**

The Allocation of Safety Objectives and Requirements (ASOR) is the process of using hazard severity to determine the objectives and requirements of the system. There are two levels of requirements in this process: (1) objectives (or goals) and (2) requirements (or minimum levels of acceptable performance). The purpose of the ASOR is to establish requirements that ensure that the probability of a hazard leading to an accident has an inverse relationship to the severity of occurrence. This inverse relationship is called the Target Level of Safety (TLS). For example, a “hazardous” or severity 2 hazard would have a requirement (shown by arrows in Figure 4-1) to show by analysis or test to have a probability of occurrence of Extremely Remote or less than one in one-million operating hours for the fleet or system. The objective or (desired probability) in this case would be Extremely Improbable or one occurrence in one billion per operating hour for the fleet or system. See Figure 4-2 for the steps in this process.

Once the TLS is determined for each hazard, requirements can be written to ensure that the appropriate hazard controls are established as system requirements.

## Steps

## Hazard Classification

1. Determine potential severity of each hazard in the OHA.
2. Map severity to this chart to determine probability requirement (minimum) and objective (desired) Target Level of Safety (TLS)
3. Allocate the safety objectives and requirements (ASOR) from the TLS to air and/or ground elements

Severity Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A					
Remote B					
Extremely Remote C					
Extremely Improbable D					

High Risk
Medium Risk
Low Risk

Figure 4-2: Target Level of Safety Determination

#### 4.1.5 Identification of High Level Hazard controls

The next step is to determine the hazard controls. Controls are measures, design features, warnings, and procedures that mitigate or eliminate risk. They either reduce the severity or probability of a risk. System Safety uses an order of precedence when selecting controls to reduce risk (MIL-STD-882, 1984). This order of precedence as discussed in Section 3.6, and Table 3.6-1

Clearly risk reduction by design is the preferred method of mitigation. But even if the risk is reduced, the term “reduction” still implies the existence of residual risk, which is the risk left over after the controls are applied. For example, residual risk can be controlled in a manner described in Table 4-3. This table describes the NAS System Function, NAS System Hazard, and NAS System Control.

**Table 4-3: Development of Controls for Hazards in the NAS**

<b>NAS System function</b>	<b>NAS System hazard</b>	<b>NAS System Controls</b>
Provide air - ground communications.	Loss of air – ground communication.	Multiple communication channels. Multiple radios. Procedures for loss of communication. Phase dependent: communication is not always critical.
Provide CSA precision approach instrument guidance to runways.	Loss of precision instrument guidance to the runway.	Reliability. Alternate approaches available. Procedures for alternate airport selection. Fuel reserve procedures. System detection and alert to CSA. Phase and condition (IMC vs. VMC) dependent.
Provide En Route Flight Advisories of severe weather.	Lack EFAS warning of severe weather to CSA flight crew.	Early detection systems (satellite) for severe weather. Multiple dissemination means. Procedures (condition dependent) require alternate airports. Fuel reserve procedures.

As the engineer performs the assessment, controls that do not yet exist can be identified and listed. These controls are included in the requirements of the OSA. This is done by turning the controls into measurable and testable requirements or “shall” statements. A critical function of System Engineering is the determination and allocation of requirements early in the concept and definition phase. System Safety’s function in this process is to develop safety-related requirements early in the design to facilitate System Engineering. A primary source of safety requirements is the OSA. The controls identified, both existing and recommended, should be translated into a set of system level requirements. For example, Table 4-4 lists the same hazards and controls that were examined in Table 4-3. The requirements are examples only and are meant for illustration.

Table 4-4: Examples of Controls and Requirements

<b>NAS System Function</b>	<b>NAS System Hazard</b>	<b>NAS System Controls</b>	<b>NAS System Requirements</b>
Provide air to ground communications and control.	Loss of air to ground communication and control.	Multiple communication channels. Multiple radios. Procedures for loss of communication. Phase dependent: communication is not always critical.	The NAS system shall provide for multiple communication modes in the enroute structure, at least 2 channels in each region being in the VHF frequency spectrum, and one available through the satellite communication system. The total Mean Time Between Failure (MTBF) of these systems may not be less than X hours.
Provide CSA precision approach instrument guidance to runways.	Loss of precision instrument guidance to the runway.	Reliability. Alternate approaches available. Procedures for alternate airport selection. Fuel reserve procedures. System detection and alert to CSA. Phase and condition (IMC vs. VMC) dependent.	The NAS shall provide at least two backup non-precision approaches at each airport with a precision approach capability. The NAS procedures shall require part 121 operators to select an alternate destination if the forecast weather at the planned destination is less than 500' and 1 mile over the destinations weather planning minimums within one hour of the planned arrival.
Provide Enroute Flight Advisories of severe weather.	Lack EFAS warning of severe weather to CSA flight crew.	Early detection systems (satellite) for severe weather. Multiple dissemination means. Procedures (condition dependent) require alternate airports. Fuel reserve procedures.	The NAS shall detect icing conditions greater than moderate accretion when it actually exists in any area of 10 miles square and at least 1000' thick for greater than 15 minutes duration.

**Tasks in the ASOR phase**

Determine existing and recommended hazard controls for each hazard.

Develop requirements based on the TLS and controls.

- Allocate the requirements so that both ground CNS/ATM and airborne systems share the controls.

## 4.2 COMPARATIVE SAFETY ASSESSMENT (CSA)

Comparative Safety Assessments (CSAs) are performed to assist management in the process of decision making. The CSA is a risk assessment, in that it defines both severity and likelihood in terms of the current risk of the system. Whereas an OSA defines the target level of safety, a risk assessment provides an estimation of the risk associated with the identified hazards.

The first step within the CSA process involves describing the system under study in terms of the 5M model (chapter 3). Since most decisions are a selection of alternatives, each alternative must be described in sufficient detail to ensure the audience can understand the hazards and risks evaluated. Many times one of the alternatives will be “no change”, or retaining the baseline system. A preliminary hazard list (PHL) is developed and then each hazard’s risk is assessed in the context of the alternatives. After this is done, requirements and recommendations can be made based on the data in the CSA. A CSA should be written so that the decision-maker can clearly distinguish the relative safety merit of each alternative. An example (with instructions) of a CSA is included in Appendix B.

### 4.2.1 Principles of Comparative Safety Assessments

In general, CSA should:

Be objective

Be unbiased

Include all relevant data

Use assumptions only if specific information is not available. If assumptions are made they should be conservative and clearly identified. Assumptions should be made in such a manner that they do not adversely affect the safety of the system.

Define risk in terms of severity and likelihood in accordance with chapter 3, paragraph 3.4. Severity is independent of likelihood in that it can and should be defined without considering likelihood of occurrence. Likelihood is dependent on severity. The definition of likelihood should be made on how often an accident can be expected to occur, not how often the hazard occurs.

Compare the results of the risk assessment of each hazard for each alternative considered in order to rank the alternatives for decision making purposes.

Assess the safety risk reduction or other benefits associated with implementation of and compliance with an alternative under consideration.

Assess risk in accordance with the risk determination defined in Tables 3-2 and 3-3.

### 4.2.2 Steps in performing a CSA

Define the system under study in terms of the 5m model described in chapter 3 for the baseline system and all alternatives.

Perform a functional analysis in accordance with the FAA System Engineering handbook. This analysis will result in a set of hierarchical functions that the system performs.

From the functions and system description, develop a preliminary hazard list as described earlier in this chapter.

List these PHL hazard conditions in the form contained in Appendix B

Evaluate each hazard – alternative combination for severity using the definitions contained in chapter 3. This must be done in accordance with the principles contained in this manual, which require evaluation of the hazard severity in the context of the worst credible conditions.

Evaluate the likelihood of occurrence of the hazard conditions resulting in an accident at the level of severity indicated in (4) above. These definitions can be found in chapter 3, Table 7 of this guidebook. This means that the likelihood selected is the probability of an accident happening in the conditions described in (4), and not the probability of just the hazard occurring.

Document the assumptions and justification for how severity and likelihood for each hazard condition was determined.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

## **Chapter 5: Post-Investment Decision Safety Activities**

<b>5.0</b>	<b>POST-INVESTMENT DECISION SAFETY ACTIVITIES .....</b>	<b>2</b>
<b>5.1</b>	<b>OBJECTIVES AND REQUIREMENTS.....</b>	<b>2</b>
<b>5.2</b>	<b>PREPARING A SYSTEM SAFETY PROGRAM PLAN.....</b>	<b>5</b>
<b>5.3</b>	<b>SYSTEM SAFETY PROGRAM PLAN CONTENTS .....</b>	<b>8</b>
<b>5.4</b>	<b>INTEGRATED SYSTEM SAFETY PROGRAM PLAN .....</b>	<b>18</b>
<b>5.5</b>	<b>PROGRAM BALANCE.....</b>	<b>23</b>
<b>5.6</b>	<b>PROGRAM INTERFACES.....</b>	<b>23</b>
<b>5.7</b>	<b>TAILORING .....</b>	<b>26</b>

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

## 5.0 Post-Investment Decision Safety Activities

After a program baseline is approved, it transitions to the IPT for Solution Implementation. In this phase, the IPT prepares the necessary documentation to acquire the system. At this point, the IPT has been involved during the IA process, and has prepared the Acquisition Program Baseline, Acquisition Strategy Paper and Integrated Program Plan for approval by the JRC. It is now the team's responsibility to work with the procurement organization to prepare the Request for Proposal and Statement of Work. This chapter defines how to establish a System Safety Program for the acquisition. Chapter 6 defines guidelines for how to manage the contracting activity for a contractor's System Safety Program Plan. It is appropriate to point out that an initial System Safety Program Plan (SSPP) is prepared prior to the Investment Decision and well as one following JRC2, as described in this chapter.

### 5.1 Objectives and Requirements

The principal objective of an SSP within the FAA is to ensure that safety is consistent with mission requirements and is designed into systems, subsystems, equipment, facilities, and their interfaces and operation. The degree of safety achieved in a system depends directly on management emphasis and commitment. The FAA and its contractors must apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system, ensuring that accident risk is identified and understood, and that risk reduction is always considered in the management review process.

A formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to the managing activity (MA) is not only effective from a safety point of view but is also cost effective.

The FAA SSP is structured on common-sense procedures that have been effective on many programs. These procedures are commonly known as the Safety Order of Precedence as summarized in Table 5-1. These four general procedures are used to establish the following SSP activities:

- Eliminate identified hazards or reduce associated risk through design, including material selection or substitution.
- Design to minimize risk created by human error in the operation and support of the system.
- Protect power sources, controls, and critical components of redundant subsystems by separation, isolation, or shielding.
- When design approaches cannot eliminate a hazard, provide warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These will be standardized in accordance with MA requirements.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

**Table 5-1: Safety Order of Precedence**

Description	Priority	Definition
Design for minimum risk.	1	From the first design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.
Incorporate safety devices.	2	If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.
Provide warning devices.	3	When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response.
Develop procedures and training.	4	Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

- Design software controlled or monitored functions to minimize initiation of hazardous events or accidents.
- Review design criteria for inadequate or overly restrictive requirements regarding safety.
- Recommend new design criteria supported by study, analyses, or test data.
- Isolate hazardous substances, components, and operations from other activities, personnel, and incompatible materials.
- Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards.
- Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration).
- Consider application specific approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail-safe design, fire suppression, and protective clothing, equipment, devices, and procedures.
- Minimize the severity of personnel injury or damage to equipment in the event of an accident.

### **5.1.1 Management Responsibilities**

The MA, in order to meet the objectives and requirements of system safety, must conduct the following activities.

- Plan, organize, and implement an effective SSP that is integrated into all life cycle phases.
- Establish definitive SSP requirements for the procurement or development of a system. The requirements must be set forth clearly in the appropriate system specifications and contractual documents.
- Ensure that a System Safety Program Plan (SSPP) is prepared that reflects in detail how the total program is conducted.
- Review and approve for implementation the SSPPs prepared by the contractor.
- Supply historical safety data as available.
- Monitor contractors' system activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.
- Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.
- Evaluate new design criteria for inclusion into FAA specifications and standards, and submit recommendations to the respective responsible organization.
- Establish System Safety Working Groups as appropriate to assist the program manager in developing and implementing an SSP.
- Establish work breakdown structure elements at appropriate levels for system safety management and engineering.

### **5.1.2 Management Risk Reviews**

Management is responsible for reducing the risk of accidents to an acceptable level. The SSP is the vehicle to achieve this objective. Unless there is a dedicated SSP, safety is not a first priority regardless of intentions. Reducing risk is a primary objective of the SSP. The system safety activities assist the program manager in identifying the following:

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

- Nature of the accident and hazards
- Place of its occurrence
- Alternatives to control risks through design, operations, and procedures
- Implementation and effectiveness of hazard control.
- A properly planned SSP defines and funds the analyses necessary to identify risks throughout the life cycle of the system.

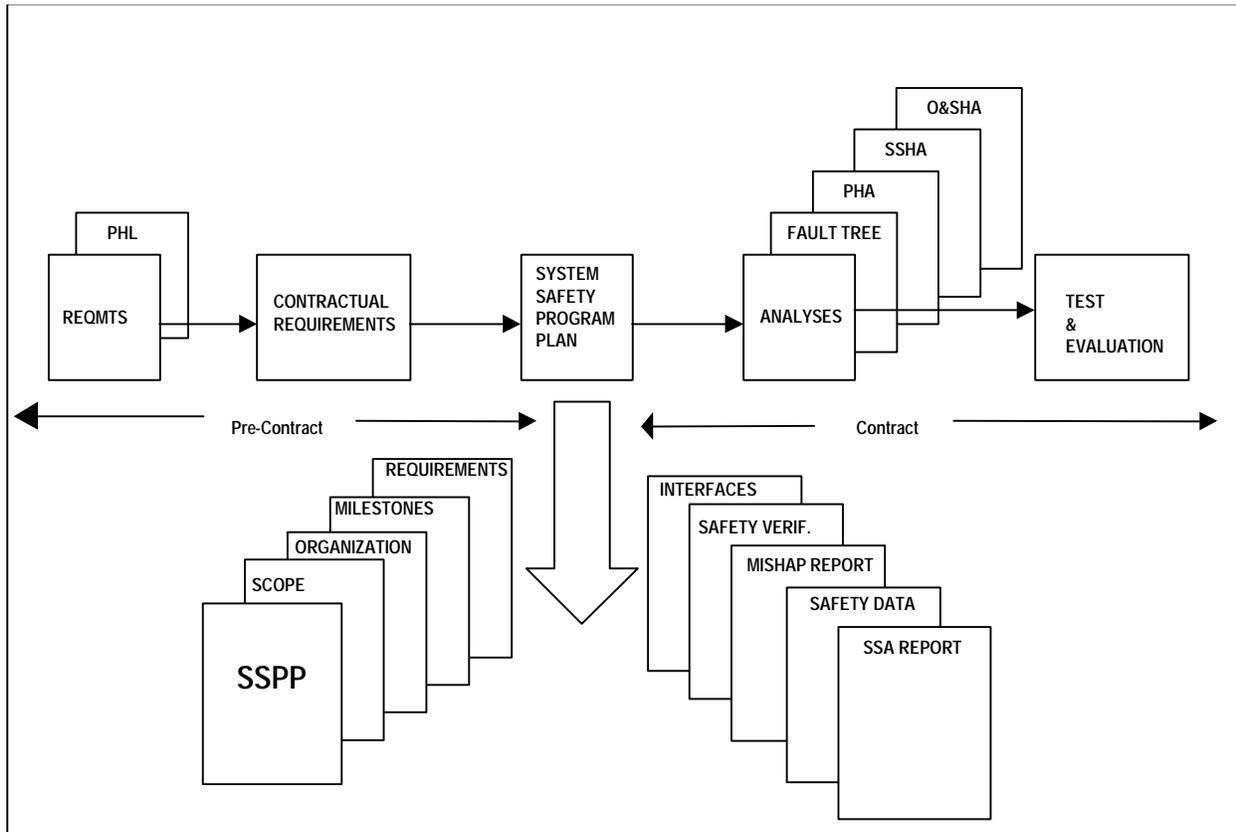
The following is a partial list of safety activities that can help the program manager control safety risks.

- Develop and distribute safety guidance for the entire life cycle of the system (i.e., design, development, production, test, transportation, handling, operation, and maintenance).
- Integrate safety activities into all systems engineering and National Airspace Integrated Logistics Support (NAILS) activities. This integration requires the entire design, manufacturing, test and logistics support teams to identify hazards and implement controls.
- Perform safety analysis in a timely manner.
- Communicate safety requirements and analyses to all subcontractors of safety significant equipment.
- Ensure that safety analysis results are discussed in design and document reviews.
- Execute closed loop procedures to ensure that required safety controls are actually implemented (e.g., warnings in technical manuals and training programs).
- Review historical data for similar applications.
- Demonstrate corrective actions for identified risks.

## 5.2 Preparing a System Safety Program Plan

An approved System Safety Program Plan (SSPP) is a contractually binding understanding between the FAA and a contractor on how the contractor intends to meet the specified system safety requirements. When there are projects or systems that have multiple subcontractors, an Integrated System Safety Program plan (ISSPP) should be developed. These plans should describe in detail the contractor's safety organization, schedule, procedures, and plans for fulfilling the contractual system safety obligations. The SSPP is a management vehicle for both the FAA and the contractor. The FAA uses the SSPP approval cycle to ensure that proper management attention, sufficient technical assets, correct analysis and hazard control methodology, and tasks are planned in a correct and timely manner. Once approved, the FAA uses the SSPP to track contractor System Safety Program (SSP) progress. The SSPP is of value to the contractor as a planning and management tool that establishes "before the fact" an agreement with the FAA on how the SSP will be executed and in what depth. In summary, the approved SSPP is an SSP baseline document that minimizes the potential for downstream disagreement of SSP methodology. Figure 5-1 shows the position of the SSPP relative to other parts of the SSP. MIL-STD-882 and the SSMP provide guidance on establishing an SSPP. These documents describe in detail the tasks and activities of system safety management and system safety engineering that are required to identify, evaluate, and eliminate hazards, or reduce the associated risk to a level acceptable to the FAA throughout the system's life cycle.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000



**Figure 5-1: System Safety Program Plan**

The FAA establishes the contractual requirements for a SSPP in the Statement of Work (SOW). The FAA requires the contractor to establish and maintain an effective and efficient SSP. This is usually the first safety requirement stated in the SOW. SSP requirements are defined by MIL-STD-882, Section 4. They are the only mandatory requirements and cannot be tailored. The System Safety Program Plan purpose is to plan and document the system safety engineering effort necessary to ensure a safe system. The SSPP will:

- Describe the program's implementation of the requirements of MIL-STD-882D, including identification of the hazard analysis and accident risk assessment processes to be used.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

- Include information on how system safety will be integrated into the overall system Integrated Product Development System and Integrated Product Team structure in the FAA.
- Define how hazards and residual risk are communicated to the program manager, and how the program manager will formally accept and track the hazards and residual risk.

The SSPP contains the scope, organization, milestones, requirements, safety data, safety verification, accident reporting, and safety program interfaces.

The Statement of Work will normally include the following elements:

- Acceptable level of risk with reporting thresholds\*
- Minimum hazard probability and severity reporting thresholds\*
- MA requirements for accident reporting
- Requirements for and methodology to the MA for the following:
- Residual hazards/risks
- Safety critical characteristics and features
- Operating, maintenance, and overhaul safety requirements
- Measures used to abate hazards
- Acquisition management of hazardous materials
- Qualifications of key system safety personnel
- Other specific SSP requirements

Note: An asterisk (\*) following an item indicates required SOW contents.

The SSPP is usually required to be submitted as a deliverable for MA approval 30 to 45 days after start of the contract. In some situations, the MA may require that a preliminary SSPP be submitted with the proposal to ensure that the contractor has planned and costed an adequate SSP. Since the system safety effort can be the victim of a cost competitive procurement, an approval requirement for the SSPP provides the MA with the necessary control to minimize this possibility.

A good SSPP demonstrates risk control planning through an integrated program management and engineering effort. It is directed towards achieving the specified safety requirements of the SOW and equipment specification. The plan includes details of those methods the contractor uses to implement each system safety task described by the SOW and those safety related documents listed in the contract for compliance (MIL-STD-882, paragraph 6.2). Examples of safety-related documents include Occupational Safety and Health Administration (OSHA) regulations and other national standards, such as the National Fire Protection Association (NFPA). The SSPP lists all requirements and activities required to satisfy the SSP objectives, including all appropriate related tasks. A complete breakdown of system safety tasks, subtasks, and resource allocations for 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.

Plans generated by one contractor are rarely efficient or effective for another. Each plan is unique to the corporate personality and management system. This is important to remember in competitive procurement of a developed or partially developed system. The plan is prepared so that it describes the

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

system safety approach to be used on a given program at a given contractor's facilities and describes the system safety aspects and interfaces of all appropriate program activities. The contractor's approach to defining the critical tasks leading to system safety certification is included.

The plan should describe an organization featuring a system safety manager who is directly responsible to the program manager or the program manager's agent for system safety. This agent must not be organizationally inhibited from assigning action to any level of program management. The plan further describes methods by which critical safety problems are brought to the attention of program management and for management approval of closeout action. Organizations that show responsibility through lower levels of management are ineffective, and therefore unacceptable.

The SSPP is usually valid for a specific phase of the system life cycle, because separate contracts are awarded as development of equipment proceeds through each phase of the life cycle. For example, a contract award may be for the development of a prototype during the validation phase. A subsequent contract may be awarded to develop pre-production hardware and software during full-scale development, and still another awarded when the equipment enters the production phase. Progressing from one phase of the life cycle to the next, the new contract's SOW should specify that the SSPP prepared for the former contract be revised to satisfy the requirements of the new contract and/or contractor.

## **5.3 System Safety Program Plan Contents**

### **5.3.1 Program Scope**

The SSPP must define a program to satisfy the system safety requirements imposed by the contract. It describes, as a minimum, the four elements of an effective SSP:

- A planned approach for task accomplishment
- Qualified staff to accomplish tasks
- Authority to implement tasks through all levels of management
- Appropriate staffing and funding resources to ensure tasks are completed

Each plan should include a systematic, detailed description of the scope and magnitude of the overall SSP 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. It is helpful to the evaluator if two matrices are included:

- Contractual paragraph compliance mapped to an SSPP.
- Contractual paragraph compliance mapped to those functions within the contractors organization that have the responsibility and have been allocated resources for ensuring that those requirements are met.
- The SSPP should start with a brief section, entitled Scope, that describes the equipment to be covered, the program phase, and the source of the SSP requirements.

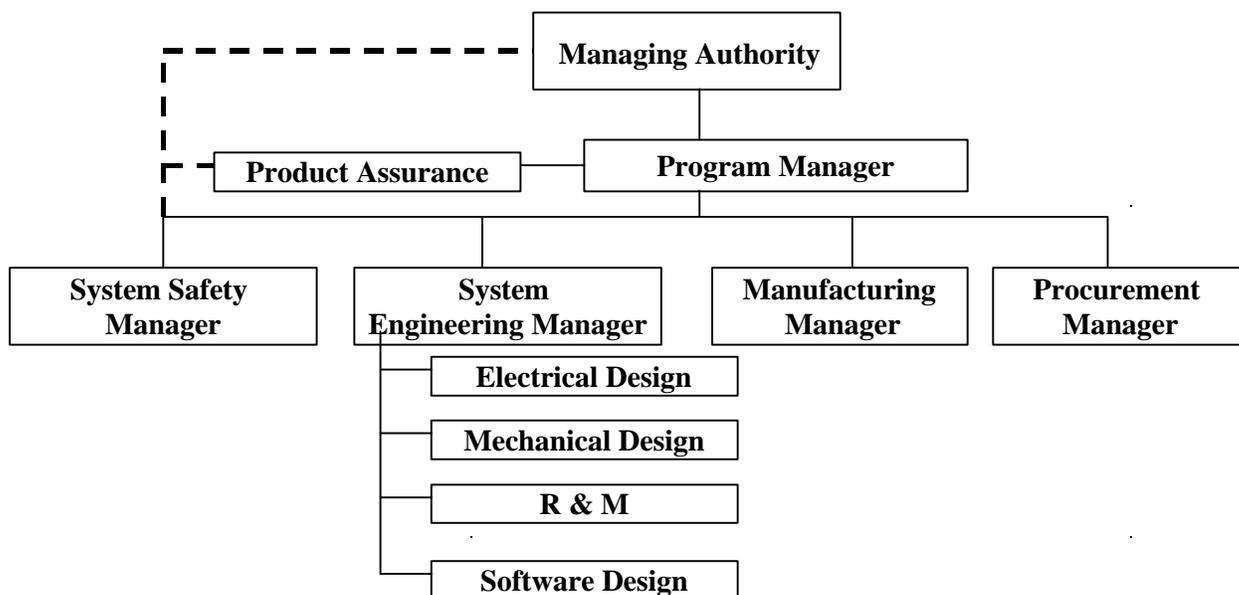
### **5.3.2 System Safety Organization**

The SSPP contains a section that describes the details of Systems Safety Organization. These details are described below.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

**The system safety organization or function as it relates to the program organization**

- The organizational and functional relationships
- Lines of communication.
- The position of the safety organization in a sample program organization (illustrated in Figure 5-2). Note that the system safety manager is at the same reporting level as the managers of design engineering. The organization includes:
  - The contractor's system safety personnel. Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel should be the responsibility of the system safety manager through the manager's interface with other program disciplines. The system safety manager should also be responsible for initiation of required action whenever internal coordination of controls fail in the resolution of problems.
  - Other contractor organizational elements involved in the System Safety Working Groups (SSWGs). System safety responsibilities are an inherent part of every program function and task. Examples include reliability and test and evaluation (T&E).



**Note: The System Safety manager is a staff function to the Program Manager, with access to all lines of upper management included within the Managing Authority.**

**Figure 5-2: Sample Safety Organization Chart**

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

***Responsibility and authority of all personnel with significant safety interfaces***

- The contractor's system safety personnel.
- Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel should be the responsibility of the system safety manager through the manager's interface with other program disciplines.
- The system safety manager should also be responsible for initiation of required action whenever internal coordination of controls fail in the resolution of problems.
- Other contractor organizational elements involved in the System Safety Working Groups (SSWGs). System safety responsibilities are an inherent part of every program function and task. Examples include reliability and test and evaluation (T&E).
- The organizational unit responsible for executing each task (e.g. reliability or T&E) and its authority in regard to resolution of all identified hazards. Resolution and action relating to system safety matters may be effective at all organizational levels but must include the organizational level possessing resolution authority (e.g. program or engineering manager). The SSP manager should be identified by name, with address and phone number.

***The staffing plan of the system safety organization for the duration of the contract***

It should include staff loading, control of resources, and the qualifications of key system safety personnel assigned, including those who possess coordination/approval authority for contractor prepared documentation.

***The procedures by which the contractor will integrate and coordinate the system safety efforts,***

including assignment of the system safety requirements to internal organizations and subcontractors, coordination of subcontractor SSPs, integration of hazard analysis, program status reporting, and SSWGs.

***The process by which contractor management decisions will be made,***

including timely notification of unacceptable risks, necessary action, accidents or malfunctions, waivers to safety requirements, and program deviations.

The contractor must provide a description of a system safety function with a management authority, as the agent of the program manager, to maintain a continual overview of the technical and planning aspects of the total program. Although the specific organizational assignment of this function is a contractor's responsibility, the plan must show a direct accountability to the program manager with unrestricted access to any level of management to be acceptable.

The ultimate responsibility for all decisions relating to the conduct and implementation of the SSP rests with the program director or manager. Each element manager is expected to be fully accountable for the implementation of safety requirements in the respective area of responsibility.

In the usual performance of their duties, SSP managers must have direct approval authority over any safety critical program documentation, design, procedures, or procedural operation. A log of non-deliverable data should be maintained showing all program documentation reviewed, concurrence or non-

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

concurrence, reasons why the system safety engineer concurs or non-concurs, and actions taken as a result of non-concurrence. The MA should assess activity and progress by reviewing this log.

For major programs, the staffing forecast can be provided at the significant safety task level.

The contractor is required to assign a system safety manager who meets specific educational and professional requirements and who has had significant assignments in the professional practice of safety. Qualifications should reflect the system's criticality and SSP magnitude. Application of common sense is necessary. Clearly, the safety manager for an airframe program requires different credentials than one responsible for an avionics program. For major programs, a range of six to nine years of system safety experience is required. In some cases, it is justifiable to require either a registered Professional Engineer (PE) or a board Certified Safety Professional

In other cases, work experience may be substituted for educational requirements. Small programs or organizations may have limited access to personnel with full time safety experience, and the MA should be confident that such credentials are necessary for the specific application before invoking them.

The minimum qualifications for the systems safety manager or staff should be included in the contract. This may be difficult: The existence of a CSP is a rarity at electronic development and manufacturing companies. If a CSP is required, the contractor is likely to hire a part-time CSP consultant, a questionable approach. PEs are more common, but few have careers involving safety. Appendix A in MIL-STD-882 provides a table of minimum qualifications for programs based upon complexity and demands on CSP or PE qualifications. This approach ignores the hazard severity of the system.

Table 5-2 is suggested as a qualification baseline. It is not absolute and is offered only as guidance. The MA may adjust these qualifications, as appropriate.

### **5.3.3 Program Milestones**

To be effective, the system safety activities on any program must be integrated into other program activities. To be efficient, each SSP task must be carefully scheduled to have the most positive effect. A safety analysis performed early in the design process can lead to the inexpensive elimination of a hazard through design changes. The later the hazard is identified in the design cycle, the more expensive and difficult the change. Hazards identified in T&E production, or following deployment may be impractical to change. In such cases, hazards may still be controlled through procedural and training steps but having to do so, when they could have been prevented, reflects unnecessary long-term costs and risk.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

**Table 5-2: Key Personnel Systems Safety Qualifications**

<b>Program Complexity</b>	<b>Program Severity</b>	<b>Education</b>	<b>Experience</b>	<b>Certification</b>
High	Catastrophic	BS in Engineering or applicable other	Six years in system safety	CSP or PE desired; equivalent 10 yrs experience
High	Critical	BS in Engineering or applicable other	Six years in system safety or related discipline	CSP or PE desired; equivalent 10 yrs experience
High	Marginal	BS in Engineering or applicable other	Two years in system safety or related discipline	CSP or PE desired; equivalent 10 yrs experience
Moderate	Catastrophic	BS in Engineering or applicable other	Four years in system safety	CSP or PE desired; equiv. 10 yrs experience
Moderate	Critical	BS in Engineering or applicable other	Four years in system safety or related discipline	None
Moderate	Marginal	BS plus training in system safety	Two years in system safety or related discipline	None
Low	Catastrophic	BS plus training in system safety	Four years in system safety or related discipline	None
Low	Critical	BS plus training in system safety	Two years in system safety or related discipline	None
Low	Marginal	High School Diploma plus training in system safety	Two years in system safety or related discipline	None

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

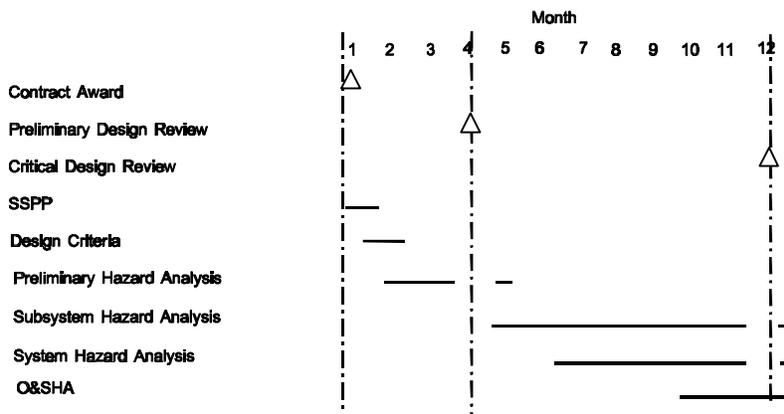
A SSPP prepared in accordance with MIL-STD-882 provides the FAA with an opportunity to review the contractor's scheduling of safety tasks in a timely fashion, permitting corrective action when applicable. MIL-STD-882 guides the contractor to plan and organize the system safety effort and provides the MA with necessary information for FAA support planning by requiring the elements listed below. Requirements to be adjusted for program, as necessary.

#### SSP milestones

Program schedule of safety tasks including start and completion dates, reports, reviews, and estimated staff loading

Identification of integrated system safety activities (e.g., design analysis, tests, and demonstration) applicable to the SSP but specified in other engineering studies to preclude duplication. (See Chapter 6, System Safety Integration and Risk Assessment)

The SSPP must provide the timing and interrelationships of system safety tasks relative to other program tasks. A suitable program milestone section of an SSPP will include a Gantt chart showing each significant SSP task, the period of performance for each, and related overall program milestones. For example, one expects the establishment of design criteria and the generation of the SSPP to begin almost immediately during any design phase; analyses to run concurrent to design activities and have at least interim completions prior to major design reviews; and the establishment of hazard tracking systems prior to a significant testing. Figure 5-3 shows an example of a Gantt chart.



**Figure 5-3: Sample SSPP Gantt Chart**

The schedule for each SSP task in the SSPP should be tied to a major milestone (e.g., start 30 days after or before the preliminary design review [PDR]) rather than a specific date, as MIL-STD-882 requires. In this manner, the SSPP does not need revision whenever the master program schedule shifts. The same MA control is maintained through the program master schedule but without the associated cost of documented revision or schedule date waiver.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

### **5.3.4 Requirements and Criteria**

A formally submitted SSPP provides the opportunity for the MA and the contractor to clearly reach the same understanding of technical and procedural requirements and plans before precious assets are expended. MIL-STD-882D Appendix A, provides guidance on the type of information to be included in the SSPP. The inclusion of this information expedites reaching a common understanding between the MA and the contractor. This information includes the following.

#### ***Safety Performance Requirements***

These are the general safety requirements needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate them into the system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of: a hazard category developed through a accident risk assessment matrix, an overall system accident rate, demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable accident risk assessment procedures. Listed below are some examples of how safety performance requirements could be stated.

Quantitative requirements. – usually expressed as a failure or accident rate, such as “ the Catastrophic system accident rate shall not exceed  $x.xx \times 10^y$  per operational hour.”

Accident risk requirements – could be expressed as “ No hazards assigned a Catastrophic accident severity are acceptable.” Accident risk requirements could also be expressed as a level defined by the accident risk assessment matrix. (see Chapter x. yy) such as “No Category 3 or higher accident risks are acceptable.”

Standardization requirements – are expressed relative to a known standard that is relevant to the system being developed. Examples include: The system will comply with the Federal Code of Regulations CFR-XXX, or “The system will comply with international standards developed by ICAO.”

#### ***Safety Design Requirements***

The program manager, in concert with the chief engineer and utilizing system engineering and associated system safety professionals, should establish specific safety design requirements for the overall system. The objective of safety design requirements is to achieve acceptable accident risk through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources. These are reviewed for safety parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. These requirements and criteria are expanded for inclusion in the associated follow-on or lower level specifications.

A composite list of all SSP requirements is included in the requirements and criteria section of the SSPP for several reasons. The list includes the following.

Organization and integration of safety requirements establishing clear SSP objectives. Frequently, safety requirements are included at multiple levels in a variety of specifications. Assembling a safety requirements composite list can be time consuming and, therefore, generating and formally documenting this list can expect to save significant staff labor costs and likely omissions by those without significant system safety experience.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

Providing MA assurance that no safety requirements have been missed and that the safety requirements have been interpreted correctly.

### **Documentation**

The inclusion of a description of risk assessment procedures, and safety precedence is an important example of where the SSPP contributes to the MA and the contractor reaching a common understanding. Without such details explicitly described in the SSPP, both the MA and contractor could, in good faith, proceed down different paths until they discover the difference of interpretation at a major program milestone.

The hazard analyses described in Chapters 8 & 9 illustrate some methodologies used to identify risks, and assign severity and criticality criteria. Safety precedence is a method of controlling specific unacceptable hazards. A closed loop procedure is required to ensure that identified unacceptable risks are resolved in a documented disciplined manner. The inclusion of such procedures demonstrates both necessary control and personnel independence.

The presence of the safety criteria in the SSPP is an important step in the system safety management process. This information must flow down to the system and design engineers (including appropriate subcontractors). SSPP must provide a procedure that incorporates system safety requirements and criteria in all safety critical item (CI) specifications. Such safety requirements include both specific design and verification elements.

Unambiguous communication between the FAA and the contractor depends on standardized definitions. The FAA may choose for expediency, to invoke a MIL-STD-882 SSP. It must be noted that the definitions included in MIL-STD-882 are not identical to those used in the FAA community. Therefore, the SOW should indicate that the definitions in this handbook (or other FAA documents) supersede those in MIL-STD-882, see Glossary for examples.

### **5.3.5 Hazard Analyses**

The SSPP describes the specific analyses to be performed during the SSP. The following characteristics of those analyses should be included.

The analysis techniques and formats to be used in the qualitative or quantitative analysis to identify risks, their hazards and effects, hazard elimination, or risk reduction requirements, and how these requirements are met.

The depth within the system to which each technique is used, including risk identification associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments.

The integration of subcontractor hazard analyses with overall system hazard analyses.

Analysis is the method of identifying hazards. A sound analytical and documentation approach is required if the end product is to be useful. An inappropriate analytical approach can be identified in the contractor's discussion within the SSPP.

Each program is required to assess the risk of accident in the design concept as it relates to injury to personnel, damage to equipment, or any other forms of harm. The result of this assessment is a definition of those factors and conditions that present unacceptable accident/accident risk throughout the program. This definition provides a program baseline for formulation of design criteria and assessment of the adequacy of its application through systems analysis, design reviews, and operational analysis. System

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

safety analyses are accomplished by various methods. As noted in Chapters 8&9 of this handbook, the basic safety philosophy and design goals must be established prior to initiation of any program analysis task. Without this advanced planning, the SSP becomes a random identification of hazards resulting in operational warnings and cautions instead of design correction (i.e., temporary, not permanent solutions)

The SSPP, therefore, describes the methods to be used to perform system safety analyses. The methods may be quantitative or qualitative, inductive or deductive, but must produce results consistent with mission goals.

It is important that the SSP describes procedures that will initiate design change or safety trade studies when safety analyses indicate such action is necessary. Specific criteria or safety philosophy guides trade studies or design changes. Whenever a management decision is necessary, an assessment of the risk is presented so that all facts can be considered for a proposed decision. It is common to find budget considerations driving the design without proper risk assessment. Without safety representation, design decisions may be made primarily to reduce short-term costs increasing the accident risk. Such a decision ignores the economics of an accident. In many cases accident and accident costs far exceed the short-term savings achieved through this process.

The contractor's system safety engineers should be involved in all trade-studies. The SSPP must identify the responsible activity charged with generating CRAs, and with reviewing and approving the results of trade-studies to assure that the intent of the original design criteria is met.

The hazard analysis section of the SSPP should describe in detail, the activities which will identify the impact of changes and modifications to the accident potential of delivered and other existing systems. All changes or modifications to existing systems must be analyzed for impact in the safety risk baseline established by the basic system safety analysis effort. In many cases, this analysis can be very limited where in others a substantial effort is appropriate. The results must be included for review as a part of each engineering change proposal.

### **5.3.6 Safety Data**

The SSPP should illustrate the basic data flow path used by the contractor. This information shows where the system safety activity includes reviewing internally generated data and where it has approval authority. The safety data paragraph should list system safety tasks, contract data requirements list (CDRL) having safety significance but no specific safety reference, 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 review on request.

### **5.3.7 Safety Verification**

Safety verification must be demonstrated by implementing a dedicated safety verification test and/or assessment program. The following information should be included in the SSPP.

- The verification (e.g., test, analysis, inspection) requirements for ensuring that safety is adequately demonstrated. Identify any certification requirements for safety devices (e.g., fire extinguisher, circuit breakers) or other special safety features (e.g., interlocks). Note that

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

some certification requirements will be identified as the design develops so the SSPP should contain procedures for identifying and documenting these requirements.

- Procedures for making sure test information is transmitted to the MA for review and analysis.
- Procedures for ensuring the safe conduct of all tests.

The FAA System Engineering Manual may be consulted for further information on verification and validation.

### **5.3.8 Audit Program**

The contractor's SSPP should describe the techniques and procedures to be used in ensuring the accomplishment of the internal and subcontractor SSPs. Specific elements of an audit program by the prime contractor should include the following:

- On-site inspection of subcontractors.
- Major vendors, when appropriate.
- An accurate staff-hour accounting system.
- Hazard traceability.

### **5.3.9 Training**

This portion of the SSPP contains the contractor's plan for using the results of SSP in various training areas. Often hazards that relate to training are identified in the Safety Engineering Report (SER) or in the System Engineering Design Analysis Report. Procedures should provide for transmitting this information to any activity preparing training plans. The specifics involved in safety training may be found in Chapter 14.

The SSP will produce results that should be applied in training operator, maintenance, and test personnel. This training should not only be continuous but also conducted both formally and informally as the program progresses. The SSPP should also address training devices.

### **5.3.10 Accident/Incident Reporting**

The contractor should be required to notify the MA immediately in case of an accident. The SSPP must include details and timing of the notification process.

The SSPP should also define the time and circumstances under which the MA assumes primary responsibility for accident and incident investigation. The support provided by the contractor to government investigators should be addressed. The procedures by which the MA will be notified of the results of contractor accident investigations should be spelled out. Provisions should be made for a government observer to be present for contractor investigations.

Any incident that could have affected the system should be evaluated from a system safety point of view. An incident in this case is any unplanned occurrence that could have resulted in an accident. Incidents involve the actions associated with hazards, both unsafe acts or unsafe conditions that could have resulted in harm. Participants within the system safety program should be trained in the identification of

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

incidents; this involves a concept called behavioral-based safety, which is discussed in Chapter 12, Facilities System Safety.

### **5.3.11 Interfaces**

Since conducting an SSP will eventually affect almost every other element of a system development program, a concerted effort must be made to effectively integrate support activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing.

To ensure that the SSP is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall SSP. This part of the SSPP must show the contractor's procedures for accomplishing this task. The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the SSP. Occasionally, the MA procures subsystems or components under separate contracts to be integrated into the overall system. Subcontracted subsystems that impact safety should be required to implement an SSP.

The integration of these programs into the overall SSP is usually the responsibility of the prime contractor for the overall system. When the prime contractor is to be responsible for this integration, the Request for Proposal (RFP) must specifically state the requirement. This subparagraph of the SSPP should indicate how the prime contractor plans to effect this integration and what procedures will be followed in the event of a conflict.

The MA system safety manager should be aware that the prime contractor is not always responsible for the integration of the SSP. For example, in some SSPs, the MA is the SSP integrator for several associate contractors. The next section of this chapter contains guidance specific to the management of a complex program with multiple subcontractors requiring an Integrated System Safety Program Plan.

## **5.4 Integrated System Safety Program Plan**

The tasks and activities of system safety management and engineering are defined in the System Safety Program Plan, (SSPP). An Integrated System Safety Program Plan (ISSPP) is modeled on the elements of an SSPP, which is defined in Mil-Std 882C.<sup>1</sup> An ISSPP is required when there are large projects or large systems; the system safety activities should be logically integrated. Other participants, tasks, operations, or sub-systems within a complex project should also be incorporated.

The first step is to develop a plan that is specifically designed to suit the particular project, process, operation, or system. An ISSPP should be developed for each unique complex entity such as a particular line-of-business, project, system, development, research task, or test. Consider a complex entity that is comprised of many parts, tasks, subsystems, operations, or functions and all of these sub-parts should be combined logically. This is the process of integration. All the major elements of the ISSPP should be integrated. How this is accomplished is explained in the following paragraphs.

### **5.4.1 Integrated Plan**

The Program Manager, Prime Contractor, or Integrator develops the Integrated System Safety Program Plan. The Plan includes appropriate integrated system safety tasks and activities to be conducted within

---

<sup>1</sup> Military Standard 882C, explains and defines System Safety Program Requirements, Military Standard 882D is a current update as of 1999. This version no longer provides the details that version C had provided.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

the project. It includes integrated efforts of management, team members, subcontractors and all other participants.

#### **5.4.2 Integrated Program Scope and Objectives**

The extent of the project, program, and system safety efforts is defined under scope. The system safety efforts should be in-line with the project or program. Boundaries are defined as to what may be excluded or included within the ISSPP.

The objective is to establish a management integrator to assure that coordination occurs between the many entities that are involved in system safety. The tasks and activities associated with integration management are defined in the document. The ISSPP becomes a model for all other programs within the effort. Other participants, partners, sub-contractors are to submit plans which are to be approved and accepted by the integrator. The Plans then become part of the ISSPP.

#### **5.4.3 Integrated System Safety Organization**

The integrated system safety organization is detailed within the plan. The duties and responsibilities are defined for the System Safety Integration Manager and staff. Each sub-entity such as a partner, or sub-contractor, should appoint a manager or senior system safety engineer or lead safety engineer that will manage the entity's SSPP. All appropriate system safety participants are to be given specific responsibilities. The participants should have specific qualifications in system safety, which include a combination of experience and education.

#### **5.4.4 Integrated System Safety Working Group**

A System Safety Working Group (SSWG) is formed to help manage and conduct tasks associated with the program. The group specifically provides a consensus entity that enhances work performed. The SSWG is a major part of the SSPP.

For large or complex efforts where an ISSPP has been established, activities of the Integrated System Safety Working Group (ISSWG) are defined in the ISSPP. The ISSWG includes responsive personnel who are involved in the system safety process. The plan specifically indicates that, for example, Operations, System Engineering, Test Engineering, Software Engineering, and System Safety Engineering personnel are active participants in the ISSWG. The integrator may act as the chair of the ISSWG with key system safety participants from each sub-entity. The group may meet formally on a particular schedule. Activities are documented in meeting minutes. Participants are assigned actions.

The ISSWG activities may include:

- Monitoring interface activities to assure that system safety is adequately integrated.
- Reviewing or conducting activities, analysis, assessments, and studies, appropriate to system safety.
- Conducting hazard tracking and risk resolution activities.
- Conducting formal safety reviews.

#### **5.4.5 Integrated Program Milestones**

The Integrated System Safety Process Schedule is defined within the ISSPP. The schedule indicates specific events and activities along with program milestones. To accomplish the integration specific

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

system analysis techniques have evolved. One example is the use of Program Evaluation Review Technique (PERT).<sup>2</sup> It is essentially the presentation of system safety tasks, events and activities on a network in sequential and dependency format showing independencies, and task duration and completion time estimates. Critical paths are easily identifiable. Its advantage is the greater control provided over complex development and production programs as well as the capacity for distilling large amounts of scheduling data in brief, orderly fashion. Management decisions are implemented. Needed actions may be more clearly seen, such as steps to conduct a specific test.

A similar or sub-technique of PERT is known as Critical Path Method (CPM).<sup>3</sup> It also involves the identification of all needed steps from a decision to a desired conclusion --depicted systematically --to determine the most time-consuming path through a network. This is designated on the diagram as the "critical path". The steps along the path are "critical activities".

Because of the dynamics and the variability of safety management efforts, the networks developed should suit the complexity required. For large programs a master PERT network can be developed with lower level PERT charts referenced to provide needed detail. The use of CPM, in conjunction with PERT, can explore possible variables that influence programs.<sup>4</sup> Further detail on PERT and CPM can be acquired from the references.

#### **5.4.6 Integrated System Safety Requirements**

The integrated engineering requirements for system safety are described within the ISSPP. As the design and analysis matures specific system safety standards and system specifications are to be developed and the ISSPP is to be updated. Initially, generic requirements are defined for the design, implementation, and application of system safety within the specific project, or process. The Integrator defines the requirements needed to accomplish the objectives of the ISSPP. Here one specifies the system safety products to be produced, the risk assessment code matrix, risk acceptability criteria, and residual risk acceptance procedures. This effort should also include guidelines for establishing project phases, review points, and levels of review and approval.<sup>5</sup>

#### **5.4.7 Integrated Risk/Hazard Tracking and Risk Resolution**

Integrated Risk/Hazard Tracking and Risk Resolution is described within the ISSPP. This is a procedure to document and track contributory system risks and their associated controls by providing an audit trail of risk resolution. The controls are to be formally verified and validated and the associated contributory

---

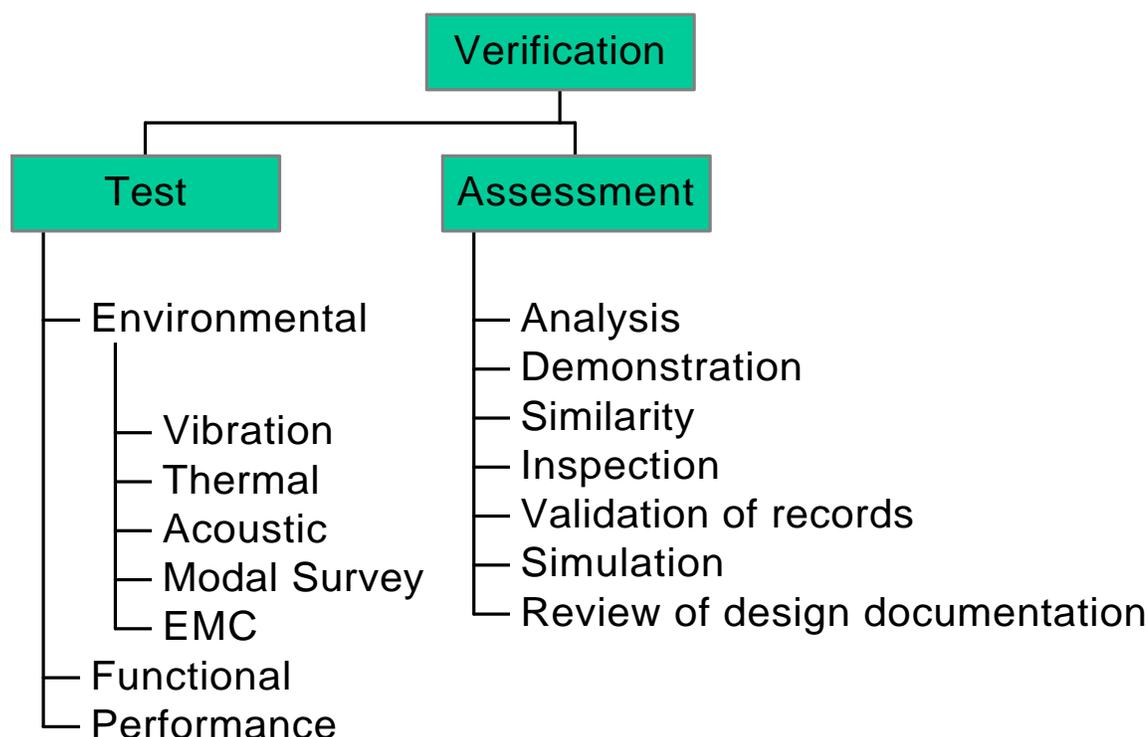
<sup>2</sup> J.V. Grimaldi and R.H. Simonds, Safety Management, Richard D. Irwin, Inc. Homewood, Illinois, Third Edition, 1975.

<sup>3</sup> IBID, Grimaldi

<sup>4</sup> System Safety Society, System Safety Analysis Handbook, 2<sup>nd</sup> Edition, 1997.

<sup>5</sup> J. Stephenson, System Safety 2000, A Practical Guide for Planning, Managing, and Conducting System Safety Programs, Van Nostrand Reinhold, New York, 1991.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000



**Figure 5-4: Safety Verification Methods**

hazard is to be closed. This activity is conducted and/or reviewed during ISSWG meetings or formal safety reviews.

Integrated Risk/Hazard Tracking and Risk Resolution is accomplished by the use of the Safety Action Record (SAR). The SAR document captures the appropriate elements of hazard analysis, risk assessment and related studies, conducted in support of system safety. See Chapter 2 for a discussion of the Hazard Tracking/Risk Resolution process ( Paragraph 2.2.1.5)

#### **5.4.8 Integrated Safety Verification and Validation**

Specific verification techniques are discussed within the ISSPP. Safety verification is needed to assure that system safety is adequately demonstrated and that all identified system risks that have not been eliminated are controlled. Risk controls (mitigation) must be formally verified as being implemented. Safety verification is accomplished by the methods shown in Figure 5-4.

It should be noted that no single method of verification indicated above provides total system safety assurance. Safety verification is conducted in support of the closed-loop hazard tracking and risk resolution process.

Hazard Control Analysis considers the possibility of insufficient control of the system. Controls are to be evaluated for effectiveness. They are to enhance the design. Keep in mind that system safety efforts are

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

not to cause harm to the system. Consider that any change to a system must be evaluated from a system risk viewpoint. For more information regarding verification and validation see the FAA System Engineering Manual.

#### **5.4.9 Integrated Audit Program**

The ISSPP should call for the Quality Assurance function to audit the program. All activities in support of system safety are to be audited. This includes contractor internal efforts and all external activities in support of closed-loop Hazard Tracking and Risk Resolution. The government will be given access to audit data.

#### **5.4.10 Integrated Training**

When required, ISSPP participants are to receive specific training in system safety in order to conduct analysis, hazard tracking and risk resolution. Additional training is to be provided for ISSWG members and program auditors to assure awareness of the system safety concepts discussed herein.

Specific training is to be conducted for system users, controllers, systems engineers, and technicians. Training considers normal operations with standard operating procedures, maintenance with appropriate precautions, test and simulation training, and contingency response. Specific hazard control procedures will be recommended as a result of analysis efforts. See Chapter 14 for more information on System Safety training.

#### **5.4.11 Integrated Incident Reporting and Investigation**

Any incident, accident, malfunction, or failure effecting system safety is to be investigated to determine causes and to enhance analysis efforts. As a result of investigation, causes are to be determined and eliminated. Testing and certification activities are also to be monitored; anomalies, malfunctions, failures that affect system safety are to be corrected.

Concepts of system safety integration are also applied systematically through formal accident investigation techniques. Many systematic techniques have been successfully applied for example<sup>6</sup>: Scenario Analysis (SA), Sequentially Timed Events Plot (STEP), Root Cause Analysis (RCA), Energy Trace Barrier Analysis (ETBA), Management Oversight and Risk Tree (MORT), and Project Evaluation Tree (PET).<sup>7</sup> For further details consult the references provided. Consider that hazard analysis is the inverse of accident investigation and similar techniques are applied in the application of inductive and deductive processes of hazard analysis and accident investigation.

#### **5.4.12 System Safety Interfaces**

System Safety interfaces with other applicable disciplines both internally to systems engineering and externally. System Safety is involved in all Program disciplines, i.e., Risk Management, Facilities, Software Development, Certification, Testing, Contract Administration, Health Management, Environmental Management, Ergonomics, Human Factors, as examples. These disciplines may be directly involved in the hazard analysis, hazard control, hazard tracking, and risk resolution activities.

---

<sup>6</sup> IBID, System safety Society

<sup>7</sup> IBID, Stephenson

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

### **5.4.13 Integrated Inputs to the ISSPP**

The external inputs to the system safety process are the design concepts of the system, formal documents, engineering notebooks, and design discussions during formal meetings and informal communications. The on-going output of the system safety process is hazard analysis, risk assessment, risk mitigation, risk management, and optimized safety.

Inputs:

- Concept of Operations
- Requirements Document
- System/Subsystem Specification
- Management and System Engineering Plans, (e.g. Master Test Plan)
- Design details

Outputs: Hazard Analysis consists of

- Identifying safety related risks (contributory hazards) throughout system life cycle
- Conducting system hazard analysis evaluating human, hardware, software, and environmental exposures
- Identifying and incorporating hazard (risk) controls
- Risk Assessment involves:
  - Defining risk criteria i.e., severity and likelihood
  - Conducting risk assessment i.e., Risk Acceptability and Ranking
- Risk Management consists of:
  - Conducting Hazard Tracking and Risk Resolution
  - Optimize safety (assure acceptable safety related risks)
  - Monitoring controls

## **5.5 Program Balance**

The purpose of an SSP is to eliminate or reduce risk of an accident to an acceptable level within the available program assets. The system safety activity, like all other systems engineering functions, is sized through a trade-off between cost, schedule, and performance. The sizing of an SSP must find a balance between acceptable risk and affordable cost. Neither a system with unacceptable accident risk nor one that cannot be procured because of the costs of achieving unreasonable safety goals is acceptable.

## **5.6 Program Interfaces**

Both the nature of safety objectives and economics require the use of information available through other engineering disciplines. The capability of the safety engineering staff can be greatly increased through integration with other engineering disciplines. System Safety integration and risk assessment have been discussed in earlier sections of this Chapter. For a summary of other organizations that need to be involved in system safety, see Table 5-4.

Design engineers are key players in the system safety effort. Together with systems engineers, they translate user requirements into system design and are required to optimize many conflicting constraints. In doing this, they eliminate or mitigate known hazards but may create unidentified new hazards. System safety provides design engineers with safety requirements, validation and verification requirements, and

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

advice and knowledge based on the SSP's interfacing with the many participants in the design and acquisition processes.

On a typical program, safety engineers interface with a number of other disciplines as reflected in Table 5-3. In most cases, the frequency of interfacing with these other disciplines is less than that with the design engineers. Nevertheless, the exchange of data between safety engineering and the program functions is both important and in some cases mutually beneficial.

Reliability engineers, for example, perform analyses usable by and often without additional cost to safety engineering. These analyses do not supplant safety-directed analyses. They provide data that improve the quality and efficiency of the safety analysis process. Three types of reliability analyses are reliability models, failure rate predictions, and Failure Modes and Effects Criticality Analysis (FMECA).

The safety/maintainability engineering interface is an example of providing mutual benefits. The system safety program analyzes critical maintenance tasks and procedures. Hazards are identified, evaluated, and appropriate controls employed to minimize risk. Maintainability analyses, on the other hand, provide inputs to the hazard analyses, particularly the Operational and Support Hazard Analyses (O&SHA).

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

**Table 5-3: Other Engineering Organizations Involved in Safety Programs**

ORGANIZATION	NORMAL FUNCTIONS	SAFETY FUNCTIONS
Design Engineering	Design equipment and system to meet contractual specifications for mission	Analyses safest designs and procedures. Ensures that safety requirements in end product item specifications and codes are met. Incorporates safety requirements for subcontractors and vendors in specifications and drawings.
Human (Factors) Engineering	Ensures optimal integration of human, machine, and environment.	Analyses human machine interface for operation, maintenance, repair, testing, and other proposed tasks to minimize human error, provide safe operating conditions, and to prevent fatigue. Makes procedural analysis.
Reliability Engineering	Ensures equipment will operate successfully for specific periods under stipulated conditions.	Performs failure modes and effects criticality analysis (FMECA) and failure rate predictions quantifying probability of failure. Performs tests, as necessary, to supplement analytical data. Reviews trouble and failure reports for safety connotations.
Maintainability Engineering	Ensures hardware status and availability.	Ensures that operating status can be determined, minimizes wearout failures through preventative maintenance, and provides safe maintenance access and procedures. Participates in analyzing proposed maintenance procedures and equipment for safety aspects.
Test Engineering	Conducts laboratory and field tests of parts, subassemblies, equipment, and systems to determine whether their performance meets contractual requirements.	Evaluates hardware and procedures to determine whether they are safe in operation, whether additional safeguards are necessary. Determines whether equipment has any dangerous characteristics or has dangerous energy levels or failure modes. Evaluates effects of adverse environments on safety.
Product (Field) Support	Maintains liaison between customer and producing company.	Assists customer on safety problems encountered in the field. Constitutes the major channel for feedback of field information on performance, hazards, accidents, and near misses.
Production Engineering	Determines most economical and best means of producing the product in accordance with approved designs.	Ensures that designed safety is not degraded by poor workmanship and unauthorized production process changes.
Industrial Safety	Ensures that company personnel are not injured nor company property damaged by accidents.	Provides advice/information on accident prevention for industrial processes and procedures.
Training	Improves technical and managerial capabilities of company and user personnel.	Ensures that personnel involved in system development, production, and operation are trained to the levels necessary for safe accomplishment of their tasks.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

Close cooperation between system safety and quality assurance (QA) benefits both functions in several ways. QA should incorporate, in its policies and procedures, methods to identify and control critical items throughout the life cycle of a system. The safety function flags safety-critical items and procedures. QA then can track safety-critical items through manufacturing, acceptance tests, transportation, and maintenance. New or inadequately controlled hazards can then be called to the attention of the safety engineer.

Human engineering (HE) and safety engineering are often concerned with similar issues and related methodologies, (See Chapter 17, Human Factors Safety Principles). HE analyzes identified physiological and psychological capabilities and limitations of all human interfaces. A variety of human factors inputs affect the way safety-critical items and tasks impact the production, employment, and maintenance of a system. Environmental factors that affect the human-machine interface are also investigated and safety issues identified.

The safety/testing interface is often underestimated. Testing can be physically dangerous. The safety and test engineers must work together to minimize safety risk. Testing is a vital part of the verification process and must be included in a comprehensive SSP. It verifies the accomplishment of safety requirements. Testing may involve:

- Components
- Mock-ups
- Simulations in a laboratory environment
- Development and operation test and evaluation efforts.

System safety may require special tests of safety requirements or analyze results from other tests for safety verification.

The requirements for interface between safety and product support are similar to those involving safety and manufacturing. Each examines personnel and manpower factors of design. System safety ensures that these areas address concerns related to identified hazards and the procedures. Operational, maintenance, and training hazard implication are passed on to the user as a result of the design and procedural process.

## **5.7 Tailoring**

An effective SSP is tailored to the particular product acquisition. The FAA's policy is to tailor each SSP to be compatible with SSMP, the criticality of the system, the size of the acquisition, and the program phase of that system's life cycle. The resultant safety program becomes a contractual requirement placed upon system contractors and subcontractors.

Readily adaptable to the FAA's mission, MIL-STD-882D was created to provide a standardized means for establishing or continuing SSPs of varying sizes at each phase of system development. The SSMP along with Mil-Std-882 contains a list of tasks from which the FAA program manager may tailor an effective SSP to meet a specific set of requirements. Each task purpose is stated at the beginning of each task description. Fully understanding these purposes is critical before attempting to tailor an SSP. There are three general categories of programs: Low Risk, Moderate Risk, and High Risk.

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

Selecting the appropriate category is difficult and in practice depends on some factors difficult to quantify, particularly in the early phases of a program. Therefore, this decision should be reviewed at each phase of the program, permitting the best information available to direct the magnitude of the safety program. The following steps applied to the risk methodology in Chapter 3 illustrate the technique used for the program risk decision process.

- Generate a CRA (and PHA if needed) in the IA phase. These analyses will provide the types and risks of hazards. The development of an airframe and that of a ground communications system could both produce a system that can lead to death, a Severity 1 or 2 hazard. A development program that is far more complex and includes more Severity 1 or 2 hazards, with a higher probability of occurrence than another, is clearly a high risk program, the other a low risk one. The PHL includes information from sources such as safety, analytical, and historical experience from similar systems and missions. The PHL process should be updated and continued in the investment analysis phase.
- Begin the Preliminary Hazard Analysis (PHA) as soon as possible. The PHA focuses on the details of the system design. In addition to the historical experiences used for the PHL, information about technologies, materials, and architectural features such as redundancy are available as sources to the PHA. Systems using new and immature technologies or designs are more risky than those that use proven technologies or modifications of existing designs.
- Use a detailed hazard analysis to provide new and more precise information about safety risk for the program production and deployment phases. This step will minimize the risk of accidents during the test and evaluation process.

A major challenge that confronts government and industry organizations responsible for an SSP is the selection of those tasks that can materially aid in attaining program safety requirements. Scheduling and funding constraints mandate a cost-effective selection, one that is based on identified program needs. The considerations presented herein are intended to provide guidance and rationale for this selection. They are also intended to provoke questions and encourage problem solving by engineers, operations, and support personnel.

After selection, the tasks must be identified and tailored to match the system and program specifications. It is important to coordinate task requirements with other engineering support groups (e.g., reliability, logistics) to eliminate duplication of tasks and to become aware of additional information of value to system safety. The timing and depth required for each task, as well as action to be taken based on task outcome, are program requirements. For these reasons, precise rules are not stated.

Some contractual activities provide cost savings, flexibility, and pre-award planning without affecting compliance or control. These are:

- Coordinate the delivery schedule of safety analysis deliverables with program milestones such as a major design review rather than days after contract award. This prevents the need for contractual changes to adjust for schedule changes. The deliverables should be provided approximately 30 days prior to the milestones, thereby providing current information and the ability of the reviewer to prepare for the design review. The deliverable can be established as a major program milestone; however, this carries the risk of halting an entire program for a single deliverable.
- Consider requiring updates to the first deliverable rather than autonomous independent deliverables at major milestones. For example, if the first system hazard analysis is

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

- scheduled for delivery at the Systems Design Review (SDR), the submittal required at the Preliminary Design Review (PDR) might be limited to substitute and supplementary pages. This requires planning such as configuration control requirements (e.g., page numbering and dating schemes).
- If major design decisions that significantly affect the cost of safety analyses are expected during the contract, fix the size of the effort in a manner that maintains FAA control. An example would be a flight control methodology decision such as would be applied to fly-by-wire, glass cockpit, or mechanical systems. The number of fault trees required in a safety analysis depends on the system selected. A good contractual approach would be to fix the number of fault trees to be provided during negotiations. The contract would reflect that both the FAA and the contractor must agree on which fault trees are to be performed. Thus the task can be tailored to the design well downstream from contract award without affecting performance or cost.
  - Maintain a reasonable balance between the analyses and deliverables specified. When the program manager determines that limiting the deliverables is economically necessary, the contractor must maintain a detailed controlled and legible project log that is available for MA review and audit. A compromise approach would be to permit deliverables in contractor format eliminating formatting costs. Requiring FAA approval of alternating deliverables may also be considered. In this situation, program control is maintained at the program major milestones. The MA has the option of reviewing the status of all safety tasks and analyses at these points in the program. The MA has approval authority at each formal design review. This control is more significant than that of a single deliverable.

### 5.7.1 Small Programs

Tailoring of safety program requirements is important for small programs, because the cost of an SSP can easily match or exceed the cost of the program itself. The program manager must carefully consider both the cost of an item and its criticality in establishing the SSP requirements for such items. The actual benefit may not justify the actual cost of safety. However, sometimes the perceived risk is so high that increased cost is justified. In most situations, such as for the development of a router bridge, a modem, or a fiber optic communications local area network (LAN), SSP costs can be limited without measurably increasing the risk of accident.

The tasks below are recommended as a minimum effort for a small SSP.

- Prepare a preliminary hazards list (PHL)
- Conduct a preliminary hazard analysis (PHA)
- Assign a Risk Assessment code (see Chapter 3).
- Assign a priority for taking the recommended action to eliminate or control the hazard, according to the risk assessment codes.
- Evaluate the possibility of negative effects from the interfaces between the recommended actions and other portions of the system.
- Take the recommended actions to modify the system.
- Prepare a SER or Design Analysis Report (DAR)<sup>8</sup> as completion to the SSP.

---

<sup>8</sup> FAA System Engineering Manual

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

There are hazard review checklists available for hazard risk identification. These checklists can be found in System Safety literature and within safety standards and requirements. (See bibliography)

The PHA is developed as an output of the preliminary hazard list. It is the expansion of this list to include risks, hazards, along with potential effects and controls.

An in-depth hazard analysis generally follows the PHA with a subsystem hazard analysis (SSHA), a system hazard analysis (SHA), and an operating and support hazard analysis (O&SHA) as appropriate. For most small programs, a PHA will suffice when appropriate. The PHA then should include all identified risks, hazards, and controls that are associated with the lifecycle of the system.

A comprehensive evaluation is needed of the risks being assumed prior to test or evaluation of the system or at contract completion. The evaluation identifies the following:

- All safety features of the hardware, software, human and system design
- Procedural risks that may be present
- Specific procedural controls and precautions that should be followed

The risks encountered in a small program can be as severe and likely to occur as those in a major program. Caution needs to be exerted to ensure that in tailoring the system safety effort to fit a small program, one does not over-reduce the scope, but instead uses the tailoring process to optimize the SSP for the specific system being acquired, or evaluated.

### **5.7.2 Government-Furnished Equipment**

As part of a system acquisition effort, the FAA may provide equipment necessary for the system development. The interface between the GFE and the new system must be examined if not previously examined. This type of analysis, once considered a separate MIL-STD-882 task, is now considered as part of the overall system analyses. The contractor is responsible for the overall system's safety but not for the inherent risk of the GFE itself. For such situations, the following contractual requirements are suggested:

- If hazard data are available, identify the system safety analyses needed and date they are required.
- Identify and perform any additional system safety analyses needed for interfaces between GFE and the other systems.
- Ideally, the GFE has sufficient history available to the FAA that unsatisfactory operating characteristics are well known or have been identified in previous hazard analyses. The MA should identify these unsatisfactory characteristics or provide the analyses, if available, to the contractor. The contractor will then compensate for these characteristics in the interface design. In some cases, such characteristics may not be known or analyses and/or history is not available. Then either the contractor or the MA must perform the analyses necessary for interface design.

### **5.7.3 Commercial Off The Shelf/Non-developmental Items (COTS/NDI)**

COTS/NDI are commercially developed hardware or software that are currently being marketed publicly. A computer modem, LAN card (or system), radio, and desktop computers are some examples. Procurement of these items saves development costs but is difficult for the system safety activity to

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

assess, and even more difficult to influence. Simple items, such as the examples above, are usually developed without an SSP. The amount of safety attention required should vary depending on the criticality of the application and the available characterization history. Ideally, experience with the device or more likely a similar model is available to provide the MA with guidance on the safety attention required.

More complex and critical items require a MA decision process to ensure that the risk of accident is acceptable. Commercial subsystem development for items such as a radio or system development for aircraft are likely to include some form of failure-related analysis such as a FMECA or fault tree analysis. A review of this contractor-formatted analysis may provide the necessary assurance. A poorly or non-documented analysis provides the opposite effect.

The COTS/NDI concept provides significant up-front cost and schedule benefits but raises safety and supportability issues. For the NAS to benefit fully from COTS/NDI acquisitions, the SSP must be able to ensure the operational safety of the final system without unnecessarily adding significantly to its acquisition cost. The retrofitting of extensive safety analyses or system modifications may negate any advantage of choosing COTS/NDI

For COTS/NDI acquisitions, a safety assessment for the intended use should be performed and documented before purchase. Such analyses should contribute to source and/or product selection. This should be contained in the buyer's SSPP. COTS/NDI will be evaluated for operational use by considering all aspects of the item's suitability for the intended purpose. Suitability criteria should include technical performance, safety, reliability, maintainability, inter-operability, logistics support, expected operational and maintenance environment, survivability, and intended life cycle. To assure risk acceptability, appropriate hazard analysis must be conducted to evaluate the risks associated with initial field testing of COTS/NDI.

Many developers of COTS/NDI may not have SSPs or staff to assess the suitability of COTS/NDI proposed for NAS applications. Therefore, the MA must do the following.

- Establish minimum analysis requirements for each procurement. These vary due to the nature of the item being procured and the criticality of its mission. Examples include mission and usage analysis and specific hazard analyses to determine the potential system impact on the remainder of the system or the NAS itself.
- Include in each procurement document the system safety analyses required for accurate and standardized bidding
- Restrict the application of the procured COTS/NDI to the missions analyzed, or reinitiate the analysis process for new missions.
- Apply skillful, creative tailoring when limiting the SSP scope to accommodate program size and procurement schedules.
- Marketing investigation, hazard analysis, and System Safety Working Groups are additional considerations and are explained below.

#### **5.7.4 Marketing Investigation**

The MA could conduct a market investigation to identify the safety or other appropriate standards used to design the system. The MA must determine the extent to which the system was certified or otherwise

FAA System Safety Handbook, Chapter 5: Post-Investment Decision Safety Activities  
December 30, 2000

evaluated by government and non-government agencies such as the FAA, Department of Defense (DOD), and Underwriter Labs. It must then determine what this information provides when compared to mission requirements. The following basic questions form the basis of a COTS/NDI procurement checklist, such as:

- Has the system been designed and built to meet applicable or any safety standards? Which ones?
- Have any hazard analyses been performed? Request copies of the analyses and the reviewing agency comments.
- What is the accident and accident history for the system? Request specifics.
- Are protective equipment and/or procedures needed during operation, maintenance, storage, or transport? Request specifics.
- Does the system contain or use any hazardous materials, have potentially hazardous emissions, or generate hazardous waste?
- Are special licenses or certificates required to own, store, or use the system?

### ***Hazard Analysis***

A safety engineering report may be all that is necessary or available to gather detailed hazard information concerning a COTS/NDI program. If the selected program must be modified to meet mission requirements, other hazard analyses may be required, especially if the modifications are not otherwise covered.

### ***System Safety Working Groups.***

Requiring an SSWG meeting early in the program will help clarify system safety characteristics versus mission requirements and allow time to address issues. A follow-up SSWG meeting can be used to ensure satisfactory closure of issues. Periodic SSWG meetings throughout the life cycle of the system can be used to address ongoing concerns and special issues. See Chapter 6.4.2 for more information.

## **Chapter 6:**

# **System Safety Guidelines for Contracting**

<b>6.1 CONTRACTING PRINCIPLES.....</b>	<b>2</b>
<b>6.2 CONTRACTING PROCESS .....</b>	<b>2</b>
<b>6.3 EVALUATING BIDDING CONTRACTORS (SYSTEM SAFETY CHECKLIST).....</b>	<b>9</b>
<b>6.4 MANAGING CONTRACTOR SYSTEM SAFETY (CONTRACT OVERSIGHT).....</b>	<b>24</b>

## 6.0 System Safety Guidelines for Contracting

### 6.1 Contracting Principles

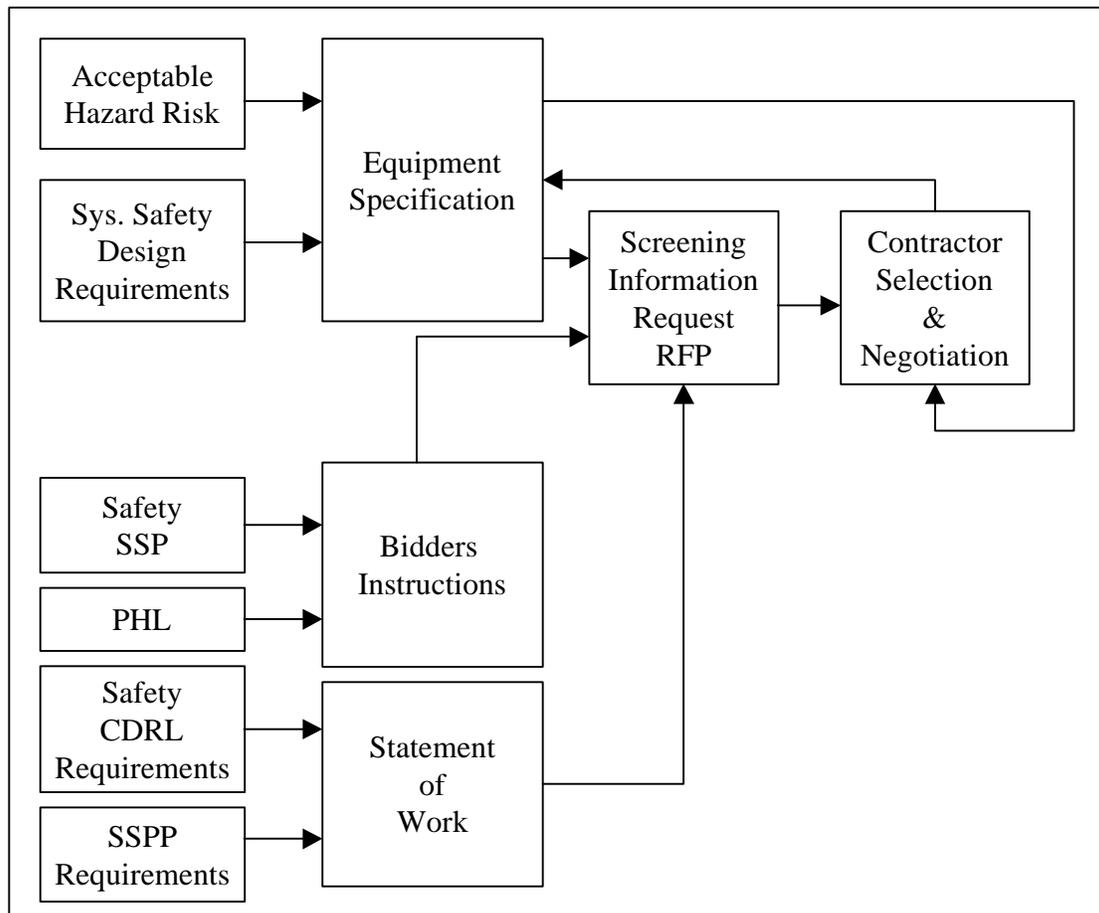
Contracting provides the legal interface between the FAA, as a buying agency, and a selling organization, usually a contractor. The contract document binds both parties to a set of provisions and requirements. This means that if desired safety criteria, analyses, or tests are not specified in the contract, the contractor is not obligated to provide them. In other words, the contractor is not required to comply with post contract requirements. It is the IPT leader's responsibility to define these requirements early enough in the acquisition cycle to include them in the negotiated contract.

### 6.2 Contracting Process

The AMS provides a definitive contracting process, or series of activities, which must be accomplished in order to effect an acquisition. These activities are broken into five (5) major lifecycle components: Mission Analysis, Investment Analysis, Solution Implementation, In-Service Management and Service Life Extension. These components are described in Chapter 4. This chapter focuses on the basic acquisition steps of solution implementation. They may be summarized as follows:

- Acquisition planning,
- Documentation of detail requirements
- Communicating requirements to industry, and
- Evaluation of the resulting proposals or bids,
- Negotiation and/or selection of the source to perform the contract, and
- Management of the awarded contract to assure delivery of the supplies or services required.

The execution of these steps should be tailored for each acquisition. Figure 6-1 illustrates a sample acquisition from planning through contract negotiation. The following paragraphs describe the activities within the contracting process.



**Figure 6-1 Example of the Contracting Process**

### 6.2.1 Acquisition Planning

To insure inclusion of the desired safety criteria and system safety program (SSP) in the contract, a great deal of planning is required before proposals and costs are solicited from potential contractors. This results in technical and administrative requirements.

For the former, qualified technical personnel must either select and/or tailor an existing specification for the items required or create a new one if an appropriate one does not exist. The specification must reflect two types of safety data:

- Performance parameters (e.g., acceptable risk levels, specific safety criteria such as electrical interlocks)
- Test & Evaluation Requirements (e.g., specific safety tests to be performed and/or specific program tests to be monitored for safety).

Traditionally, administrative requirements have been specified in the request for proposal. MIL-STD-882D has taken a position that given the technical requirements, defining the administrative requirements can be left to the bidding contractor to define as part of the bidding process. The proposal evaluation team will judge the adequacy of the proposed safety program. Inadequate proposed safety programs can either be judged not-responsive or amended during negotiation.

The following administrative requirements must be defined and included in the negotiated contract and/or Statement of Work (SOW):

- Delivery Schedule (e.g., Schedule of safety reviews, analyses, and deliverables. It is suggested that delivery be tied to specific program milestones rather than calendar dates e.g., 45 days before Critical Design Review).
- Data Requirements (e.g. Number of safety analysis reports to be prepared, required format, content, approval requirements, distribution.)

Another valuable element of acquisition planning is estimating contractor costs of safety program elements to assist in:

- Determining how much safety effort is affordable; and is it enough?
- Optimize the return on safety engineering investment.
- Perform a sanity check of contractor's bids.

### **6.2.2 Development and Distribution of a Solicitation**

To transmit the requirements to potential bidders, an Invitation for Bids, (if the Sealed Bidding method is used), or a Screening Information Request (SIR) Request for Proposals (RFP), if a competitive proposals process is used. These documents contain the specification (or other description of the requirement), data requirements, criteria for award, and other applicable information. For some programs with complex safety interfaces (e.g. multiple subcontractors), or high safety risk the IPT may require the submission of a draft System Safety Program Plan (SSPP) or Integrated System Safety Program Plan (ISSPP) with the contractor's proposal. The purpose is to provide evidence to the FAA that the contractor understands the complexity of the safety requirement and demonstrates the planning capability to control such risks. In those cases, where the responsibility for defining the SSP's administrative elements has been assigned to the contractors, the inclusion of a draft SSPP or ISSPP with the proposal is essential.

Each solicitation contains at least three sections that impact the final negotiated SSP:

- Equipment Specification
- Statement of Work (SOW)
- Instructions for preparation of proposals/bids and evaluation criteria. (Sections L and M respectively)

### **6.2.3 Equipment Specification**

Specifications are the instructions dictating to the designer the way the system will perform. A system specification is prepared for all equipment procured by FAA. The system specification and more detailed requirements that flow down to lower level specifications define design requirements. The careful selective

use of FAA and Military Standards can simplify the specification of design criteria. For example, FAA-G-2100F provides physical safety design criteria. MIL-STD-1522 contains specific instruction for pressure vessels, placement of relief valves, gauges, and high-pressure flex hose containment. MIL-STD-454, Requirement 1 specifies design controls for electrical hazards and MIL-STD-1472 for ergonomic issues. Whether these specifications are contractor prepared or supplied by the managing activity, it is important that proper instructions are given directly to the designer who controls the final safety configuration of the system.

MIL-STD-490 gives a format for preparing universally standard types of specifications. Appendix I of MIL-STD-490 identifies the title and contents of each paragraph of the system specification. Other appendices describe other types of specifications, such as prime item development, product, and so on. Several paragraphs in each specification are safety related. These include:

**Health and Safety Criteria.** This paragraph concerns the health of operations personnel. It should include firm requirements for radiation levels (such as X-rays from high-power amplifiers and antenna radiation patterns), toxic gases, and high noise environments. Each system has its unique operating environment. In so far as possible, associated health problems must be anticipated and a firm requirement for solving those problems should be included in this section. Those problems missed may be identified by the contractor's SSP. The advantage of identifying actual or anticipated health problems in this section of the system specification is that their solution will be included in the contract price and be a design requirement.

**Safety Requirements.** This paragraph should contain general system-level safety requirements. Some examples of these requirements can be found in requirement 1 of MIL-STD-454 and paragraph 5.13 of MIL-STD-1472. Citing an entire document or design handbook and expecting the contractor to comply with every thing therein is unrealistic. Where practical, assigned acceptable probability numbers for Category I and II hazards, should be included in this paragraph.

**Functional Area Characteristics.** This paragraph has subparagraphs that address more specific lower-level safety requirements, such as safety equipment. Paragraph 3.7 of MIL-STD-490 defines specifications and identifies all emergency-use hardware, such as fire extinguishers, smoke detection systems, and overheat sensors for the system operating environment.

**Quality Conformance Inspections.** This paragraph requires the contractor to verify by inspection, analysis, or actual test, each requirement in section 3 of the system specification including systems safety. Paragraph 4.2, often requires verification of corrective actions taken to manage the risk of all Category I and II hazards. The corrective measures would be verified by inspection, analysis, or demonstration.

#### **6.2.4 Statement of Work (SOW)**

The SOW, usually Section C of the RFP, defines the work anticipated to be necessary to complete the contract. This is the only means the procuring activity has available to communicate the scope of the system safety task. There are two viable approaches to preparing a SOW for a bid package. The first is to specify adherence to Section 4 of MIL-STD-882D which provides the minimum components of a SSP but not specific analyses or deliverables. The second includes these details in the SOW as part of the procurement package. The first approach increases the complexity of the source selection and negotiation processes, but may reduce acquisition costs. The latter is more traditional but is in conflict with current trends of increasing flexibility. In either case, the negotiated SOW must be explicit. The following discussion is applicable to an explicit SOW whether it be submitted with RFP package or negotiated.

The SOW task descriptions can consist of a detailed statement of the task or contain only references to paragraphs in other documents such as MIL-STD-882 or this handbook. Elaborate task descriptions are not required. A simple statement, however, in the body of the SOW such as, "The contractor shall conduct a System Safety Program to identify and control accident risk" does not define the safety requirements adequately. A contractor might argue that it is only required to caution it's design team to look out for and minimize hazards.

#### **System Safety Section**

This section of the SOW must contain enough detail to tell the contractor exactly what kind of SSP is required. Some SSP issues that could be detailed in the SOW follow:

- The requirement for planning and implementing an SSP tailored to the requirements of MIL-STD-882.
- Defining relationships among the prime contractor and associate contractors, integrating contractors, and subcontractors i.e. "Who's the Boss?".
- The requirement for contractor support of safety meetings such as System Safety Working Groups (SSWG). If extensive travel is anticipated, either the FAA should estimate the number of trips and locations or structure the contract to have this element on a cost reimbursable basis.
- Definition of number and schedule of safety reviews, with a statement of what should be covered at the reviews. Safety reviews are best scheduled for major design reviews, such as the system design review, preliminary design review, and critical design review.
- Requirement for contractor participation in special certification activities, such as for aircraft. The FAA may anticipate that support from a communications supplier may be necessary for the aircraft certification process.
- Procedures for reporting hazards. The CDRL will specify the format and delivery schedule of hazard reports. Note that permitting contractor format can save documentation costs but, in the case where there are multiple contractors may make integration difficult.

- Definition of required analyses to be performed, such as the preliminary hazards list, preliminary hazard analysis, and system hazard analysis. The contract data requirements list specifies the format and delivery schedule of required analyses.
- The specification of required safety testing, i.e., special test of specific components or subsystems or monitoring specific other tests.
- Basic risk management criteria. Specify a set of conditions that state when the risk of the hazard is acceptable and that require the contractor to specify alternate methods for satisfying the acceptable risk requirement. (See Chapter 3 for examples of criteria for severity, likelihood, and risk acceptability.)
- Special safety training or certification that might be needed for safe operation of critical systems.
- Reviews of engineering change proposals and deviations and waivers to make sure design changes do not degrade the safety level of the system.
- Techniques for doing analyses, such as the fault hazard analysis and fault tree analysis. If included, specify on which system and subsystems the contractor should do these analyses. Specify the candidate top events for fault tree analyses, such as flight control or power systems. (See Chapters 8 & 9 for a discussion of analysis techniques and analytical tools.)

### 6.2.5 Contract Data Requirements List

A Contract Data Requirements List (CDRL) is usually appended to the SOW. Contractual data to be delivered falls into two general categories:

- Financial, administrative, or management data. The procuring activity requires these data to monitor contractor activities and to control the direction contractor activities are taking. Contractors that require the use of the Cost Schedule Control System (CS)<sup>2</sup> or equivalent permit the FAA to monitor expended safety engineering effort and progress on a monthly basis. This type of system makes it clear whether or not a contractor is only applying safety resources to major program milestones.
- Technical data required to define, design, produce, support, test, deploy, operate, and maintain the delivered product.

Preparing data submissions can be expensive and represent a major portion of the contractor's safety resources. The system safety data requirements listed on the CDRL, therefore, should represent only the absolute minimum required to manage or support the safety review and approval process. Two choices are to be made and reflected in the CDRL: 1) Should the contractor prepare the data in a format specified by a data item description (DID) or in contractor format. 2) Which submittals require approval for acceptance and payment.

The contractor does not get paid for data not covered by the CDRL/DID. He is not obligated to deliver anything not required by a CDRL. It is advantageous to effectively utilize the DIDs when available. When specifying DIDs they should be examined carefully, sentence by sentence, to assure applicability. It is

suggested that the data review and approval cycle be 30-45 days. Longer review cycles force the contractor, in many cases, to revise an analysis of an obsolete configuration.

### 6.2.6 Bidders' Instructions

The bidder's instructions reflect how the proposal will be evaluated. There are a few instructions that, when included in the instructions for the management and technical sections of the proposal, simplify evaluation. The bidders' response should be keyed to specific Specification and SOW requirements and evaluated by means of a RFP required compliance matrix (reference Figure 6-2). Proposed costs should be supplied against the Work Breakdown Structure (WBS) permitting visibility of the SSP costs. For large programs, the costs should be separable by major SSP tasks.

<b><u>RFP</u></b>	<b><u>PROPOSAL</u></b>
<b>Specification</b> <b>3.6.3 Acceptable Hazard Level</b> <b>Electrical Design Criteria</b>	<b>Tech. Vol. 8.3</b> <b>Tech. Vol. 4.7, 8.3, 12.0</b>
<b>SOW</b> <b>6.3 SSP Tasks</b> <b>CDRLs</b>	<b>Tec. Vol. 8.3, Appendix B</b> <b>Appendix B</b>
<b>Instructions to Bidder</b> <b>13a Draft SSPP</b> <b>13.b Draft PHL</b>	<b>Appendix B</b> <b>Tech. Vol. 8.3, Mgmt. Vol. 2.0</b>

**Figure 6-2: Sample Compliance Matrix**

The details of the proposed SSP are important to the safety program evaluator, either as a separable document or section of the proposal. Requiring a draft plan as part of the proposal package is an excellent communication tool but it must be remembered that such a requirement increases the contractor's cost of bidding for a contract. For large programs, this cost may be incidental, for others it may significant. When the requirement for a SSPP is included in the RFP, the following type of statement tailored to specific program needs could be contained in the management section of the bidders' instructions:

The offeror shall submit an initial SSPP in accordance with DI-SAFT-80100 as modified by CDRLXXX. This plan shall detail the offeror's approach to paragraph 10 of DID DI-SAFT-80100 (as modified). This preliminary plan shall be submitted as a separate annex to the proposal and will not be included in overall proposal page limitations.

NOTE: This approach takes advantage of standardized DIDs and does not mean to imply that page limitations on system safety plans are inappropriate. A well-prepared plan can cover the subject in less than 50 pages.

To encourage attention on system safety in the technical proposal, the bidders instructions should include wording such as: "The offeror shall submit a summary of system safety considerations involved in initial trade studies." In later development phases, it may be advantageous to require the offeror to "submit a preliminary assessment of accident risk." The validation phase may require the bidder to describe system safety design approaches that are planned for particularly high-risk areas (i.e., separated routing of

hydraulic lines, or separate room installation of redundant standby generators.) During this program phase, the following statement could be included:

The offeror shall submit a description of the planned system safety design and operational approach for identification and control of safety-critical, high-risk system design characteristics.

As previously noted, the RFP can request submission of draft data items, such as the SSPP or Preliminary Hazard List (PHL), before contract award. Alternatively, the bidders can be instructed to discuss their proposed SSP in detail, including typical hazards and design solutions for them or candidate hazards for analysis. Careful wording can provide almost the same results as a draft data item. Key areas of interest, such as personnel qualifications or analysis capabilities, can be cited from data items as guides for the bidders' discussions. For example, "discuss your proposed SSP in detail using data item DI-SAFT-80100, paragraphs 10.2 and 10.3, as a guide." Using DI-SAFT-80100 as a guide, sample criteria could include the following:

- Describe in detail the system safety organization, showing organizational and functional relationships and lines of communication
- Describe in detail the analysis technique and format to be used to identify and resolve hazards
- Justify in detail any deviations from the RFP.

Proposals are evaluated against the award criteria included in the RFP. If safety is not listed in the award criteria, the bidder's responses to safety requirements have little impact on the award decision. Negotiations take place with each contractor still in contention after initial review. The IPT members review in detail all segments of each contractor's proposal and score the acceptability of each element in the evaluation criteria. Extensive cost and price analysis of the contractors' proposals must be accomplished so that a determination that the final price is "fair and reasonable" to the government and to the contractor. The relative proposed cost of the SSP reflects on the seriousness that each contractor places on System Safety. It is not, in itself the ultimate indicator, as some contractors may "work smarter" than others.

### **6.3 Evaluating Bidding Contractors (System Safety Checklist)**

There are three components of the evaluation process:

- Proposal Evaluation
- Contractor Evaluation
- Negotiation

#### **6.3.1 Proposal Evaluation**

This section provides an extensive list of SSP criteria that can either be used to structure a SSP requirement for a solicitation or used to evaluate a contractor's response to a Request for Proposal (RFP). Caution should be taken not to penalize a contractor for not responding to a requirement found below that is not explicitly or reasonably implicitly included in the specified requirements.

The data that follows is divided into eight groups and provided in a checklist format. The contents are comprehensive and should be tailored for each application. A contractor's response to an RFP that addresses all issues listed below is likely to be large for most proposals. Additionally, adherence to the complete list is not appropriate for many acquisitions. Formal questions to the bidders or discussions during negotiations can resolve reasonable omissions.

### ***System Safety Program Plan (SSPP)***

A SSPP should provide the following information:

- Details of the system safety manager to program manager relationship and accountability.
- Identification of the organization(s) directly responsible for accomplishing each subtask and company policies, procedures, and/or controls governing the conduct of each subtask.
- A description of methods to be used in implementation of each SSPP task including a breakout of task implementation responsibilities by organizational component discipline, functional area, or any planned subcontractor activity.
- A composite listing of applicable company policies, procedures, and controls, by title, number, and release date.
- A chart showing the contractor's program organization identifying the organizational element assigned responsibility and authority for implementing the SSP.
- Identification of the interfaces of the system safety organization and other organizations, including cross-references to applicable sections of other program plans.
- A clearly detailed method by which problems encountered in the implementation of the SSP and requirements can be brought to the attention of the contractor program manager.
- Procedures to be used to assure resolution of identified unacceptable risks.
- The internal controls for the proper and timely identification and implementation of safety requirements affecting system design, operational resources, and personnel.
- A schedule of the system safety activities and a milestone chart showing relationships of the system safety activities with other program tasks and events. Tasks and data inputs and outputs which correspond to the program milestones should be identified. Milestones are controlled by program master schedule and internal operations directives.
- Staffing levels required for successful completion of contractually required tasks.
- A description of the contractor's program and functional system safety organization.

See Chapter 5 for a more detailed discussion of SSPP contents and the SSPP template. The ISSPP should be considered a special case of the SSPP that involves multiple major subcontractors that must be integrated by the Prime Contractor/Integration Contractor.

### ***Contractor's System Safety Program Management***

An SSPP is only as good as the contractor's management commitment to systems safety. The FAA should not dictate prospective (or contracted) contractor's organizational structures. An assessment can be made of such organizations to determine if the contractor can meet the Government's objectives. Criteria include:

- A centralized accident risk management authority, as delegated from the contractor program manager. It must maintain a continuous overview of the technical and planning aspects of the total program.
- An experienced system safety manager directly accountable to the program manager for the conduct and effectiveness of all contracted safety effort for the entire program.
- A single point of contact for the FAA interface with all contractor internal program elements, and other program associate or subcontractors for safety-related matters. The contractor system safety manager maintains liaison with Government sources to obtain:
  - Safety data as a design aid to prevent repetitive design or procedural deficiencies.
  - Information on operational systems which are similar to the system under this contract and should be studied for past safety problems and their solutions.
  - Authority for access of personnel to nonproprietary information on accident and failure causes and preventive measures in possession of government agencies and contractors involved with those systems.
- Approval authority for critical program documentation and all items related to safety contained in the contract data requirements list (CDRL).
- Internal approval authority and technical coordination on waiver/deviations to the contractually imposed system safety requirements, as defined.
- Internal audits of safety program activities, as defined, and support FAA audits, when requested.
- Participation in program level status meetings where safety should be a topic of discussion. Provide the contractor program manager the status of the SSP and open action items.

### ***Contractor's SSP***

Requirements and guidance for a contractor's SPP are specified in the Statement of Work (SOW) and the Data Item Description (DID). Good SSP's have the following characteristics which should be reflected in either the SSPP or internal documented practices:

- Review of and provide inputs to all plans and contractual documents related to safety.
- Maintenance of safety-related data, generated on the program by the safety staff.

- Maintenance of a log, available for FAA review, of all program documentation reviewed and records all concurrence, non-concurrence, reasons for non-concurrence, and actions taken to resolve any non-concurrence.
- Coordination of safety-related matters with contractor program management and all program elements and disciplines.
- Coordination of system safety, industrial safety, and product safety activities on the program to ensure protection of the system during manufacture and assembly.
- Establishment of internal reporting systems and procedures for investigation and disposition of accidents and safety incidents, including potentially hazardous conditions not yet involved in an accident/incident; such matters are reported to the purchasing office as required by the contract.
- Performance of specified Hazard Analyses.
- Participation in all requirements reviews, preliminary design reviews, critical design reviews, and scheduled safety reviews to assure that:
  - All contractually imposed system safety requirements are met.
  - Safety program schedule and CDRL data deliverable content are compatible.
  - Hazard analysis method formats, from all safety program participants, permit integration in a cost effective manner.
  - Technical data are provided to support the preparation of required analyses.
- Participates in all test, flight, or operational readiness reviews and arranges for presentation of required safety data.
- Provision for technical support to program engineering activities on a daily basis. Such technical support includes consultation on safety-related problems, research on new product development, and research and/or interpretation of safety requirements, specifications, and standards.
- Planned participation in configuration control board activities, as necessary, to enable review and concurrence with safety-significant system configuration and changes.
- Review of all trade studies. Identification of those that involve or affect safety. Participation in all safety related trade studies to assure that system safety trade criteria are developed and the final decision is made with proper consideration of accident risk.
- Provisions for system safety engineering personnel participation in all trade studies identified as being safety-related. Ensure that safety impact items and accident risk assessments are given appropriate weight as decision drivers.
- Provides trade study documentation that shows the accident risk for the recommended solution is equal to or less than the other alternative being traded, or provide sufficient justification for recommending another alternative.

- Identification of any deficiencies regarding safety analysis or risk assessment, when they are not provided with government-furnished equipment and property.
- Identification of deficiencies where adequate data to complete contracted safety tasks is not provided.
- Acknowledgement of specified deliverable safety data format, as cited on the CDRL. Where no format is indicated, the contractor may use any format that presents the information in a comprehensible manner.
- Provision for safety certification of safety-critical program documentation and all safety data items contained in the CDRL.
- Recognition that the SSP encompasses operational site activities. These activities include all operations listed in operational time lines, including system installation, checkout, modification, and operation.
- Acknowledgment that SSP consideration must be given to operations and interfaces, with ground support equipment, and to the needs of the operators relating to personnel subsystems, such as panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.
- Incorporation of facility safety design criteria in the facility specifications.
- Evaluation of the safety impact of system design changes. Revisions or updates subsystem hazard analyses and operating and support hazard analyses to reflect system design changes during the life of the program.
- Attention given to planning, design, and refurbishment of reusable support equipment, including equipment carried on flight vehicles, to assure that safety is not degraded by continued usage.
- Planned review of engineering change proposals (ECP) to evaluate and assess the impact on safety design baseline. This safety assessment must be a part of the ECP and include the results of all hazard analyses done for the ECP.
- Planned system safety training for specific types and levels of personnel (i.e., managers, engineers, and technicians involved in the design, product assurance operations, production, and field support). Safety inputs to training programs are tailored to the personnel categories involved and included in lesson plans and examinations.
- Contractor safety training may also include government personnel who will be involved in contractor activities.
- Safety training includes such subjects as hazard types, recognition, causes, effects, and preventive and control measures; procedures, checklists, and human error; safeguards, safety devices, and protective equipment, monitoring and warning devices, and contingency procedures.
- Provision for engineering and technical support for accident investigations when deemed necessary by the management activity. This support includes providing contractor technical personnel to the accident investigation board.

### ***Integrated System Safety Program Plan***

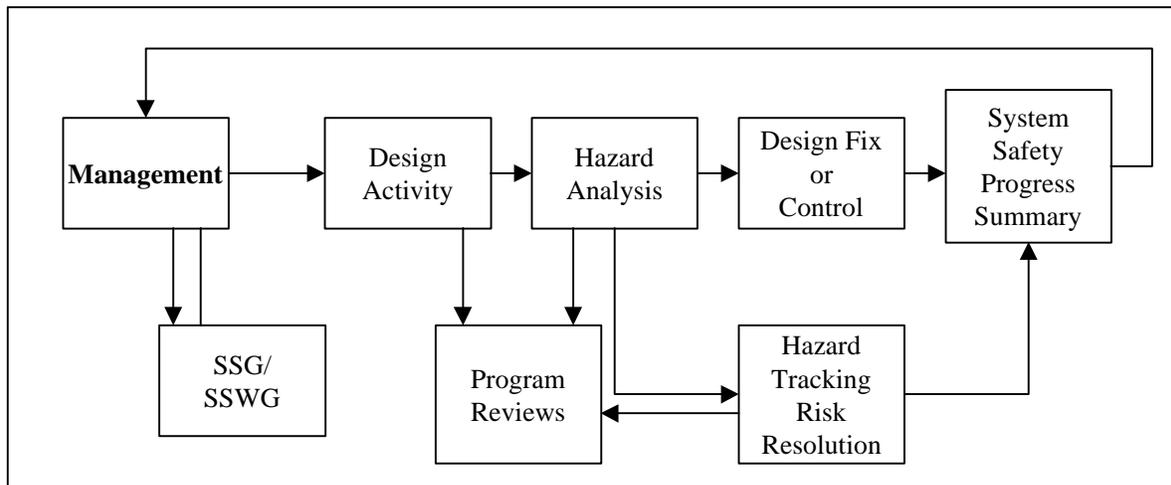
Complex programs with many contractors often require a systems integration contractor. The systems safety staff of the systems integrator contractor is required, in-turn, to generate an Integrated System Safety Plan (ISSP), which establishes the authority of the integrator and defines the effort required from each associate contractor for integration of system safety requirements for the total system. The system safety integrator initiates action to ensure that each associate contractor is contractually required to be responsive to the SSP. If the associate contractors are not system integrator subcontractors, the integrator contractor should propose contractual modifications when required for the successful performance of the ISSP. Associate contractor system safety plans can be incorporated as appendices to the ISSP.

### ***Detailed Contractor Integration Activities***

Generation of the System Safety Program Plan (SSPP) is the first management task of a System Safety Program (SSP) following contract award as discussed in Chapter 4. These are primarily management tasks and are applicable to many SSPs. When selected, they should be included in the requirements of the Request for Proposal (RFP) or contract Statement of Work (SOW). The SSPP must include planning for these activities when they are contractually specified. These management tasks activities, are:

- Contractor Integration
- System Safety Program Reviews/Audits
- System Safety Working Group/System Safety Working Group Support
- Hazard Tracking/Risk Resolution
- System Safety Progress Report

Figure 6.3 illustrates the improved communications.



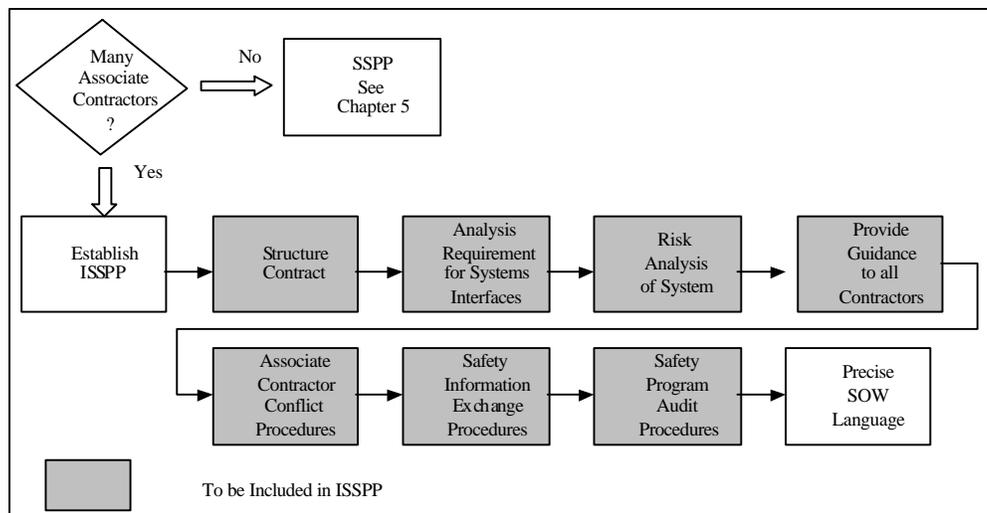
**Figure 6-3: Improved Communication Paths**

### ***Contractor Integration***

Major program projects often require multiple associate contractors, subcontractors, integration contractors, and architect and engineering (AE) firms. On these programs, the integrating contractor often has the responsibility to oversee system safety efforts of associate contractors or AE firms.

A program with many associate contractors or subcontractors requires an ISSPP that provides, major emphasis on the integration process, flowdown of system safety requirements and responsibilities, and monitoring of subcontractor performance. This SSPP is called an Integrated System Safety Program Plan (ISSPP), which generally follows the requirements of MIL-STD-882. Figure 6-4 illustrates the ISSPP additional tasks.

The systems integrator or construction contractor has the visibility and, therefore, must have the responsibility of performing the system hazard analyses and assessments that cover the interfaces between the various contractors' portions of the system or construction effort. When an integration contractor does not exist, and the managing authority procures the subsystems directly, this responsibility is given to the managing authority. In situations where an integration contractor exists, the managing authority must clearly and contractually define the role and responsibilities of the integration contractor for the associate contractors. Management is responsible for assisting the integrator in these efforts to ensure that all contractors and firms mutually understand the system safety requirements and their respective responsibilities in order to comply with them.



**Figure 6-4 ISSPP Additional Tasks**

The following is a list of tasks from which the managing authority may choose the systems integration contractor's responsibilities. Those selected should be included in the RFP and SOW.

1. Prepare ISSPP following the requirements. The ISSPP will define the role of the systems integration contractor and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition, the plan may address and identify:

- (a) Definitions of where the control, authority, and responsibility transitions from the integrating contractor to the subcontractors and associate contractors

- (b) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method utilized
  - (c) Data each associate contractor is required to submit to the integrator and scheduled delivery keyed to program milestones
  - (d) Schedule and other information considered pertinent by the integrator
  - (e) The method of development of system-level requirements to be allocated to each associate contractor as a part of the system specification, end-item specifications, and other interface documents
  - (f) Safety-related data pertaining to off-the-shelf items
  - (g) Integrated safety analyses to be conducted and support required from associate contractors and subcontractors
  - (h) Integrating contractor's roles in the test range or other certification processes
  - (i) SSP milestones
2. Initiate action through the managing authority to ensure each associate contractor is required to be responsive to the ISSPP. Recommend to the management contractual modification where the need exists.
  3. Examine the integrated system design, operations, and specifically the interfaces between the products of each associate contractor during risk assessment. This requires using interface data that can often only be provided by an associate contractor.
  4. Summarize the mishap risk presented by the operation of the integrated system during safety assessments.
  5. Provide assistance and guidance to associate contractors regarding safety matters.
  6. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to systems and item specifications. When the integrator cannot resolve problems, notify the managing authority for resolution and approval.
  7. Initiate action through the managing authority to ensure information required by an associate contractor from the integrating contractor (or other associate contractors) to accomplish safety tasks is provided in an agreed-to format. Establish associated logs to prevent such requests from "becoming lost."
  8. Develop a method of exchanging safety information between contractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort. Provide for informal one-on-one telephone contact. Consider establishing system safety databases at the systems integration contractor with telephone access and/or the distribution of monthly safety reports featuring contributions from each contractor. These may be extracted from monthly progress reports, if the progress report requirements are specified accordingly.
  9. Implement an audit program to ensure that the objectives and requirements of the SSP are being accomplished. Notify in writing, any associate contractor of its failure to meet contract program or technical system safety requirements for which it is responsible. The integrator for the safety effort will send a copy of the notification letter to the managing authority, whenever such written notification is given. Establish a deficiency log to track the status of any such issues

Details to be specified in the SOW shall include, as applicable:

- Imposition of MIL-STD-882D
- Imposition of this System Safety Handbook
- Designation of the system safety integrating contractor
- Designation of the status of the other contractors
- Requirements for any special integration safety analyses
- Requirements to support test, environmental, and/or other certification processes.

### ***Test and Evaluation (T&E) Guidelines***

Consideration of the safety aspects testing is important as they present the earliest opportunity in a program for accidents to occur and for risk mitigations to be demonstrated. The T&E and operations safety interfaces encompass all development, qualification, acceptance, and pre-operational tests and activities. The following guidelines should be considered, as appropriate, for inclusion in the RFP, contractual requirements, and/or the SSPP:

- Test procedures must include inputs from the safety analyses and identify test and operations and support requirements.
- Verification of system design, and operational planning compliance with test or operating site safety requirements, is documented in the final analysis summary.
- Establishment of internal procedures for identification and timely action or elimination/control of potentially hazardous test conditions induced by design deficiencies, unsafe acts, or procedural errors. Procedures should be established to identify, review, and supervise potentially hazardous, high-risk tests, including those tests performed specifically to obtain safety data.
- Contractor system safety organization review and approval of test plans, procedures, and safety surveillance, procedures, and changes to verify incorporation of safety requirements identified by the system analysis. The contractor system safety organization assures that an assessment of accident risk is included in all pretest readiness reviews.
- Safety requirements for support equipment are identified in the system safety analyses.
- Support equipment safety design criteria are incorporated in the segment specifications.
- Test, operations, and field support personnel are certified as having completed a training course in safety principles and methods.
- Safety requirements for ground handling have been developed and included in the transportation and handling plans and procedures. Safety requirements for operations and servicing are included in the operational procedures. The procedures are upgraded and refined, as required, to correct deficiencies that damage equipment or injure personnel.

### **Safety Audits**

System safety audits should be conducted by the system safety manager and, on a periodic basis, by a contractor management team independent of the program. The list of issues to be included in the audit program may be selected from the following list:

- The status of each safety task
- Interrelationship between safety and other program disciplines
- Identification and implementation of safety requirements criteria
- Documented evidence which reflects planned versus actual safety accomplishment.
- Program milestones and safety program milestones
- Schedule incompatibilities that require remedial corrective action
- Contractor initiates positive corrective actions where deficiencies are revealed by the audits.
- Verification or corrective action on problems revealed by previous audits.
- Subcontractor audits to ensure that:
  - ◆ They are designing and producing items whose design or quality will not degrade safety
  - ◆ Safety analyses are conducted as required
  - ◆ System safety problems are being brought to the attention of their own program managers and prime contractor management.

### **How to Use The Checklist**

The checklist above can be used for evaluating a bidders response and/or a SSPP submitted to the for approval. The process to use the checklist for evaluation is as follows:

- For each program, group the items in the checklist into four categories:
  - Those explicitly required by the SOW and/or contract
  - Those that, in the view of the reviewer, are desirable or necessary to perform in meeting the explicitly stated requirements
  - Those that are not applicable to the program for which the evaluation is being performed
  - Those that, in the opinion of the evaluator, were not included in the RFP, SOW, or contract.
- For purposes of evaluation, the latter two categories must handled delicately. If an important omission was made by a bidder(s) and not explicitly included in the RFP, all bidders must be given an equal opportunity to bid the missing SSP elements.
- Ultimately, the first two categories are used for evaluation. Clearly, the decision process must utilize the explicitly stated or negotiated requirements. The applicable elements in the checklist can be graded requirement by requirement either as simply compliant or non-compliant or by assigning "grades" to the response of each requirement. Grade responses numerically reflect the degree of compliance as:

0	Unacceptable (does not meet minimum requirements)
1	Marginal (success doubtful)
2	Acceptable (probable success)
3	Excellent (success likely)
4	Superior (success very likely)
5	Outstanding (high probability of success)

A variation of grading management responses might be:

0	No management planning, personnel not qualified, no authority, resources minimal
1	Planning barely adequate, little management involvement, resources inadequate
2	Planning adequate, implementation weak, management modestly concerned, resources ineffectively utilized
3	Planning generally good, implementation good, management involved, resources adequate and used effectively, program well received in most program areas
4	Strong planning, implementation, management involvement; good use of resources, program well received in all affected areas
5	Strong, excellently implemented program in all areas
6	Outstanding innovative program. Industry leader.

The final step is to add (or average) the scores for each bidder to determine acceptability or the best. For close decisions, the process can be repeated for the implicit requirements as described in group 2 above.

### 6.3.2 Contractor Evaluation

A good proposal must be backed up with a competent and dedicated staff. A number of programs have stumbled because the winning organization either did not have the necessary staff or management processes to execute the proposed program.

#### ***Contractor System Safety Components***

One way of assessing both contractor system safety capability and intent is to break down the system safety "big picture" into important organizational activities and examine the documentation used or generated by each. The following describes six such components, the associated SSP responsibilities, and benefits.

- **Corporate or Division.** Many companies establish safety policies at the Corporate and Division levels. These safety policies or standards are imposed on all company development and/or production activities. The presence of such standards, accompanied by audit procedures can provide the evaluation team with an indication of company commitment, standardized safety approaches, and safety culture.
- **Procurement Activity.** Contractors write specifications and SOWs for subcontractors and vendors. An internal procedure or actual examples of previous subcontracts should demonstrate an intelligent process or requirements "flow down". It is not sufficient to impose system safety requirements on a prime contractor and monitor that contractor's SSP if that contractor uses major system components developed without benefit of a SSP.
- **Management of Program's SSP.** The contractor's SSPP describes in detail planned management controls. The plan should reflect a combination of contractual direction, company policies, and "hands-on" experience in developing, managing, and controlling the SSP and its resources. The contractor's SSP manager's credentials must include knowing not only company policies, procedures, and practices but also the technical requirements, necessary activities and tools, and the characteristics of the operational environments.
- **Contractor's Engineering SSP.** The system safety engineer should possess in-depth knowledge of engineering concepts including hazard risk assessment and control, the system, and associated accident risk to implement the SSP. The engineer develops design checklists, defines specific requirements, performs hazard analyses, operates or monitors hazard tracking systems, and in conjunction with the design team implements corrective action. Qualifications of system safety personnel are discussed in Chapter 4.
- **Specifications and Requirements.** The potential exists for engineers and designers, possessing minimal safety knowledge, to be charged with incorporating safety criteria, specifications, and requirements into the system or product design. It is essential that this activity be monitored by system safety engineering to verify that these requirements and criteria are incorporated in the design. It is important that someone with system safety competence "flow down" the safety requirements throughout the "specification tree". It is the lower level specifications (C typically) that are the detailed design criteria which get translated into the design. If safety requirements are not properly incorporated at this level they will be missed in the design process.
- **Operational or Test Location.** The contractor must demonstrate in his SSPP, Test Plans, and Logistics documentation that the SSP does not end at the factory door. The contractor must consider safety during test programs and planned support for government or system integrator activities.

### ***Management and Planning of an SSP***

Four primary drivers of an effective SSP are:

- Personnel qualifications and experience
- Managerial authority and control
- Effective program planning
- Sufficient resources.

If one of these is missing or insufficient, the program will fail.

**Personnel Qualifications and Experience.** To provide decision makers with competent hazard risk assessments, the FAA's program/assistant manager must insist that the contractor have qualified, responsive system safety management and technical personnel. This is necessary since the contractor's system safety manager is the one who certifies, for his employer, that all safety requirements have been met. Necessary qualifications vary from program to program as discussed in Chapter 5, Table 5-2

FAA sponsored programs are either the procurement of hardware/systems or services. In the former, the role of the evaluator is often to determine if bidding contractors have the capability (and track history) to meet contractual requirements. In the latter case of acquisition of services, the evaluation may be more focused on the qualification of individuals. In either case, the evaluator is usually provided resumes for proposed individuals, in others more generic "job descriptions" that establish minimum qualifications for well defined "charters".

A useful approach to evaluating either proposed key positions resumes or job descriptions is to utilize a "Job Analysis Worksheet". A sample is included as Figure 6-5. It is appropriate to require key resumes (and an obligation to use the associated individuals post award) in the Request for Proposal's (RFP) instructions to bidders. A Job Analysis Worksheet is a checklist of desired job requirements per required skill level reflecting the knowledge, skills, and abilities (KSA) necessary to implement the program successfully. The submitted key resumes or alternatively position descriptions is reviewed against the job requirements as reflected in each KSA to determine if the candidate meets the FAA's requirements. A sample position description is provided as Exhibit 6-4.

**Figure 6-5 Sample Job Analysis Worksheet: System Safety Manager**

Knowledge, Skills, and Abilities (KSA)

- 1 Knowledge and ability to manage interrelationships of all components of an SSP in support of both management and engineering activities. This includes planning, implementation, and authorization of monetary and personnel resources.
- 2 Knowledge of theoretical and practical engineering principles and techniques.
- 3 Knowledge of systems
- 4 Knowledge of operational and maintenance environments.
- 5 Knowledge of management concepts and techniques.
- 6 Knowledge of this life-cycle acquisition process.
- 7 Ability to apply fundamentals of diversified engineering disciplines to achieve system safety engineering objectives.
- 8 .Ability to adapt and apply system safety analytical methods and techniques to related scientific disciplines.
- 9 Ability to do independent research on complex systems to apply safety criteria.
- 10 Skill in the organization, analysis, interpretation, and evaluation of scientific/engineering data in the recognition and solution of safety-related engineering problems.
- 11 Skill in written and oral communication.
- 12 Ability to keep abreast of changes in scientific knowledge and engineering technology and apply new information to the solution of engineering problems.

Major Job Requirements

- 1 Acts as agent of the program manager for all system safety aspects of the program. Provides monthly briefings to the program management on the status of the SSP.
- 2 Serves as system safety manager for safety engineering functions of major programs. (KSA 1 through 11)
- 3 Manages activities which review and evaluate information related to types and location of hazards. (KSA 1,2,3,4,7,9,12)
- 4 Manages activities to perform extensive engineering studies to determine hazard levels and to propose solutions. (KSA 1,2,6,7,8,9,11)
- 5 Manages the development of system guidelines and techniques for new/developing systems and emerging technologies. (KSA 6,7,8,9,10,12)
- 6 Provides system safety engineering expertise to identify/solve multidisciplinary problems involving state-of-the-art technology. (KSA 2,7,8,9,10,12)

**TITLE: ENGINEER, STAFF - SYSTEM SAFETY**Qualifications

Minimum of a baccalaureate degree in an engineering, applied science, safety or other closely related degree appropriate to system safety. Some education or experience in Business Administration is desirable; Certification as a Professional Engineer or as a Certified Safety Professional (CSP) licensed as a PE, preferably in safety engineering, or credentials as a CSP in system safety aspects. Approximately 10 years diversified experience in various aspects of system safety is desired; or demonstrated capability through previous experience and education to perform successfully the duties and responsibilities shown below.

Duties and Responsibilities

Serve as a professional authority for the SSP covering the planning, designing, producing, testing, operating, and maintaining of product systems and associated support equipment. May be assigned to small programs as system safety representative with duties as described below.

Review initial product system designs and advise design personnel concerning incorporation of safety requirements into product system, support equipment, test and operational facilities based on safety standards, prior experience, and data associated with preliminary testing of these items.

Assure a cooperative working relationship and exchange of operational and design safety data with government regulatory bodies, customers, and other companies engaged in the development and manufacture of aerospace systems. Act as a company representative for various customer and industry operational and design safety activities and assist in the planning and conducting of safety conferences.

Evaluate new or modified product systems, to formulate training programs, for updating operating crews and indoctrinating new employees in systems test and operational procedures. Establish training programs reflecting latest safety concepts, techniques, and procedures.

Direct investigations of accidents involving design, test, operation, and maintenance of product systems and associated facilities, and present detailed analysis to concerned customer and company personnel. Collect, analyze, and interpret data on malfunctions and safety personnel, at all organizational levels; and keep informed of latest developments, resulting from investigation findings, affecting design specifications or test and operational techniques. Collaborate with functional safety organizations in order to set and maintain safety standards. Recommend changes to design, operating procedures, test and operational facilities and other affected areas; or other remedial action based on accident investigation findings or statistical analysis to ensure maximum compliance with appropriate safety standards.

Coordinate with line departments to obtain technical and personnel resources required to implement and maintain safety program requirements.

**Figure 6-6 Sample Job Description**

### 6.3.3 Negotiation

Negotiation consists of fact finding, discussion, and bargaining. The process leads to several benefits:

- A full understanding of the safety requirement by the contractor and of the contractor's commitment to meeting and understanding of these requirements
- Correction of proposed SSP deficiencies.
- A mutual understanding of any safety tradeoffs that may be necessary. Trade-off parameters include performance, schedule, logistics support, and costs.

The negotiation process is the last chance to insure that all necessary safety program and safety risk criteria is incorporated in the contract. It permits both the FAA and the contractor to clear-up different requirement interpretations and implementation conflicts. Just as importantly, the contractor and the FAA can maximize effectiveness for planned safety program cost expenditures. Delivering System Safety Assessment Reports (SSAR) or Safety Engineering Reports (SER), for example, in a specific media format, e.g., a desktop publishing package may be an unexpected cost driver for a company that has standardized on an office suite such as MS or Corel Office. Similarly, when approval of SARs is specified, the contractor needs to cost assumed rework. If the assumption is high, the FAA may choose to forgo approval on early program submittals and substitute comments instead. There are obvious risks associated with foregoing approval on deliverables.

## 6.4 Managing Contractor System Safety (Contract Oversight)

Proactive Government participation in the contractor's system safety program is a critical path in achieving confidence in the effectiveness of the contractors system safety program and accuracy and coverage of safety analyses. The appropriate issues are:

- Contract direction can only be provided through the Government contracting office.
- Government personnel must provide corrective feedback, as needed, in such a manner that does not discourage candor and sharing of information. To that end, participation in frequent Technical Information Meetings (TIMs) and other activities such as Hazard Record Review Boards is a positive action.
- Formal review with official feedback is primarily provided through Major Program Milestones (such as a Critical Design Review , CDR) and the contract deliverables, e.g., S/SHA and SAR.

### 6.4.1 Major Program Milestones

#### ***System Design Review (SDR)/SDR Safety Review***

For SDR, the following should be available for review:

- SSPP
- Work breakdown of system safety tasks, subtasks, and manpower

- Overview of system and mission, including safety-critical systems, subsystems, and their interrelationship with mission operations
- Proposed support equipment
- Operational scenarios
- Tabulation of hazards identified
- Review of initial checklist.

The following key points should be considered in the review:

- Identification of key safety people in the contractor's organization
- Authority and responsibility of key safety positions
- Key system safety personnel qualifications
- Safety program milestones
- Proposed hazard analysis methods
- Control system for identification, recording, tracking, resolution, and closeout of problems.
- Contractor staffing and monetary resources.
- The nature of the hazards the applicable to the system application and design. For example, on a recent program the contractor decided that failure to detect weather conditions couldn't be a hazard for a ground based system. In this case, the weather protection system provided information to aircraft so it was a hazardous condition. In another case, hazard analyses were planned only for hardware and the FAA safety team leader was concerned about software hazard mitigation.

Minimum requirements for a successful SSP are:

- Contractor's demonstration of capability to perform system safety activities in compliance with contractual requirements such as tailored MIL-STD-882 and/or the FAA SSMP.
- Contractor's demonstration of understanding of applicability of safety requirements and specific hazard identification

### ***Preliminary Design Review (PDR)/PDR Safety Review***

This phase occurs early in system development prior to the detailed design process. It measures the progress and adequacy of the design approach and establishes physical and functional interfaces between the system and other systems, facilities, and support equipment.

The safety review performed at PDR considers the identified hazards and looks at the intended design controls. The cognizant FAA system safety manager usually reviews the following documents at this point:

- Preliminary Hazard or Accident Risk Assessment Reports approved by both the contractor's program manager and system safety manager
- Draft preliminary checklists
- Scenarios, including planned operations
- Current hazards lists and risk assessments
- System and subsystem descriptions
- Other hazard reports.

During the documentation review, the following key points should be checked:

- Preliminary hazards analysis activities
- Effectiveness of verification effort
- Changes to the SDR baseline
- Proposed operations and ground support equipment
- Proposed facilities design.

Finally, the government system safety manager must determine if the following requirements have been met:

- Preliminary design meets requirements established by the negotiated contract
- Hazards, compatible with the level of system development have been identified
- Proposed hazard controls and verification methods are adequate
- Safety-critical interfaces have been established and properly analyzed.
- A Hazard Tracking and Incident Reporting System are in place.

### ***Critical Design Review (CDR)/CDR Safety Review***

CDR occurs when the detail design is complete and fabrication drawings are ready to release. The Safety CDR centers on the final hazard controls incorporation into the final design and intended verification techniques. Requirements compliance is assessed. By this review, some design related safety hazards/risks will be closed, however, some hazards/risks may remain open with management's cognizance. The information sources to review are:

- SER and/or DAR verified by program manager
- Operating and support hazard analysis approach
- Operating timeline matrices.
- Operational scenarios identifying:
  - Hazardous operations
  - Support equipment planning and preliminary design

FAA System Safety Handbook, Chapter 6: System Safety Guidelines for Contracting  
August 2, 2000

- Proposed procedures list
- Proposed operational hazard controls.
- Hazard Tracking and Risk Resolution Results

The key points for evaluation are:

- System hazard analysis activities
- Operating and support hazard analysis activities
- Training requirements
- Personnel protection requirements
- Safety-critical support equipment design
- Effectiveness of design hazard controls
- Interface analysis.

The requirements that must be met at CDR for a successful program are:

- Final design meets negotiated contractual requirements
- Hazard controls have been implemented and verification methods defined
- Support equipment preliminary design hazards and controls have been identified
- All interface analyses are complete
- Contractor certification that all contractual design requirements are met.

### ***Pre-operational Safety Review***

At this review, the contractor presents the final hazard reports with controls incorporated and verified for both the operational hardware and the support equipment. Ideally, procedures and technical orders are complete; however, if they are not, then a tracking system must ensure that controls are incorporated and safety validation is performed prior to first use. The following information sources should be reviewed:

- Completed and verified operating and support hazard analyses (O&SHA)
- Approved change proposals
- Completed and verified system hazards analyses
- Completed and verified checklists
- Contractor's hazard closeout logs
- Summary of hazards analysis results and assessment of residual risk

The key points for evaluation are:

- Operating and support hazards analysis

- Changes to CDR baseline
- System hazard analysis
- Closeout of action items
- Assessment of residual risk.

The requirements for a successful safety program at the pre-operational phase are:

- Acceptable systems and operational hazards analysis
- Operational procedures/technical orders are complete and verified
- All hazards are controlled effectively and controls verified as effective
- Checklists are completed and actions verified
- All hazard records in the SAR database are reviewed and the residual risk accepted by the MA.
- Demonstrated a complete validation, verification, and if applicable certification program, to the FAA

### ***System Safety Program Reviews***

SSP status and results to date should be on the agenda of all major program milestone reviews such as the preliminary and critical design reviews. The criticality of some systems under development may be important enough for the managing authority to require special safety reviews or audits. Such special meetings are appropriate for many National Airspace System (NAS) programs.

The purpose of such meetings is to provide greater emphasis on the details of the SSP progress and analyses than is practical at a major milestone review. Given that they are required, the schedule duration, the pace of development, and the phase of the program should determine the frequency. One scenario for a two-year full-scale development program might include a kick-off safety meeting shortly after contract award and one safety review prior to Preliminary Design Review (PDR). Special meetings during the T&E phase would be held when test results suggest a need. Since one of the primary purposes of a special safety review is to discuss safety program tasks in greater detail than is compatible with a major program milestone schedule, some cost savings may be achieved by requesting parallel safety sessions at a major milestone review. This approach permits the desired detail to be discussed without accumulating the costs of an independent meeting.

All program reviews and audits provide an opportunity to review and assign action items and to explore other areas of concern. A mutually acceptable agenda/checklist should be negotiated in advance of the meeting to ensure all system safety open items are covered and that all participants are prepared for meaningful discussions.

SSP reviews to be specified in the SOW shall include, as applicable:

#### **6.4.2 System Safety Working Groups/Work Group Support**

The acquisition of expensive, complex, or critical systems, equipment, or major facilities requires considerable interaction between the integration contractor and associate contractors simultaneously. In these situations, the managing authority may require the formation of a System Safety Working Group/System Safety Working Group (SSWG). The SSWG is a formally chartered group of staff, representing organizations participating in the acquisition process. This group exists to assist the managing authority system program manager in achieving the system safety objectives. Contractor support of an SSWG is useful and may be necessary to ensure procured hardware or software is acceptably free from risks that could injure personnel or cause unnecessary damage or loss of resources.

The contractor, as an active member of the SSWG, may support the managing authority by providing or supporting presentations to the government certifying activities such as phase safety reviews or safety review boards. The following list provides management with SSWG support options to selectively impose on contractors:

- Present the contractor safety program status, including results of design or operations risk
- Summarize hazard analyses, including identification of problems and status of resolution
- Present results of analyses of prior mishaps or accidents, and hazardous malfunctions, including recommendations and action taken to prevent recurrences
- Respond to action items assigned by the chairman of the SSWG
- Develop and validate system safety requirements and criteria applicable to the program
- Identify safety deficiencies of the program and providing recommendations for corrective actions or prevention of recurrence
- Plan and coordinate support for a required certification process
- Document and distribute meeting agendas and minutes

SSWG details to be specified in the SOW should include, as applicable:

- Contractor membership requirements and role assignments (e.g., recorder, member, alternate, or technical advisor)
- Frequency or total number SSWG meetings and probable locations
- Specific SSWG support tasks required

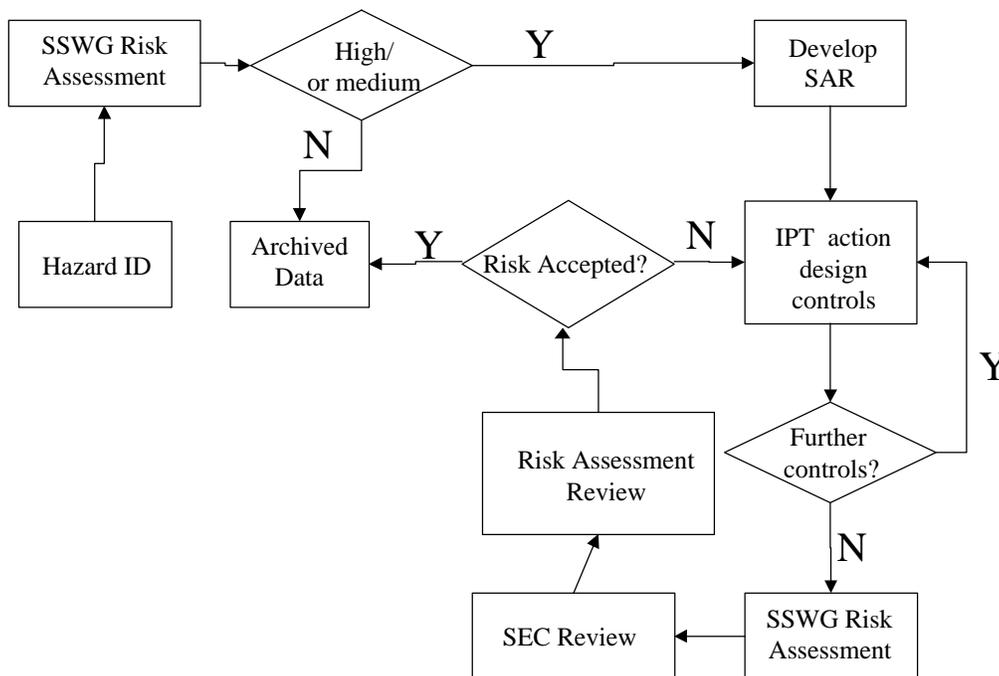
### **6.4.3 Hazard Tracking and Risk Resolution**

Each program with or without an active system safety effort can identify system hazards that require control to an acceptable risk level. A system is required to document and track hazards and resolution progress to ensure that each is controlled to an acceptable risk level.

Hazard tracking need not be a complex procedure. Any hazard tracking tool that tracks the information contained in Section 6.2 and complies with the SSMP and SSPP is acceptable for hazard tracking in the FAA at the program level. The managing authority, the system integrator, or each contractor may maintain the Safety Action Record (SAR) database. Each risk that meets or exceeds the threshold specified by the

managing authority should be entered into the SAR database when first identified. Each action taken to eliminate the risk or reduce the associated risk is documented. Management will detail the procedure for closing out the hazard or acceptance of any residual risk. The SAR may be documented and delivered as part of the system safety progress summary using, Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

Management has considerable flexibility in choosing a closed loop system to closing out a risk. See Figure 6-7. The key is the maintenance and accessibility of a SAR. The contractor can be required to establish the SAR and include within it a description of the specific corrective action taken to downgrade a medium and high risk hazards. The corrective action details and log updates can be included in monthly reports, subsequent data submissions, and at major program milestones.



**Figure 6-7: Hazard Resolution System(s)**

Management can review and approve/disapprove the corrective action or its impact by mail, at major program milestones, SSWG meetings, safety reviews board meetings, or any other engineering control process found to be effective. Although the method selected is flexible, a "paper trail" reflecting the identification of medium and high risk, a summary of the corrective action alternatives considered, conclusions, and the names of the review team is desirable.

Details to be specified in the SOW shall include, as applicable, the following:

- Hazard threshold for inclusion in the hazard log
- Complete set of data required on the hazard log, including format

- Procedures to record hazards into the log and the level of detail of the log entry
- Procedure by which the contractor shall obtain close out or risk acceptance by the MA for each hazard

#### **6.4.4 System Safety Progress Report**

Comprehensive and timely communication between management, the system integrator (when applicable), and each contractor is critical to an effective SSP. The system safety progress report provides a periodic written report of the status of system safety engineering and management activities. This status report may be submitted monthly or quarterly. It can be formatted and delivered as a Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

The contractor may prepare a periodic system safety progress report summarizing general progress made relative to the SSP during the specified reporting period and projected work for the next reporting period. The report should contain the following information.

- A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestones. It should include progress toward completion of safety data prepared or in work.
- Newly recognized significant hazards and significant changes in the degree of control of the remaining known hazards.
- Status of all recommended corrective actions not yet implemented.
- Significant cost and schedules changes that impact the safety program.
- Discussion of contractor documentation reviewed by SSWG during the reporting period. Indicate whether the documents were acceptable for safety content and whether or not inputs to improve the safety posture were made.
- Proposed agenda items for the next SSWG meeting, if such groups are formed.

## **Chapter 7: Integrated System Hazard Analysis**

<b>7.1 INTEGRATED APPROACH.....</b>	<b>2</b>
<b>7.2 RISK CONTROL .....</b>	<b>11</b>
<b>7.3 USE OF HISTORICAL DATA.....</b>	<b>18</b>

## 7.0 Integrated System Hazard Analysis

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures, based on the system safety Order of Precedence (See Table 3.2-1 in Chapter 3.) Hazard analysis is the process of examining a system throughout its life cycle to identify inherent safety related risks.

### 7.1 Integrated Approach

An integrated approach is not simple, i.e., one does not simply combine many different techniques or methods in a single report and expect a logical evaluation of system risks and hazards. The logical combining of hazard analyses is called Integrated System Hazard Analysis. To accomplish integrated system hazard analysis many related concepts about system risks should be understood. These are discussed below.

In capsulated form, to accomplish Integrated System Hazard Analysis, system risks are identified as potential system accident scenarios and the associated contributory hazards. Controls are then designed to eliminate or control the risks to an acceptable level. The ISSWG may conduct this activity during safety reviews and Integrated Risk/Hazard Tracking and Risk Resolution.

#### 7.1.1 Analysis Concepts

A scenario becomes more credible or more appropriate as the hypothesized scenario is developed to reflect reality, for example, an actual similar accident. Consistency and coherence are important during the composition of a scenario. Scenario descriptions will vary from the general to the specific. Scenarios will tend to be more specific as detailed knowledge is acquired. The completeness of the analysis also relates to how scenarios are constructed and presented. Some specific examples of scenarios are discussed in the next section.

The analyst should be concerned with machine/environment interactions resulting from change/deviation stresses as they occur in time/space, physical harm to persons; functional damage and system degradation.

The interaction consideration evaluates the interrelations between the human (including procedures), the machine and the environment: the elements of a system. The human parameter relates to appropriate human factors engineering and associated elements: biomechanics, ergonomics, and human performance variables. The machine equates to the physical hardware, firmware, and software. The human and machine are within a specific environment. Adverse effects due to the environment are to be studied. One model used for this analysis has been described earlier as the 5M model. See Chapter 3 for further elaboration.

Specific integrated analyses are appropriate at a minimum to evaluate interactions:

- Human - Human Interface Analysis
- Machine - Abnormal Energy Exchange, Software Hazard Analysis, Fault Hazard Analysis
- Environment - Abnormal Energy Exchange, Fault Hazard Analysis

The interactions and interfaces between the human, machine and the environment are to be evaluated by application of the above techniques, also with the inclusion of Hazard Control Analysis; the possibility of insufficient control of the system is analyzed.

Adverse deviations will affect system safety. The purpose of analysis is to identify possible deviations that can contribute to scenarios. Deviations are malfunctions, degradation, errors, failures, faults, and system anomalies. They are unsafe conditions and/or acts with the potential for harm. These are termed *contributory hazards* in this System Safety Handbook.

### 7.1.2 Hazards Identification and Risk Assessment

Throughout this handbook, reference is made to *hazards* and their associated *risks*. Hazards are the potential for harm. They are unsafe acts and/or unsafe conditions that can result in an accident. An accident is usually the result of many contributors (or causes) and these contributors are referred to as either initiating or contributory hazards. Depending on the context of the discussion, either hazards or their associated risks are referred to. Figures 7-1 through 7-4 provide examples of previous accident scenarios that have occurred. Note that many things had to go wrong for a particular accident to occur. Each of these accident scenarios has their associated risk. It should be noted that every contributory event has to be considered, as well as its event likelihood, when determining a specific risk. Consider that a risk is made up of a number of hazards and that each hazard has its own likelihood of occurrence. Further note that the potential worst case harm, which may be aircraft damage, injury or other property damage represents the consequence, or the severity of the accident scenario. Likelihood is determined based on an estimate of a potential accident occurring. That accident has a specific credible worst case severity. If the hypothesized accident's outcome changes, the scenario changes, and as a result, a different risk must be considered. The steps in a risk assessment are:

- Hypothesize the scenario.
- Identify the associated hazards.
- Estimate the credible worst case harm that can occur.
- Estimate the likelihood of the hypothesized scenario occurring at the level of harm (severity).

Figure 7-1 shows the sequence of events that could cause an accident from a fuel tank rupture on board an aircraft. There are a number of contributory hazards associated with this event: fuel vapor present, ignition spark, ignition and tank overpressurization, tank rupture and fragments projected. The contributors associated with this potential accident involve exposed conductors within the fuel tank due to wire insulation degradation, and the adequate ignition energy present. The outcome could be any combination of aircraft damage, and/ or injury, and/or property damage.

Figure 7-2 shows the sequence of events that could cause an accident due to a hydraulic brake failure and aircraft runway run-off. Note in this case there are again, many contributors to this event: failure of the primary hydraulic brake system, inappropriate attempt to activate emergency brake system, loss of aircraft braking capability, aircraft runs off end of runway and contacts obstructions. The outcomes could also vary from aircraft damage to injury and/or property damage. Note that the initiating events relate to the failure of the primary hydraulic brake system. This failure in and of itself is the outcome of many other contributors that caused the hydraulic brake system to fail. Further note that the improper operation of the emergency brake system is also considered an initiating event.

Figure 7-3 indicates the sequences of events that could cause an accident due to an unsecured cabin door and the aircraft captain suffers Hypoxia. Note that this event is not necessarily due to a particular failure.

FAA System Safety Handbook, Chapter 7: Integrated System Hazard Analysis  
December 30, 2000

As previously indicated, there are many contributors: the aircraft is airborne without proper cabin pressure indication, and the captain enters the unpressurized cabin without the proper personal protective equipment. The initiators in this scenario involve the cabin door not being properly secured, inadequate preflight checks, and less than adequate indication of cabin pressure loss in the cockpit. The outcome of this accident is that the captain suffers Hypoxia. Note that if both crew members investigated the anomaly, it would be possible that both pilots could have experienced Hypoxia and loss of aircraft could have occurred.

The safeguards that would either eliminate the specific hazards or control the risk to an acceptable level have also been indicated in the figures. Keep in mind that if a safeguard does not function, that in itself is a hazard. In summary, it is not easy to identify the single hazard that is the most important within the scenario sequence. As discussed, the initiating hazards, the contributory hazards, and the primary hazard must all be considered in determining the risk. The analyst must understand the differences between hazards, the potential for harm and their associated risks. As stated, a risk is comprised of the hazards within the logical sequence. In some cases, analysts may interchange terminology and refer to a hazard as a risk, or vice versa. Caution must be exercised in the use of these terms. When conducting risk assessment, the analyst must consider all possible combinations of hazards that may constitute one particular risk, which is the severity and likelihood of a potential accident.

Figure 7-1: Engine Covers Scenario

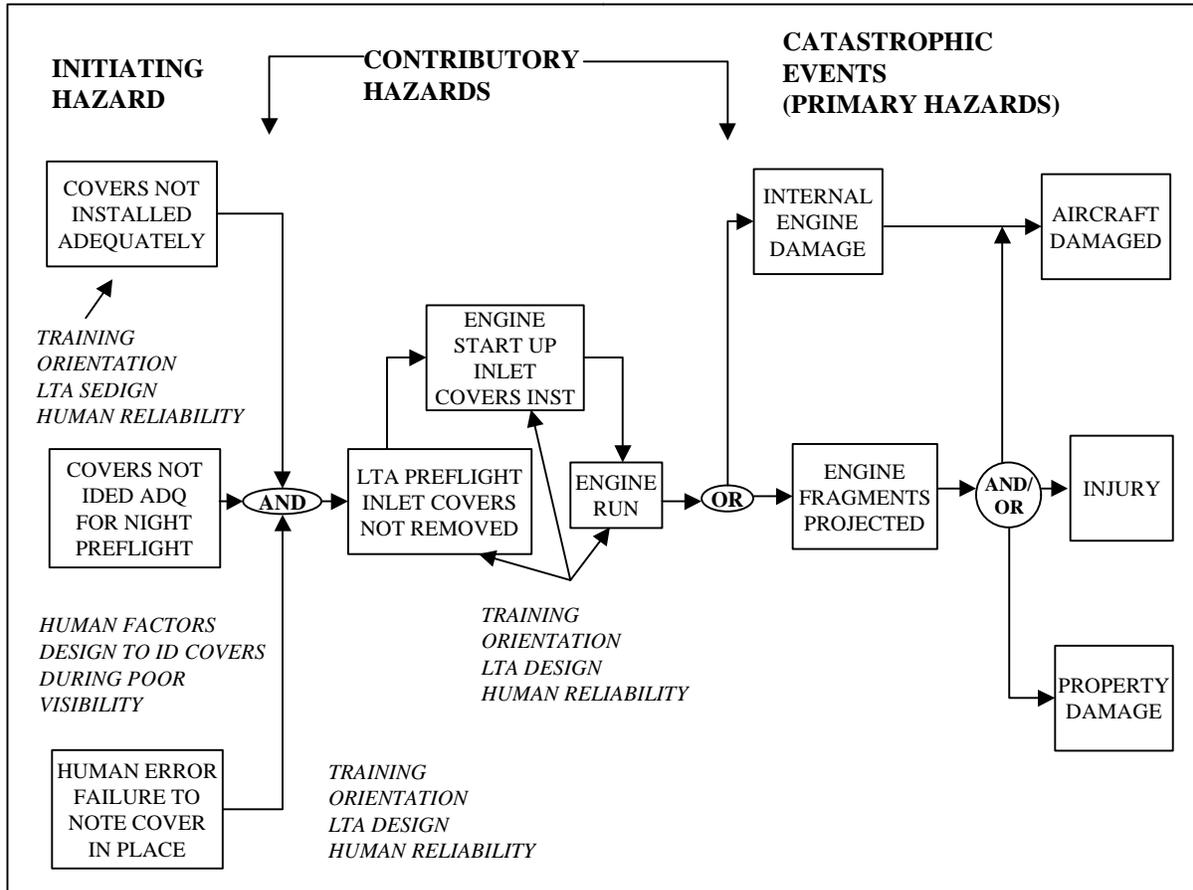


Figure 7-2: Fuel Tank Rupture Scenario

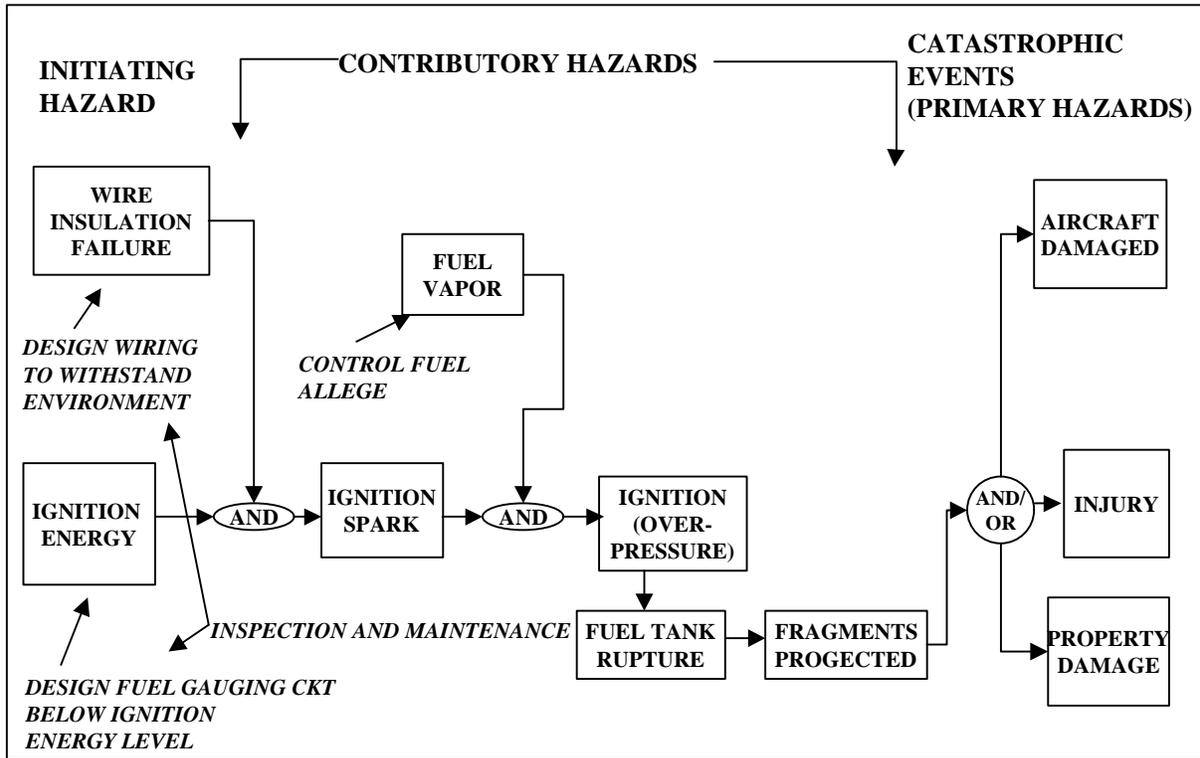


Figure 7-3: Hydraulic Brake Scenario

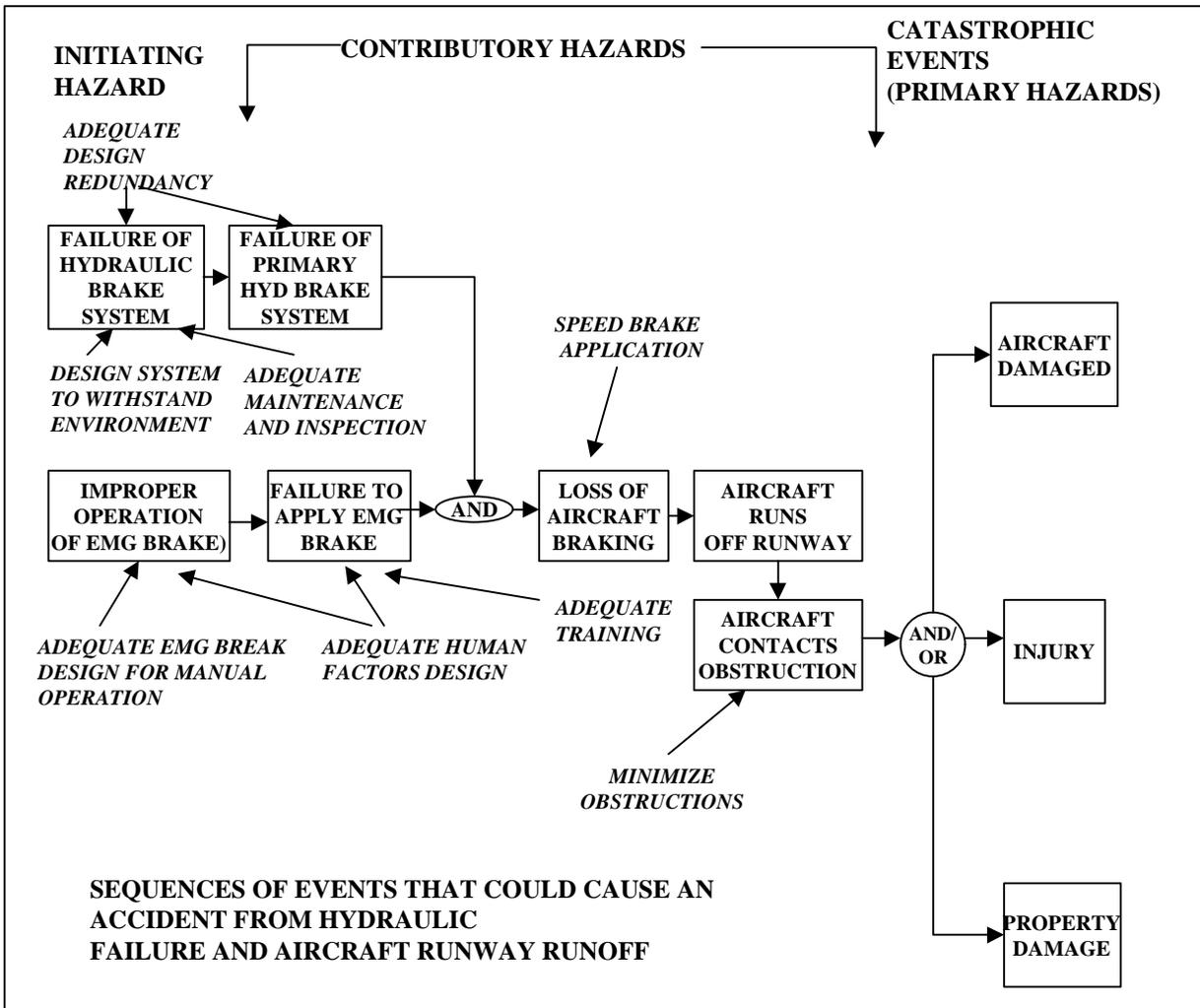
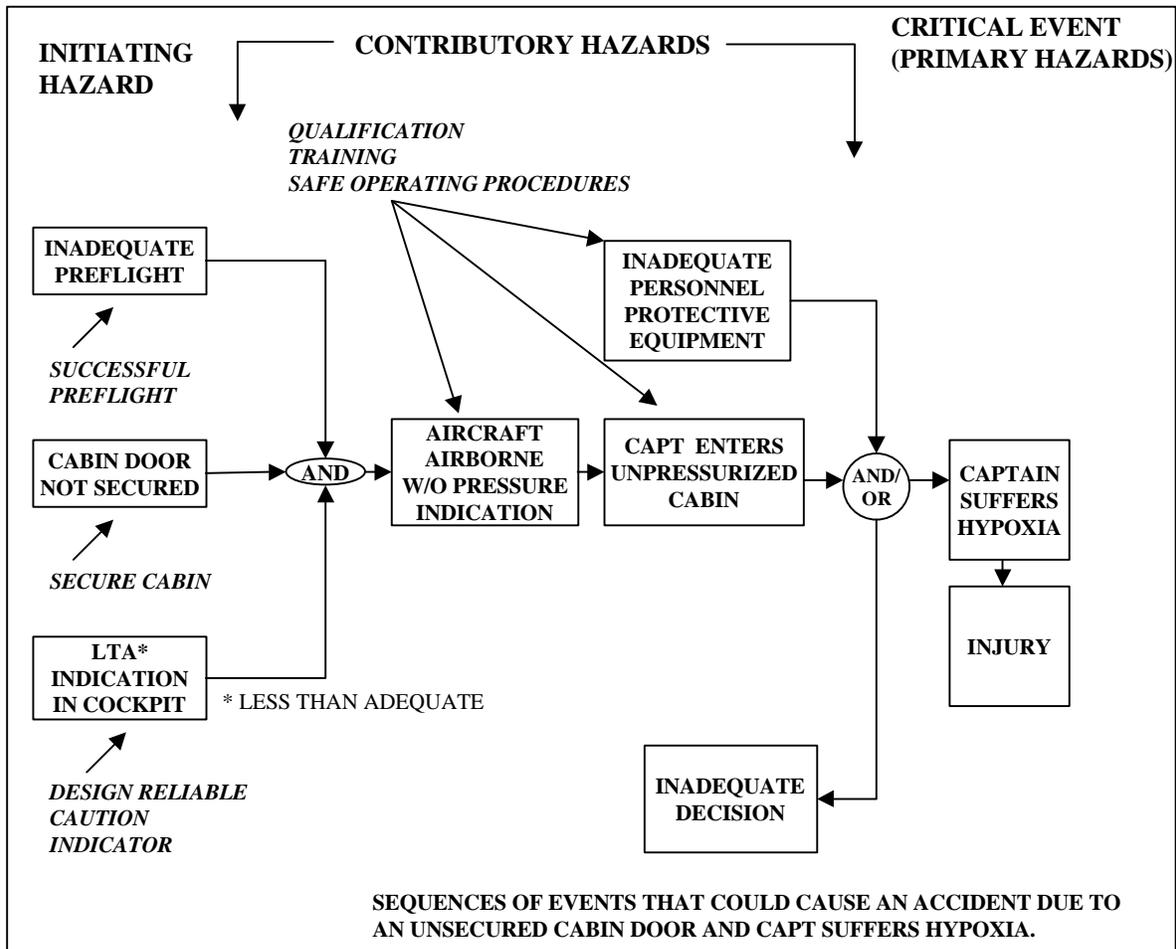


Figure 7-4: Unsecured Cabin Door Scenario



### 7.1.3 Common System Risks

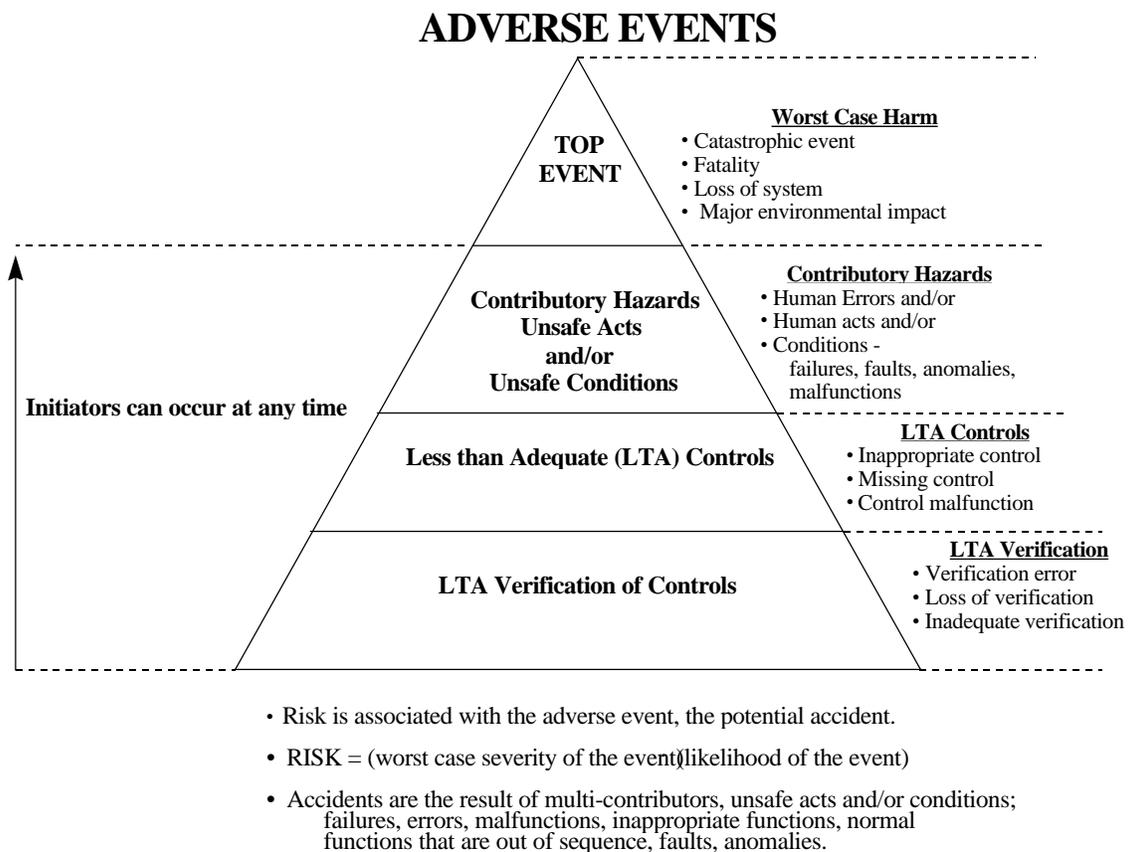
At first exposure, to the lay person, there apparently is very little difference between the disciplines of reliability and system safety, or any other system engineering practice like quality assurance, maintainability, survivability, security, logistics, human factors, and systems management. They all use similar techniques and methods, such as Failure Modes and Effects Analysis and Fault Tree Analysis. However, from the system engineering specialist's viewpoint there are many different objectives to consider and these must be in concert with the overall system objective of designing a complex system with acceptable risks.

An important system objective should include technical risk management or operational risk management. Further consideration should be given to the identification of system risks and how system risks equate within specialty engineering. Risk is an expression of probable loss over a specific period of time or over a number of operational cycles. There are situations where reliability and system safety risks are in concert and in some other cases tradeoffs must be made.

A common consideration between reliability and system safety equates to the potential unreliability of the system and associated adverse events. Adverse events can be analogous to potential system accidents. Reliability is the probability that a system will perform its intended function satisfactorily for a prescribed time under stipulated environmental conditions. The system safety objective equates to “the optimum degree of safety...” and since nothing is perfectly safe the objective is to eliminate or control known system risk to an acceptable level.

When evaluating risk, contributory hazards are important. Contributory hazards are *unsafe acts* and *unsafe conditions* with the potential for harm. Unsafe acts are human errors that can occur at any time throughout the system life cycle. Human reliability addresses human error or human failure. Unsafe conditions can be failures, malfunctions, faults, and anomalies that are contributory hazards. An unreliable system is not automatically hazardous; systems can be designed to fail-safe. Procedures and administrative controls can be developed to accommodate human error or unreliable humans, to assure that harm will not result.

The model below (Figure 7-5) shows the relationship between contributory hazards and adverse events, which are potential accidents under study.



**Figure 7-5: Relationship Between Contributory Hazards & Adverse Events**

#### **7.1.4 System Risks**

Consider a system as a composite, at any level of complexity. The elements of this composite entity are used together in an intended environment to perform a specific objective. There can be risks associated with any system and complex technical systems are everywhere within today's modern industrial society. They are part of every day life, in transportation, medical science, utilities, general industry, military, and aerospace. These systems may have extensive human interaction, complicated machines, and environmental exposures. Humans have to monitor systems, pilot aircraft, operate complex devices, and conduct design, maintenance, assembly and installation efforts. The automation can be comprised of extensive hardware, software and firmware. There are monitors, instruments, and controls. Environmental considerations can be extreme, from harsh climates, outer space, and ambient radiation. If automation is not appropriately designed considering potential risks, system accidents can result.

#### **7.1.5 System Accidents<sup>i</sup>**

System accidents may not be the result of a simple single failure, or a deviation, or a single error. Although simple adverse events still do occur, system accidents are usually the result of many contributors, combinations of errors, failures, and malfunctions. It is not easy to see the system picture or to "connect the dots" while evaluating multi-contributors within adverse events, identifying initial events, and subsequent events to the final outcome. System risks can be unique, undetectable, not perceived, not apparent, and very unusual.

Determining potential event propagation through a complex system can involve extensive analysis. Specific reliability and system safety methods such as software hazard analysis, failure modes and effects analysis, human interface analysis, scenario analysis, and modeling techniques can be applied to determine system risks, e.g., the inappropriate interaction of software, human (including procedures), machine, and environment.

#### **7.1.6 System Risk Identification**

The overall system objective should be to design a complex system with acceptable risks. Since reliability is the probability that a system will perform its intended function satisfactorily, this criteria should also address the safety-related risks that directly equate to failures or the unreliability of the system. This consideration includes hardware, firmware, software, humans, and environmental conditions.

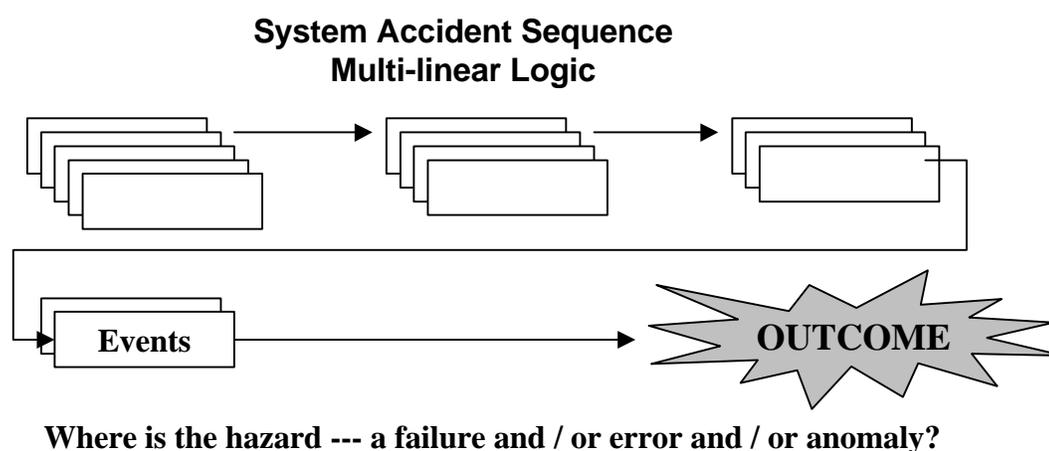
Dr. Perrow in 1984 further indicated and enhanced the multi-linear logic discussion with the definition of a system accident: "system accidents involve the unanticipated interaction of multiple failures."

From a system safety viewpoint, the problem of risk identification becomes even more complex, in that the dynamics of a potential system accident are also evaluated. When considering multi-event logic, determining quantitative probability of an event becomes extensive, laborious, and possibly inconclusive. The above model of the adverse event represents a convention (an estimation) of a potential system accident with the associated top event: the harm expected, contributory hazards, less than adequate controls, and possibly less than adequate verification. The particular potential accident has a specific initial risk and residual risk.

Since risk is an expression of probable loss over a specific period of time or over a number of operational cycles, risk is comprised of two major potential accident variables, loss and likelihood. The loss relates to harm, or severity of consequence. Likelihood is more of a qualitative estimate of loss. Quantitative likelihood estimates can be inappropriate since specific quantitative methods are questionable considering the lack of relative appropriate data. Statistics can be misunderstood or manipulated to provide erroneous

information. There are further contradictions, which add to complexity when multi-event logic is considered. This logic includes event flow, initiation, verification/control/hazard interaction, human response, and software error.

The overall intent of system safety is to prevent potential system accidents by the elimination of associated risk, or by controlling the risk to an acceptable level. The point is that reliance on probability as the total means of controlling risk can be inappropriate. Figures 7-1 through 7-3 provided examples of undesired events that require multiple conditions to exist simultaneously and in a specific sequence. Figure 7-6 summarizes multi-event logic.



**Figure 7-6: Multi-Event Logic**

## 7.2 Risk Control

The concept of controlling risk is not new. Lowrance<sup>1</sup> in 1945 had discussed the topic. It has been stated that "a thing is safe if the risks are judged to be acceptable." The discussion recently has been expanded to the risk associated with potential system accidents: system risks. Since risk is an expression of probable loss over a specific period of time, two potential accident variables, loss and likelihood can be considered the parameters of control. To control risk either the potential loss (severity or consequence) or its likelihood is controlled. A reduction of severity or likelihood will reduce associated risk. Both variables can be reduced or either variable can be reduced, thereby resulting in a reduction of risk.

The model of an adverse event above is used to illustrate the concept of risk control. For example, consider a potential system accident where reliability and system safety design and administrative controls are applied to reduce system risk. There is a top event, contributory hazards, less than adequate controls, and less than adequate verification. The controls can reduce the severity and/or likelihood of the adverse event.

Consider the potential loss of a single engine aircraft due to engine failure. Simple linear logic would indicate that a failure of the aircraft's engine during flight would result in a forced landing possibly into unsuitable terrain. Further multi-event logic which can define a potential system accident would indicate additional complexities, e.g., loss of aircraft control due to inappropriate human reaction, deviation from emergency landing procedures, less than adequate altitude, and/or less than adequate glide ratio. The reliability related engineering controls in this situation would be appropriate to system safety and would

<sup>1</sup> Lowrance, William W., Of Acceptable Risk --- Science and the Determination of Safety, 1945, Copyright 1976 by William Kaufmann, Inc.

consider the overall reliability of the engine, fuel sub-systems, and the aerodynamics of the aircraft. The system safety related controls would further consider other contributory hazards such as inappropriate human reaction, and deviation from emergency procedures. The additional controls are administrative in nature and involve design of emergency procedures, training, human response, communication procedures, and recovery procedures.

In this example, the controls above would decrease the likelihood of the event and possibly the severity. The severity would decrease as a result of a successful emergency landing procedure, where the pilot walks away and there is minimal damage to the aircraft. The analyst must consider worst case credible scenarios as well as any other credible scenarios that could result in less harm.

This has been a review of a somewhat complex potential system accident in which the hardware, the human, and the environment were evaluated. There would be additional complexity if software were included in the example. The aircraft could have been equipped with a fly-by-wire flight control system, or an automated fuel system.

Software does not fail, but hardware and firmware can fail. Humans can make software-related errors. Design requirements can be inappropriate. Humans can make errors in coding. The complexity or extensive software design could add to the error potential. There could be other design anomalies, sneak paths, and inappropriate do-loops. The sources of software error can be extensive according to Raheja, "Studies show that about 60 percent of software errors are logic and design errors; the remainder are coding -and service-related errors."<sup>2</sup> There are specific software analysis and control methods that can be successfully applied to contributory hazards, which are related to software.

Again referring to the adverse event model above, note that software errors can result in unsafe conditions or they could contribute to unsafe acts. Software controls can be inappropriate. The verification of controls could be less than adequate.

### **7.2.1 Risk Control Tradeoffs**

What appears to be a design enhancement from a reliability standpoint will not inherently improve system safety in all cases. In some cases risk can increase. In situations where such assumptions are made it may be concluded that safety will be improved by application of a reliability control, for example, redundancy may have been added within a design. The assumption may be that since it is a redundant system, it must be safe. Be wary of such assumptions. The following paragraphs present an argument that an apparent enhancement from a reliability view will not necessarily improve safety. Risk controls in the form of design and administrative enhancements are discussed along with associated tradeoffs, in support of this position.

### **7.2.2 Failure Elimination**

A common misconception that has been known in the system safety community for many years was discussed by Hammer<sup>3</sup>. It is that by eliminating failures, a product will not be automatically safe. A product may have high reliability but it may be affected by a dangerous characteristic. A Final Report of the National Commission of Product Safety (June 1970) discussed numerous products that have been injurious because of such deficiencies.

---

<sup>2</sup> Raheja, Dev G., Assurance Technologies --- Principles and Practices, McGraw-Hill, 1991, page 269.

<sup>3</sup> Hammer, Willie, Handbook of System and Product Safety, Prentice - Hall, Inc., 1972 page 21.

Consider that deficiencies are contributory hazards, unsafe acts and/or conditions that can cause harm. Without appropriate hazard analysis how would it be possible to identify the contributors?

### 7.2.3 Conformance to Codes, Standards, and Requirements

Another misconception to be considered by a reliability engineer is that conformance to codes standards and requirements provides assurance of acceptable risk. As indicated, appropriate system hazard analysis is needed to identify system hazards, so that the associated risk can be eliminated or controlled to an acceptable level.

Codes, standards, and requirements may not be appropriate, or they may be inadequate for the particular design. Therefore, risk control may be inadequate. The documents may be the result of many efforts, which may or may not be appropriately related to system safety objectives. For example, activities of committees may result in consensus, but the assumptions may not address specific hazards. The extensive analysis that has been conducted in support of document development may not have considered the appropriate risks. Also, the document may be out dated by rapid technological advancement.

As pointed out in the Final Report of the National Commission on Product Safety, industrial standards are based on the desire to promote maximum acceptance within industry. To achieve this goal, the standards are frequently innocuous and ineffective.<sup>4</sup>

Good engineering practice is required in all design fields. Certain basic practices can be utilized, but a careful analysis must be conducted to ensure that the design is suitable for its intended use.

### 7.2.4 Independent Redundancy and Monitoring

Consider another inappropriate assumption; that the system is redundant and monitored, so it must be safe. Unfortunately this may not be true. Proving that each redundant subsystem, or string, or leg is truly redundant may not be totally possible. Proving that the system will work as intended is also a concern.

Take for example a complex microprocessor and its associated software. These complex systems are never perfect according to Jones:

(response to all inputs not fully characterized), there may be remnant faults in hardware/software and the system will become unpredictable in its response when exposed to abnormal (unscheduled) conditions e.g. excess thermal, mechanical, chemical, radiation environments.<sup>5</sup>

This being the case, what can the system safety engineer do to assure acceptable risk? How does one prove independence and appropriate monitoring?

Defining acceptable risk is dependent on the specific entity under analysis, i.e., the project, process, procedure, subsystem, or system. Judgment has to be made to determine what can be tolerated should a loss occur. What is an acceptable catastrophic event likelihood? Is a single fatality acceptable, if the event can occur once in a million chances? This risk assessment activity can be conducted during a system safety working group effort within a safety review process. The point to be made here is that a simplistic assumption, which is based upon a single hazard or risk control (redundancy and monitoring), may be over simplistic.

<sup>4</sup> Ibid. Hammer page26.

<sup>5</sup> Jones, Malcolm, The Role of Microelectronics and Software in a Very High Consequence System, Proceedings of the 15<sup>th</sup> International System Safety Conference - 1997, page 336.

Proving true redundancy is not cut-and-dried in complex systems. It may be possible to design a hardware subsystem and show redundancy, i.e. redundant flight control cables, redundant hydraulic lines, or redundant piping. When there are complex load paths, complex microprocessors, and software, true independence can be questioned. The load paths, microprocessors, and software must also be independent. Ideally, different independent designs should be developed for each redundant leg. However, even independent designs produced by different manufacturers may share a common failure mode if the requirements given the software programmers is wrong.

The concepts of redundancy management should be appropriately applied.<sup>6</sup> Separate microprocessors and software should be independently developed. Single point failures should be eliminated if there are common connections between redundant legs. The switch over control to accommodate redundancy transfer should also be redundant. System safety would be concerned with the potential loss of transfer capability due to a single common event.

Common events can eliminate redundancy. The use of similar hardware and software presents additional risks, which can result in loss of redundancy. A less than adequate process, material selection, common error in assembly, material degradation, quality control, inappropriate stress testing, or calculation assumption; all can present latent risks which can result in common events. A general rule in system safety states that the system is not redundant unless the state of the backup leg is known and the transfer is truly independent.

Physical location is another important element when evaluating independence and redundancy. Appropriate techniques of separation, protection, and isolation are important. In conducting Common Cause Analysis, a technique described in the System Safety Analysis Handbook,<sup>7</sup> as well as this handbook, not only is the failure state evaluated, but possible common contributory events are also part of the equation. The analyst identifies the accident sequence in which common contributory events are possible due to physical relationships.

Other analysis techniques also address location relationships, for example, vicinity analysis, and zonal analysis. One must determine the possible outcome should a common event occur that can affect all legs of redundancy simultaneously, e.g., a major fire within a particular fire division, an earthquake causing common damage, fuel leakage in an equipment bay of an aircraft, or an aircraft strike into a hazardous location.

Keep in mind that the designers of the *Titanic* considered compartmentalization for watertight construction. However, they failed to consider latent common design flaws, such as defects in the steel plating, the state of knowledge of the steel manufacturing process, or the affects of cold water on steel.

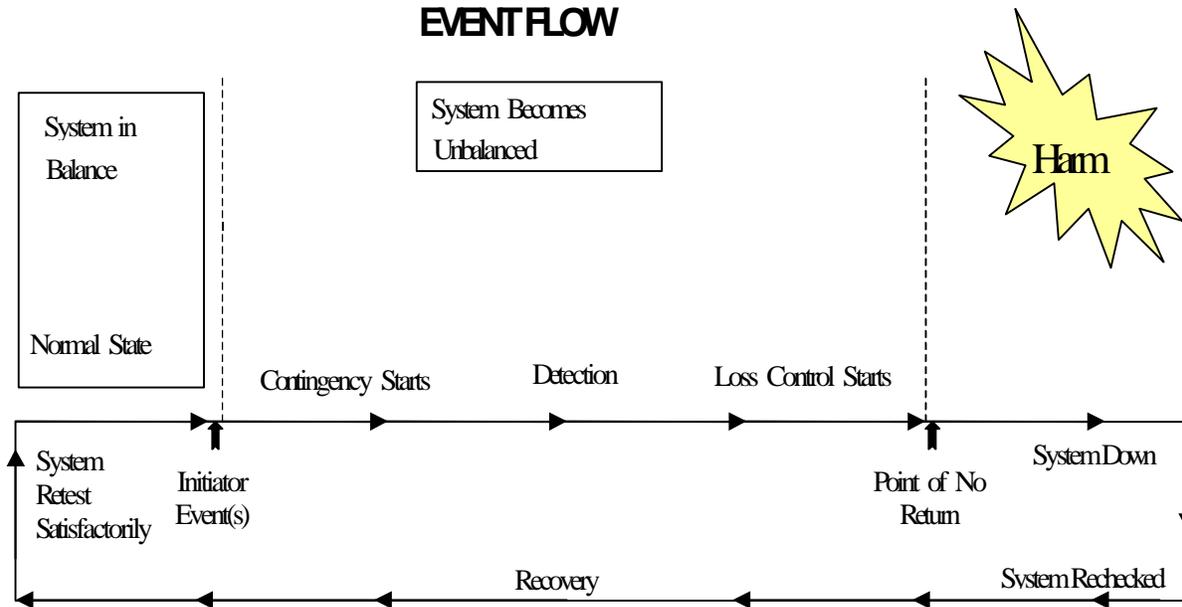
Another misconception relates to monitoring; i.e., that the system is safe because it is monitored. Safety monitoring should be designed appropriately to assure that there is confidence in the knowledge of the System State. The system is said to be *balanced* when it is functioning within appropriate design parameters. Should the system become unbalanced, the condition must be recognized in order to stabilize the system before the point of no return. This concept is illustrated in Figure 7-5. The "point of no return" is the point beyond which damage or an accident may occur.

---

<sup>6</sup> Redundancy Management requirements were developed for initial Space Station designs.

<sup>7</sup> System Safety Society, System Safety Analysis Handbook, 2<sup>nd</sup> Edition, 1997. Pages 3-37 and 3-38.

Figure 7-7: Event Flow



Monitoring devices can be incorporated into the design to check that conditions do not reach dangerous levels (or imbalance) to ensure that no contingency exists or is imminent. Monitors<sup>8</sup> can be used to indicate:

- Whether or not a specific condition exists. If indication is erroneous, contributory hazards can result.
- Whether the system is ready for operation or is operating satisfactorily as programmed. An inappropriate ready indication or inappropriate satisfactory indication can be a problem from a safety point of view.
- If a required input has been provided. An erroneous input indication can cause errors and contributory hazards.
- Whether or not the output is being generated

### 7.2.5 Probability as a Risk Control

Probability is the expectancy that an event can take place a certain number of times in a specific number of trials. Probabilities provide the foundations for numerous disciplines, scientific methodologies, and risk evaluations. Probability is appropriate in reliability, statistical analysis, maintainability, and system effectiveness.

Over time, the need for numerical evaluations of safety has generated an increase in the use of probabilities for this purpose. In 1972, Hammer expressed concerns and objections about the use of quantitative

<sup>8</sup> Ibid. Hammer, page 262.

analysis to determine probability of an accident<sup>9</sup>. These concerns and objections are based on the following reasons:

- A probability, such as reliability, guarantees nothing. Actually, a probability indicates that a failure, error, or mishap is possible, even though it may occur rarely over a period of time or during a considerable number of operations. Unfortunately, a probability cannot indicate exactly when, during which operation, or to which person a mishap will occur. It may occur during the first, last, or any intermediate operation in a series. For example, a solid propellant rocket motor developed as the propulsion unit for a missile had an overall reliability indicating that two motors of every 100,000 fired would probably fail. The first one tested blew up.
- Probabilities are projections determined from statistics obtained from past experience. Although equipment to be used in actual operations may be exactly the same as the equipment for which the statistics were obtained, the conditions under which it will be operated may be different. In addition, variations in production, maintenance, handling, and similar processes generally preclude two or more pieces of equipment being exactly alike. There are numerous instances in which minor changes in methods to produce a component with the same or improved design characteristics as previous items have instead caused failures and accidents. If an accident has occurred, correction of the cause by change in the design, material, code, procedures, or production process may immediately nullify certain statistical data.
- Generalized probabilities do not serve well for specific, localized situations. In other situations, data may be valid but only in special circumstances. Statistics derived from military or commercial aviation sources may indicate that a specific number of aircraft accidents due to bird strikes take place every 100,000 or million flight hours. On a broad basis involving all aircraft flight time, the probability of a bird strike is comparatively low. However, at certain airports near coastal areas where birds abound, the probability of a bird-strike accident is much higher.
- Human error can have damaging effects even when equipment or system reliability has not been lessened. A common example is the loaded rifle. It is highly reliable, but people have been killed or wounded when cleaning or carrying them.
- Probabilities are usually predicated on an infinite or large number of trials. Probabilities, such as reliabilities for complex systems, are of necessity based upon very small samples, and therefore have relatively low confidence levels.

### 7.2.6 Human in the Loop<sup>10</sup>

Fortunately humans usually try to acclimate themselves to automation prior to its use. Depending on the complexity of the system acclimation will take resources, time, experience, training, and knowledge. Automation has become so complex that acclimation has become an “integration-by-committee” activity. Specialists are needed in operations, systems engineering, human factors, system design, training, maintainability, reliability, quality, automation, electronics, software, network communication, avionics, and hardware. Detailed instruction manuals, usually with cautions and warnings, in appropriate language, are required. Simulation training may also be required.

---

<sup>9</sup> Ibid. Hammer, page 91 and 92.

<sup>10</sup> Allocco, Michael, *Automation, System Risks and System Accidents, 18<sup>th</sup> International System Safety Society Conference*

The interaction of the human, and machine if inappropriate, can also introduce additional risks. The human can become overloaded and stressed due inappropriately displayed data, an inappropriate control input, or similar erroneous interface. The operator may not fully understand the automation, due to its complexity. It may not be possible to understand a particular system state. The human may not be able to determine if the system is operating properly, or if malfunctions have occurred.

Imagine relying on an automated system and due to malfunction or inappropriate function, artificial indications are displayed and the system is inappropriately communicating. In this case the human may react to an artificial situation. The condition can be compounded during an emergency and the end result can be catastrophic. Consider an automated reality providing an artificial world and the human reacts to such an environment. Should we trust what the machines tell us in all cases?

The integration parameters concerning acclimation further complicate the picture when evaluating contingency, backup, damage control, or loss control. It is not easy to determine the System State; when something goes wrong, reality can become artificial. The trust in the system can be questioned. Determining what broke could be a big problem. When automation fails, the system could have a mind of its own. The human may be forced to take back control of the malfunctioning system. To accomplish such a contingency may require the system committee. These sorts of contingencies can be addressed within appropriate system safety analysis.

### 7.2.7 Software as a Risk Control

Software reliability is the probability that software will perform its assigned function under specified conditions for a given period of time<sup>11</sup>. The following axioms are offered for consideration by the system safety specialist:

- Software does not degrade over time.
- Since software executes its program *as written*, it does not fail.
- Testing of software is not an all-inclusive answer to solve all potential software-related risks.
- Software will not get better over time.
- Software can be very complex.
- Systems can be very complex.
- Humans are the least predictable links in complex systems since they may make unpredictable errors.
- Faulty design and implementation of such systems will cause them to deviate.
- Deviations can cause contributory hazards and system accidents.
- Cookbook and generic approaches do not work when there are system accidents and system risks to consider.
- It is not possible to segregate software, hardware, humans, and the environment, in the system.

---

<sup>11</sup> Ibid. Reheja, page 262.

- It may not be possible to determine what went wrong, what failed, or what broke.
- The system does not have to break to contribute to the system accident.
- Planned functions can be contributory hazards.
- Software functions can be inadequate or inappropriate.
- It is unlikely that a change in part of the software does not affect system risk.
- A change in the application may change the risk.
- Software is not generic and is not necessarily reusable.
- The system can be “spoofed”.
- A single error can propagate throughout a complex system.
- Any software error, no matter how apparently inconsequential can cause contributory events. Consider a process tool, automated calculations, automated design tools and safety systems.
- It is very hard to appropriately segregate safety-critical software in open loosely coupled systems.
- Combinations of contributory events can have catastrophic results.

Considering the many concerns and observations listed in these axioms, software-complex systems can be successfully designed to accommodate acceptable risk through the implementation of appropriately integrated specialty engineering programs that will identify, eliminate or control system risks.

### **7.3 Use of Historical Data**

Pertinent historical system safety related data and specific lessons learned information is to be used to enhance analysis efforts. For example, specific reliability data on non-developmental items (NDI) and related equipment are appropriate. Specific operational and functional information on commercial-off-the-shelf (COTS) software and hardware to be used will also be appropriate. The suitability of NDI and COTS is determined from historical data. Specific knowledge concerning past contingencies, incidents, and accidents can also be used to refine analysis activities.

---

## **Chapter 8: Safety Analysis: Hazard Analysis Tasks**

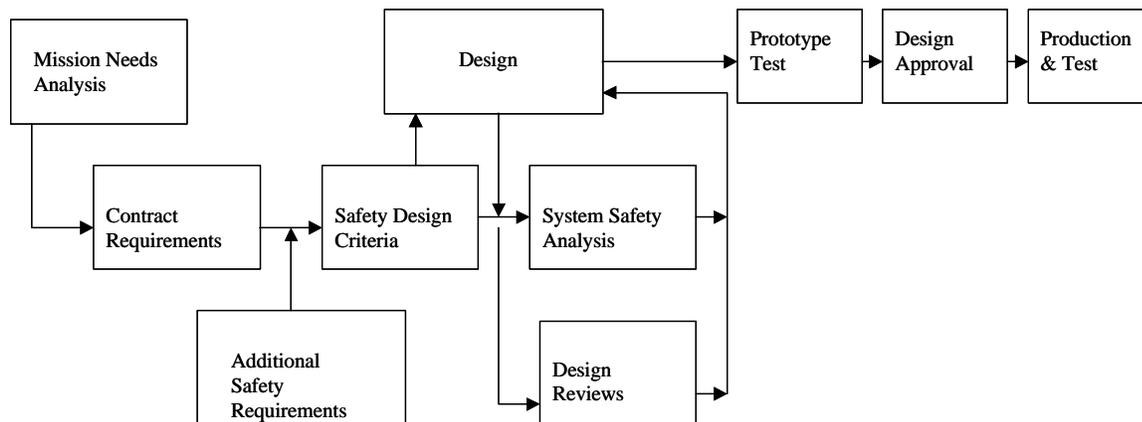
<b>8.1 THE DESIGN PROCESS.....</b>	<b>2</b>
<b>8.2 ANALYSIS.....</b>	<b>3</b>
<b>8.3 QUALITATIVE AND QUANTITATIVE ANALYSIS.....</b>	<b>7</b>
<b>8.4 DESIGN AND PRE-DESIGN SAFETY ACTIVITIES .....</b>	<b>10</b>
<b>8.5 HOW TO REVIEW AND/OR SPECIFY A SAFETY ANALYSIS.....</b>	<b>21</b>
<b>8.6 EVALUATING A PRELIMINARY HAZARD ANALYSIS.....</b>	<b>25</b>
<b>8.7 EVALUATING A SUBSYSTEM HAZARD ANALYSIS.....</b>	<b>26</b>
<b>8.8 EVALUATING A SYSTEM HAZARD ANALYSIS .....</b>	<b>29</b>
<b>8.9 EVALUATING AN OPERATING AND SUPPORT HAZARD ANALYSIS.....</b>	<b>30</b>
<b>8.10 EVALUATING A FAULT TREE ANALYSIS .....</b>	<b>31</b>
<b>8.11 EVALUATING QUANTITATIVE TECHNIQUES.....</b>	<b>35</b>

## 8.0 Safety Analysis: Hazard Analysis Tasks

### 8.1 The Design Process

A systems safety program (SSP) can be proactive or reactive. A proactive SSP influences the design process before that process begins. This approach incorporates safety features with minimal cost and schedule impact. A reactive process is limited to safety engineering analysis performed during the design process, or worse yet, following major design milestones. In this situation, the safety engineering staff is in the position of attempting to justify redesign and its associated cost.

Figure 8.1-1 is a top-level summary of a proactive SSP. Initial safety criteria is established by the managing activity (MA) and incorporated in the Request for Proposal (RFP) and subsequent contract and prime item specification. The vehicle used by the MA is a Preliminary Hazard List (PHL). Following contract award, the first technical task of a contractor's system safety staff is the flowdown of safety criteria to subsystem specifications and the translation of such criteria into a simplified form easily usable by the detailed design staff. The detailed criteria is generated from a Requirements Hazard Analysis using the PHL and Preliminary Hazard Analysis (PHA) as inputs along with requirements from standards, regulations, or other appropriate sources. Safety design criteria to control safety critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, or MA designated undesired events) must be included so that appropriate action can be taken to incorporate them in the software and hardware specifications. This analysis, in some cases, is performed before contract award.



**Figure 8-1: A Proactive System Safety Plan**

An approach of expecting each member of the design staff to research and establish a list of safety features is not only inefficient but high risk. The detailed designer has many "first" priorities and is unlikely to give focused attention to safety. An efficient and effective approach is for the system safety staff to compile comprehensive safety design criteria. These criteria should be in a simple to use format, requiring little research or interpretation. A checklist is a good format that the design engineer can frequently reference during the design process. The contractor's system safety staff and the MA can subsequently use the same checklist for design safety auditing purposes.

Sources for detailed safety design criteria include Occupational Safety and Health Administration (OSHA) standards, MIL-STD-454, Requirement 1, and MIL-STD-882. Design review is typically a continual process using hazard analyses. Active participation at internal and customer design reviews is also necessary to capture critical hazards and their characteristics. All major milestone design reviews (reference FAA Order 1810.1F, paragraph 2-8) provide a formal opportunity for obtaining safety

information and precipitating active dialogue between the MA safety staff and the contractor's safety and design engineering staff. All resulting action items should be documented with personnel responsibility assignments and an action item closing date. No formal design review should be considered complete until safety critical action items are closed out satisfactorily in the view of both the MA and the contractor. That is, both must sign that the action has been satisfactorily closed out.

All critical hazards identified by either hazard analyses or other design review activities must be formally documented. Notification of each should be provided to the appropriate contractor staff for corrective action or control. The Hazard Tracking/Risk Resolution system in Chapter 4 of this handbook should be used to track the status of each critical hazard.

## 8.2 Analysis

### 8.2.1 What is the Role of the Hazard Analysis?

Hazard analyses are performed to identify and define hazardous conditions/risks for the purpose of their elimination or control. Analyses examine the system, subsystems, components, and interrelationships. They also examine and provide inputs to the following National Airspace Integrated Logistics Support (NAIS) elements:

- Training
- Maintenance
- Operational and maintenance environments
- System/component disposal

Steps in performing a hazard analysis:

1. Describe and bound the system in accordance with system description instructions in Chapter 3.
2. Perform functional analysis if appropriate to the system under study.
3. Develop a preliminary hazard list.
4. Identify contributory hazards, initiators, or any other causes.
5. Establish hazard control baseline by identifying existing controls when appropriate.
6. Determine potential outcomes, effects, or harm.
7. Perform a risk assessment of the severity of consequence and likelihood of occurrence.
8. Rank hazards according to risk.
9. Develop a set of recommendations and requirements to eliminate or control risks
10. Provide managers, designers, test planners, and other affected decision makers with the information and data needed to permit effective trade-offs
11. Conduct hazard tracking and risk resolution of medium and high risks. Verify that recommendations and requirements identified in Step 9 have been implemented.
12. Demonstrate compliance with given safety related technical specifications, operational requirements, and design criteria.

### 8.2.2 What are the Basic Elements of A Hazard Analysis?

The analytical approach to safety requires four key elements if the resulting output is to impact the system in a timely and cost effective manner. They are:

Hazard identification

- Identification

- Evaluation
- Resolution

Timely solutions

Verification that safety requirements have been met or that risk is eliminated or controlled to an acceptable level

These concepts are described in detail below:

Identification of a risk is the first step in the risk control process. Identifying a risk provides no assurance that it will be eliminated or controlled. The risk must be documented, evaluated (likelihood and severity), and when appropriate, highlighted to those with decision making authority.

Evaluation of risks requires determination of how frequently a risk occurs and how severe it could be if and accident occurs as a result of the hazards. A severe risk that has a realistic possibility of occurring requires action; one that has an extremely remote chance may not require action. Similarly, a non-critical accident that has a realistic chance of occurring may not require further study. Frequency may be characterized qualitatively by terms such as "frequent" or "rarely." It may also be measured quantitatively such as by a probability (e.g., one in a million flight hours). In summary, the evaluation step prioritizes and focuses the system safety activity and maximizes the return-on-investment for safety expenditures.

The timing of safety analysis and resulting corrective action is critical to minimize the impact on cost and schedule. The later in the life cycle of the equipment that safety modifications are incorporated, the higher the impact on cost and schedule. The analysis staff should work closely with the designers to feed their recommendations or, at a minimum, objections back to the designers as soon as they are identified. A safe design is the end product, not a hazard analysis. By working closely with the design team, hazards can be eliminated or controlled in the most efficient manner. An inefficient alternate safety analysis approach is when the safety engineer works alone in performing an independent safety analysis and formally reports the results. This approach has several disadvantages.

Significant risks will be corrected later than the case where the design engineer is alerted to the problem shortly after detection by the safety engineer. This requires a more costly fix, leads to program resistance to change, and the potential implementation of a less effective control. The published risk may not be as severe as determined by the safety engineer operating in a vacuum, or overcome by subsequent design evolution.

Once the risks have been analyzed and evaluated, the remaining task of safety engineering is to follow the development and verify that the agreed-upon safety requirements are met by the design or that the risks are controlled to an acceptable level.

### **8.2.3 What is the Relationship Between Safety and Reliability?**

Reliability and system safety analyses complement each other. They can each provide the other more information than obtained individually. Neither rarely can be substituted for the other but, when performed in collaboration, can lead to better and more efficient products.

Two reliability analyses (one a subset of the other) are often compared to hazard analyses. Performance of a Failure Modes and Effects Analysis (FMEA) is the first step in generating the Failure Modes, Effects, and Criticality Analysis (FMECA). Both types of analyses can serve as a final product depending on the

situation. An FMECA is generated from a FMEA by adding a criticality figure of merit. These analyses are performed for reliability, and supportability information.

A hazard analysis uses a top-down methodology that first identifies risks and then isolates all possible (or probable) causes. For an operational system, it is performed for specific suspect hazards. In the case of the hazard analysis, failures, operating procedures, human factors, and transient conditions are included in the list of hazard causes.

The FMECA is limited even further in that it only considers hardware failures. It may be performed either top-down or bottom-up, usually the latter. It is generated by asking questions such as "If this fails, what is the impact on the system? Can I detect it? Will it cause anything else to fail?" If so, the induced failure is called a secondary failure.

Reliability predictions establish either a failure rate for an assembly (or component) or a probability of failure. This quantitative data, at both the component and assembly level, is a major source of data for quantitative reliability analysis. This understanding is necessary to use it correctly. In summary, however, hazard analyses are first performed in a qualitative manner identifying risks, their causes, and the significance of hazards associated with the risk.

#### **8.2.4 What General Procedures Should Follow in the Performance of a Hazard Analysis?**

Establish safety requirements baseline and applicable history (i.e., system restraints):

Specifications/detailed design requirements
Mission requirements (e.g., How is it supposed to operate?)
General statutory regulations (e.g., noise abatement)
Human factors standardized conventions (e.g., switches "up" or "forward" for on)
Accident experience and failure reports

Identify general and specific potential accident contributory factors (hazards):

In the equipment (hardware, software, and human)  
 Operational and maintenance environment  
 Human machine interfaces (e.g., procedural steps)  
 Operation  
 All procedures  
 All configurations (e.g., operational and maintenance)

Identify risks for each contributory factor (e.g., risks caused by the maintenance environment and the interface hazards). An example would be performing maintenance tasks incompatible with gloves in a very cold environment.

Assign severity categories and determine probability levels. Risk probability levels may either be assigned qualitatively or quantitatively. Risk severity is determined through hazard analysis. This reflects, using a qualitative measure, the worst credible accident that may result from the risk. These range from death to negligible effect on personnel and equipment. Evaluating the safety of the system or risk of the hazard(s), quantitatively requires the development of a probability model and the use of Boolean algebra. The latter is used to identify possible states or conditions (and combinations thereof) that may result in accidents. The model is used to quantify the likelihood of those conditions occurring.

Develop corrective actions for critical risks. This may take the form of design or procedural changes.

### **8.2.5 What Outputs Can Be Expected from a Hazard Analysis?**

An assessment of the significant safety problems of the program/system

- A plan for follow-on action such as additional analyses, tests, and training
- Identification of failure modes that can result in hazards and improper usage
- Selection of pertinent criteria, requirements, and/or specifications
- Safety factors for trade-off considerations
- An evaluation of hazardous designs and the establishment of corrective/preventative action priorities
- Identification of safety problems in subsystem interfaces
- Identification of factors leading to accidents
- A quantitative assessment of how likely hazardous events are to occur with the critical paths of cause
- A description and ranking of the importance of risks
- A basis for program oriented precautions, personnel protection, safety devices, emergency equipment-procedures-training, and safety requirements for facilities, equipment, and environment
- Evidence of compliance with program safety regulations.

## 8.3 Qualitative and Quantitative Analysis

Hazard analyses can be performed in either a qualitative or quantitative manner, or a combination of both.

### 8.3.1 Qualitative Analysis

A qualitative analysis is a review of all factors affecting the safety of a product, system, operation, or person. It involves examination of the design against a predetermined set of acceptability parameters. All possible conditions and events and their consequences are considered to determine whether they could cause or contribute to injury or damage. A qualitative analysis always precedes a quantitative one.

The objective of a qualitative analysis is similar to that of a quantitative one. Its method of focus is simply less precise. That is, in a qualitative analysis, a risk probability is described in accordance with the likelihood criteria discussed in Chapter 3.

Qualitative analysis verifies the proper interpretation and application of the safety design criteria established by the preliminary hazard study. It also verifies that the system will operate within the safety goals and parameters established by the Operational Safety Assessment (OSA). It ensures that the search for design weaknesses is approached in a methodical, focused way.

### 8.3.2 Quantitative Analysis

Quantitative analysis takes qualitative analysis one logical step further. It evaluates more precisely the probability that an accident might occur. This is accomplished by calculating probabilities.

In a quantitative analysis, the risk probability is expressed using a number or rate. The objective is to achieve maximum safety by minimizing, eliminating, or establishing control over significant risks. Significant risks are identified through engineering estimations, experience, and documented history of similar equipment.

A probability is the expectation that an event will occur a certain number of times in a specific number of trials. Actuarial methods employed by insurance companies are a familiar example of the use of probabilities for predicting future occurrences based on past experiences. Reliability engineering uses similar techniques to predict the likelihood (probability) that a system will operate successfully for a specified mission time. Reliability is the probability of success. It is calculated from the probability of failure, in turn calculated from failure rates (failures/unit of time) of hardware (electronic or mechanical).

An estimate of the system failure probability or unreliability can be obtained from reliability data using the formula:

$$P = 1 - e^{-\lambda t}$$

Where **P** is the probability of failure, **e** is the natural logarithm, **λ** is the failure rate in failures per hour, and **t** is the number of hours operated.

However, system safety analyses predict the probability of a broader definition of failure than does reliability. This definition includes:

A failure must equate to a specific hazard

Hardware failures that are hazards

Software malfunctions

Mechanically correct but functionally unsafe system operation due to human or procedural errors

Human error in design

Unanticipated operation due to an unplanned sequence of events, actions or operating conditions.

Adverse environment.

It is important to note that the likelihood of damage or injury reflects a broader range of events or possibilities than reliability. Many situations exist in which equipment can fail and no damage or injury occurs because systems can be designed to fail safe. Conversely, many situations exist in which personnel are injured using equipment that functioned reliably (the way it was designed) but at the wrong time because of an unsafe design or procedure. A simple example is an electrical shock received by a repair technician working in an area where power has not failed.

### 8.3.2 Likelihood of occurrence

Working with likelihood requires an understanding of the following concepts.

- A probability indicates that a failure, error, or accident is possible even though it may occur rarely over a period of time or during a considerable number of operations. A probability cannot indicate exactly when, during which operation, or to which person a accident will occur. It may occur during the first, last, or any intermediate operation in a series without altering the analysis results. Consider an example of when the likelihood of an aircraft engine failing is accurately predicted to be one in 100,000. The first time the first engine is tried it fails. One might expect the probability of the second one failing to be less. But, because these are independent events, the probability of the second one is still one in 100,000. The classic example demonstrating this principal is that of flipping a coin. The probability of it landing "heads-up" is 1 chance in 2 or 0.5. This is true every time the coin is flipped even if the last 10 trials experienced a "heads-up" result. Message: Do not change the prediction to match limited data.
- Probabilities are statistical projections that can be based upon specific past experience. Even if equipment is expected to perform the same operations as those used in the historical data source, the circumstances under which it will be operated can be expected to be different. Additional variations in production, maintenance, handling, and similar processes generally preclude two or more pieces of equipment being exactly alike. Minor changes in equipment have been known to cause failures and accidents when the item was used. If an accident or failure occurs, correcting it by changing the design, material, procedures, or production process immediately nullifies certain portions of the data. Message: Consider the statistical nature of probabilities when formulating a conclusion.
- Sometimes data are valid only in special circumstances. For instance, a statistical source may indicate that a specific number of aircraft accidents due to birdstrikes take place every 100,000 or million hours. One may conclude from this data, that the probability of a birdstrike is comparatively low. Hidden by the data analysis approach, is the fact that at certain airfields, such as Boston, the

Midway Islands, and other coastal and insular areas where birds abound, the probability of a birdstrike accident is much higher than the average. This example demonstrates that generalized probabilities will not serve well for specific, localized areas. This applies to other environmental hazards such as lightning, fog, rain, snow, and hurricanes. Message: Look for important variables that may affect conclusions based on statistics.

- Reliability predictions are based upon equipment being operated within prescribed parameters over a specific period of time. When the equipment's environment or operational profile exceeds those design limits, the validity of the prediction is invalid. Safety analyses based on this data attempting to predict safety performance under abnormal and/or emergency conditions may also be invalid. Reliability predictions do not extend to performance of components or subassemblies following a failure. That is, the failure rate or characteristics of failed units or assemblies are not accounted for in reliability generated predictions. Design deficiencies are not accounted for in reliability predictions. For example, a reliability prediction accounts for the failure rate of components, not the validity of the logic. Message: Be clear on what conditions the probabilities used in the risk analysis represent.
- Human error can have damaging effects even when equipment reliability is high. For example, a loaded rifle is highly reliable, yet many people have been killed or wounded when cleaning, carrying, or playing with loaded guns. Message: Consider the impact of human error on accident probability estimations.
- The confidence in a probability prediction, as in any statistic, is based on the sample size of the source data. Predictions based on small sample sizes have a low confidence level; those based on a large sample size provide a high degree of confidence. Message: Understand the source of prediction data. Consider the confidence level of the data.
- Reliability predictions of electronic components could assume an exponential failure distribution. This is a reasonable assumption for systems conservatively designed prior to wearout. The confidence that the prediction represents either a newly fielded system or an old system is less. There are recently developed approaches to reliability predictions that consider mechanical fatigue of electronic components that account for wearout. Such an improved prediction is only more valuable than the standardized approach when being applied to a specific unit when its history is known. Message: Risk of systems that exhibit wearout are more difficult to quantify than those that do not.

When the limitations are understood, the use of probabilities permits a more precise risk analysis than the qualitative approach. Calculated hazard risks can be compared to acceptable thresholds to determine when redesign is necessary. They permit the comparison of alternate design approaches during trade-studies leading to more thorough evaluations. Performing quantitative analyses requires more work than qualitative analyses and therefore costs more. If the limitations of the numbers used are not clearly stated and understood, the wrong conclusion may be reached. When care is taken, a quantitative analysis can be significantly more useful than a qualitative one.

## 8.4 Design and Pre-Design Safety Activities

The design and pre-design system safety engineering activities, are listed below:

- Activity 1 - Preliminary Hazard List (PHL)
- Activity 2 - Preliminary Hazard Analysis (PHA)
- Activity 3 - Requirements Hazard Analysis (RHA)
- Activity 4- Subsystem Hazard Analysis (SSHA)
- Activity 5 - System Hazard Analysis (SHA)
- Activity 6 - Operating and Support Hazard Analysis (O&SHA)
- Activity 7 - Health Hazard Assessment (HHA)

The completion of these activities represents the bulk of the SSP. The output and the effects of implementing the activities are the safety program. Review of the documented analyses provides the MA and integrator visibility into the effectiveness and quality of the safety program. It is recommended that these analyses be documented in a format compatible with an efficient review.

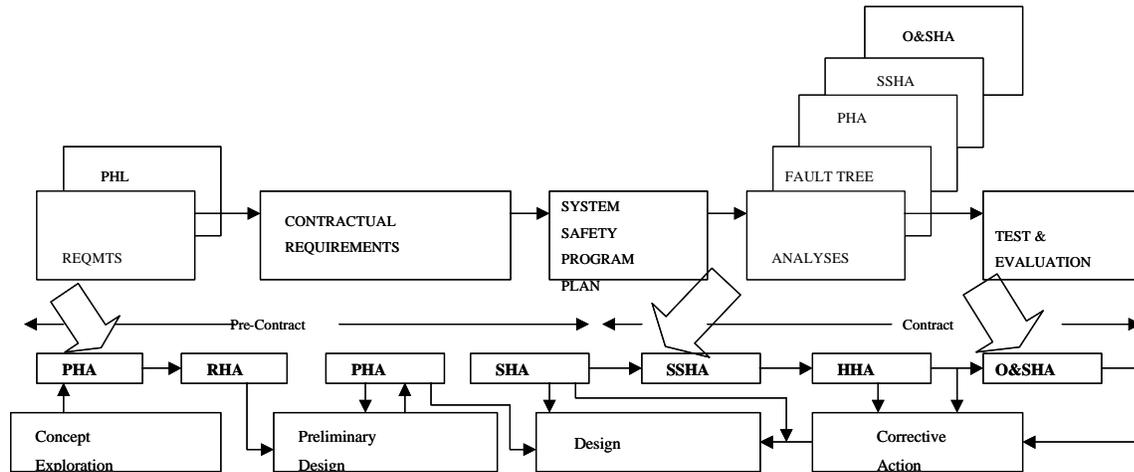
The following format features are recommended:

- Inclusion of a "road map" to show the sequence of tasks performed during the analysis.
- Presentation style, which may be in contractor format, consistent with the logic of the analysis procedure.
- All primary (critical) hazards and risks listed in an unambiguous manner.
- All recommended hazard controls and corrective actions detailed.

Questions that the reviewer should ask as the analyses are reviewed include the following:

- Do the contributory hazards listed include those that have been identified in accidents of similar systems?
- Are the recommended hazard controls and corrective actions realistic and sufficient?
- Are the recommended actions fed back into the line management system in a positive way that can be tracked?

Figure 8-2 illustrates the interrelationship of these tasks and their relationship to the design and contractual process.



**Figure 8-2: Hazard Analysis Relationships**

#### 8.4.1 Activity 1: Preliminary Hazard List

The Preliminary Hazard List (PHL) is generated at the start of each hazard analysis. It is basically a list of anything that the analyst can think of that can go wrong based on the concept, its operation and implementation. It provides the MA with an inherent list of hazards associated with the concept under consideration. The contractor may be required to investigate further selected hazards or hazardous characteristics identified by the PHL as directed by the MA to determine their significance. This information is important for the MA in making a series of decisions ranging from "Should the program continue?" to shaping the post contractual safety requirements. The PHL may be generated by either the MA or a contractor.

The PHL lists of hazards that may require special safety design emphasis or hazardous areas where in-depth analyses need to be done. Example uses of the PHL include providing inputs to the determination process of the scope of follow-on hazard analyses (e.g., PHA, SSHA). The PHL may be documented using a table-type format.

#### 8.4.2 Activity 2: Preliminary Hazard Analysis

The Preliminary Hazard Analysis (PHA) is the initial effort in hazard analysis during the system design phase or the programming and requirements development phase for facilities acquisition. It may also be used on an operational system for the initial examination of the state of safety. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states with all of the accompanying system implications.

The PHA effort should begin during the earliest phase that is practical and updated in each sequential phase. Typically, it is first performed during the conceptual phase but, when applicable, may be performed on an operational system. Performing a PHA early in the life cycle of a system provides important inputs to tradeoff studies in the early phases of system development. In the case of an operational system, it aids in an early determination of the state of safety. The output of the PHA may be used in developing system safety requirements and in preparing performance and design specifications. In addition, the PHA is the basic hazard analysis that establishes the framework for other hazard analyses that may be performed.

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

- As complete a description as possible of the system or systems being analyzed, how it will be used, and interfaces with existing system(s). If an OED was performed during pre-development, this can form the basis for a system description.
- A review of pertinent historical safety experience (lessons learned on similar systems)
- A categorized listing of basic energy sources
- An investigation of the various energy sources to determine the provisions that have been developed for their control
- Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system must comply.
- Recommendation of corrective actions.

Since the PHA should be initiated very early in the planning phase, the data available to the analyst may be incomplete and informal. Therefore, the analysis should be structured to permit continual revision and updating as the conceptual approach is modified and refined. As soon as the subsystem design details are complete enough to allow the analyst to begin the subsystem hazard analysis in detail, the PHA can be terminated. The PHA may be documented in any manner that renders the information above clear and understandable to the non-safety community. A tabular format is usually used.

The following reference input information is helpful to perform a PHA:

- Design sketches, drawings, and data describing the system and subsystem elements for the various conceptual approaches under consideration
- Functional flow diagrams and related data describing the proposed sequence of activities, functions, and operations involving the system elements during the contemplated life span
- Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, and use locations and safety-related experiences of similar previous programs or activities.

The PHA must consider the following for identification and evaluation of hazards as a minimum.

- Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
- Safety-related interface considerations among various elements of the system (e.g., material compatibility, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This must include consideration of the potential contribution by software (including software developed by other contractors) to subsystem/system accidents.
- Environmental constraints, including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation).

- If available, operating, test, maintenance, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage).
- If available, facilities, support equipment (e.g., provisions for storage, assembly, checkout, proof testing of hazardous systems/assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials; radiation or noise emitters; electrical power sources), and training (e.g., training and certification pertaining to safety operations and maintenance).
- Safety-related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, hardware or software fail-safe design considerations, subsystem protection, fire detection and suppression systems, personal protective equipment, industrial ventilation, and noise or radiation barriers).

### 8.4.3 Activity 3: Requirements Hazard Analysis

The purpose of Activity 3 is to perform and document the safety design requirements/design criteria for a system or facility undergoing development or modification. It is also an opportunity to develop safety requirements from regulations, standards, FAA Orders, Public Laws, etc. that are generic and not related to a specific identified hazard. In the early system design phase, the developer can usually anticipate the system design, including likely software control and monitoring functions. This information can be used to determine the potential relationship between system-level hazards, hardware elements and software control and monitoring and safety functions, and to develop design requirements, guidelines, and recommendations to eliminate or reduce the risk of those hazards to an acceptable level. Enough information can be collected to designate hardware and software functions as safety critical.

During the Demonstration and Evaluation and/or Full-Scale Development phases, the developer should analyze the system along with hardware/software design and requirements documents to:

- Refine the identification of hazards associated with the control of the system
- Safety-critical data generated or controlled by the system
- Safety-critical non-control functions performed by the system and unsafe operating modes for resolution.

The requirements hazard analysis is substantially complete by the time the allocated baseline is defined. The requirements are developed to address hazards, both specific and nonspecific, in hardware and software.

The requirements hazard analysis may use the PHL and the PHA as a basis, if available. The analysis relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The requirements hazard analysis is also used to incorporate design requirements that are safety related but not tied to a specific hazard. This analysis includes the following:

Determination of applicable generic system safety design requirements and guidelines for both hardware and software from applicable military specifications, Government standards, and other documents for the

system under development. Incorporate these requirements and guidelines into the high-level system specifications and design documents, as appropriate.

Analysis of the system design requirements, system/segment specifications, preliminary hardware configuration item development specifications, software requirements specifications, and the interface requirements specifications, as appropriate, including the following sub-activities:

- Develop, refine, and specify system safety design requirements and guidelines; translate into system, hardware, and software requirements and guidelines, where appropriate; implement in the design and development of the system hardware and associated software.
- Identify hazards and relate them to the specifications or documents above and develop design requirements to reduce the risk of those hazards.
- Analyze the preliminary system design to identify potential hardware/software interfaces at a gross level that may cause or contribute to potential hazards. Interfaces to be identified include control functions, monitoring functions, safety systems, and functions that may have indirect impact on safety.
- Perform a preliminary risk assessment on the identified safety-critical software functions using the hazard risk matrix or software hazard risk matrix of Chapter 10 or another process as mutually agreed to by the contractor and the MA.
- Ensure that system safety design requirements are properly incorporated into the operator, users, and diagnostic manuals.
- Develop safety-related design change recommendations and testing requirements and incorporate them into preliminary design documents and the hardware, software, and system test plans. The following subactivities should be accomplished:
  - Develop safety-related change recommendations to the design and specification documents listed above and include a means of verification for each design requirement.
  - Develop testing requirements. The contractor may develop safety-related test requirements for incorporation into the hardware, software, and system integration test documents.
  - Support the system requirements review, system design review, and software specification review from a system safety viewpoint. Address the system safety program, analyses performed and to be performed, significant hazards identified, hazard resolutions or proposed resolutions, and means of verification.

For work performed under contract details to be specified in the SOW shall include, as applicable:

- Definition of acceptable level of risk within the context of the system, subsystem, or component under analysis
- Level of contractor support required for design reviews
- Specification of the type of risk assessment process.

#### 8.4.4 Activity 4: Subsystem Hazard Analysis

The Subsystem Hazard Analysis (SSHA) is performed if a system under development contained subsystems or components that when integrated function together in a system. This analysis examines each subsystem or component and identifies hazards associated with normal or abnormal operations and is intended to determine how operation or failure of components or any other anomaly that adversely affects the overall safety of the system. This analysis should identify existing and recommended actions using the system safety precedence to determine how to eliminate or reduce the risk of identified hazards.

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

A contractor may perform and document a subsystem hazard analysis to identify all components and equipment, including software, whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard or whose design does not satisfy contractual safety requirements. The analysis may include:

- A determination of the hazards or risks, including reasonable human errors as well as single and multiple failures.
- A determination of potential contribution of software (including that which is developed by other contractors) events, faults, and occurrences (such as improper timing) on the safety of the subsystem
- A determination that the safety design criteria in the software specification(s) have been satisfied
- A determination that the method of implementation of software design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has introduced any new hazards.

If no specific analysis techniques are directed, the contractor may obtain MA approval of technique(s) to be used prior to performing the analysis. When software to be used in conjunction with the subsystem is being developed under standards, the contractor performing the SSHA will monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA (See Chapter 10 for discussion of standards commonly used). Problems identified that require the response of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process. The contractor must update the SSHA when needed as a result of any system design changes, including software changes that affect system safety.

For work performed under contract details to be specified in the SOW shall include, as applicable:

- Minimum risk severity and probability reporting thresholds
- The specific subsystems to be analyzed
- Any selected risks, hazards, hazardous areas, or other items to be examined or excluded
- Specification of desired analysis technique(s) and/or format.

### 8.4.5 Activity 5: System Hazard Analysis

A System Hazard Analysis (SHA) is accomplished in much the same way as the SSHA. However, as the SSHA examines how component operation or risks affect the system, the SHA determines how system operation and hazards can affect the safety of the system and its subsystems. The SSHA, when available, 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. Design changes will need to be evaluated to determine their effects on the safety of the system and its subsystems. This analysis should contain recommended actions, applying the system safety precedence, to eliminate or reduce the risk of identified hazards. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating the SHA with other hazard analyses. The SHA may be documented in text and/or tabular format or a combination of both text and tables. (See Chapter 6, Integrated System Hazard Analysis Concepts)

A contractor may perform and document an SHA to identify hazards and assess the risk of the total system design, including software, and specifically the subsystem interfaces. This analysis must include a review of subsystem interrelationships for:

- Compliance with specified safety criteria
- Independent, dependent, and simultaneous hazardous events including failures of safety devices and common causes that could create a hazard
- Degradation in the safety of a subsystem or the total system from normal operation of another subsystem
- Design changes that affect subsystems
- The effects of reasonable human errors
- The potential contribution of software (including that which is developed by other contractors) events, faults, and occurrences (such as improper timing) on safety of the system
- The determination that safety design criteria in the software specification(s) have been satisfied

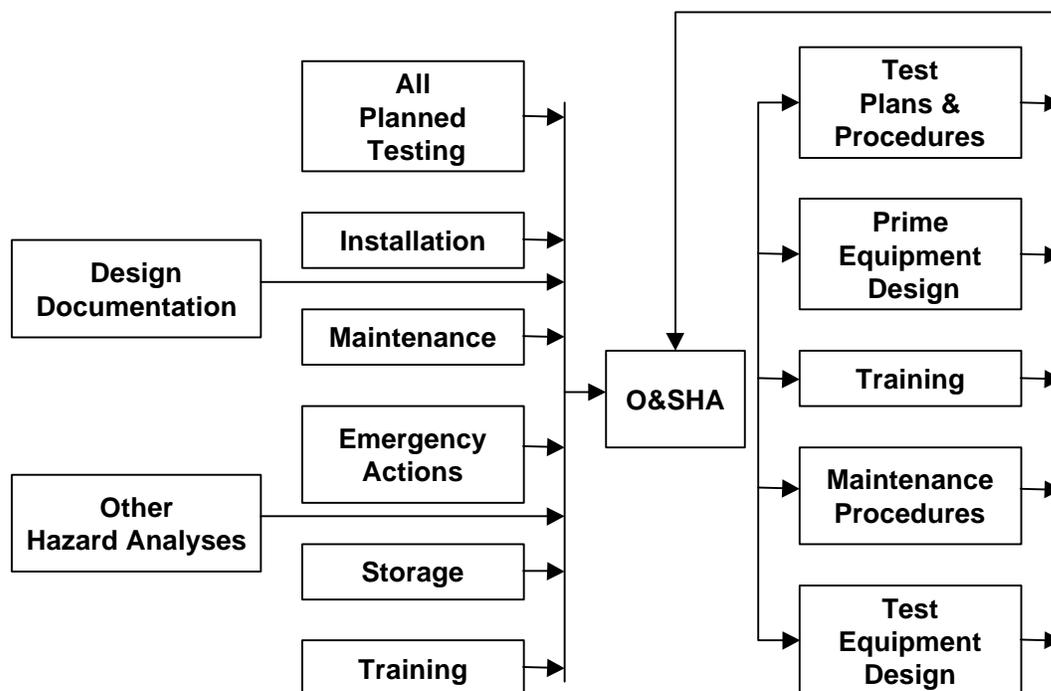
If no specific analysis techniques are directed, the contractor may obtain MA approval of technique(s) to be used prior to performing the analysis. The SHA may be performed using similar techniques to those used for the SSHA. When software to be used in conjunction with the system is being developed under software standards, the contractor performing the SHA should be required to monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to safety. (See Chapter 10, Software Safety Process) Problems identified that require the response of the software developer should be reported to the MA in time to support the ongoing phase of the software development process. A contractor should also be required to update the SHA when needed as a result of any system design changes, including software, which affect system safety. In this way, the MA is kept up to date about the safety impact of the design evolution and is in a position to direct changes.

When work is performed under contract, details to be specified in the SOW shall include, as applicable:

- Minimum risk severity and probability reporting thresholds
- Any selected hazards, hazardous areas, or other specific items to be examined or excluded
- Specification of desired analysis technique(s) and/or format

### 8.4.6 Activity 6: Operating and Support Hazard Analysis

The Operating and Support Hazard Analysis (O&SHA) is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, operation, support, and equipment involved throughout the total life cycle of a system/element. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, post-accident responses, and training. Figure 8-3 shows O&SHA elements. The O&SHA may also be selectively applied to facilities acquisition projects to make sure operation and maintenance manuals properly address safety and health requirements. Also, see Chapter 12, Existing Facilities section.



**Figure 8-3: Operating & Support Hazard Analysis (O&SHA) Elements**

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

- Engineering descriptions of the proposed system, support equipment, and facilities
- Draft procedures and preliminary operating manuals
- PHA, SSHA, and SHA reports
- Related and constraint requirements and personnel capabilities
- Human factors engineering data and reports
- Lessons learned, including a history of accidents caused by human error

FAA System Safety Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks  
December 30, 2000

- Effects of off-the-shelf hardware and software across the interface with other system components or subsystems.

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

A contractor may perform and document an O&SHA to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons considering the following:

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

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

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

FAA System Safety Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks  
December 30, 2000

The O&SHA documents system safety assessment of procedures involved in system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, and disposal. A contractor must update the O&SHA when needed as a result of any system design or operational changes. If no specific analysis techniques are directed, the contractor should obtain MA approval of technique(s) to be used prior to performing the analysis.

For work performed under contract, details to be specified in the SOW shall include, as applicable:

- Minimum risk probability and severity reporting thresholds
- Specification of desired analysis technique(s) and/or format
- The specific procedures to be evaluated.

#### **8.4.7 Activity 7: Health Hazard Assessment**

The purpose of Activity 7 is to perform and document a Health Hazard Assessment (HHA) to identify health hazards, evaluate proposed hazardous materials, and propose protective measures to reduce the associated risk to a level acceptable to the MA.

The first step of the HHA is to identify and determine quantities of potentially hazardous materials or physical agents (noise, radiation, heat stress, cold stress) involved with the system and its logistical support. The next step is to analyze how these materials or physical agents are used in the system and for its logistical support. Based on the use, quantity, and type of substance/agent, estimate where and how personnel exposures may occur and if possible the degree or frequency of exposure. The final step includes incorporation into the design of the system and its logistical support equipment/facilities, cost-effective controls to reduce exposures to acceptable levels. The life-cycle costs of required controls could be high, and consideration of alternative systems may be appropriate.

An HHA evaluates the hazards and costs due to system component materials, evaluates alternative materials, and recommends materials that reduce the associated risks and life-cycle costs. Materials are evaluated if (because of their physical, chemical, or biological characteristics; quantity; or concentrations) they cause or contribute to adverse effects in organisms or offspring, pose a substantial present or future danger to the environment, or result in damage to or loss of equipment or property during the systems life cycle.

An HHA should include the evaluation of the following:

- Chemical hazards - Hazardous materials that are flammable, corrosive, toxic, carcinogens or suspected carcinogens, systemic poisons, asphyxiants, or respiratory irritants
- Physical hazards (e.g., noise, heat, cold, ionizing and non-ionizing radiation)
- Biological hazards (e.g., bacteria, fungi)
- Ergonomic hazards (e.g., lifting, task saturation)
- Other hazardous materials that may be introduced by the system during manufacture, operation, or maintenance.

The evaluation is performed in the context of the following:

FAA System Safety Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks  
December 30, 2000

- System, facility, and personnel protective equipment requirements (e.g., ventilation, noise attenuation, radiation barriers) to allow safe operation and maintenance. When feasible engineering designs are not available to reduce hazards to acceptable levels, alternative protective measures must be specified (e.g., protective clothing, operation or maintenance procedures to reduce risk to an acceptable level).
- Potential material substitutions and projected disposal issues. The HHA discusses long-term effects such as the cost of using alternative materials over the life cycle or the capability and cost of disposing of a substance.
- Hazardous material data. The HHA describes the means for identifying and tracking information for each hazardous material. Specific categories of health hazards and impacts that may be considered are acute health, chronic health, cancer, contact, flammability, reactivity, and environment.

The HHA's hazardous materials evaluation must include the following:

- Identification of the hazardous materials by name(s) and stock numbers (or CAS numbers); the affected system components and processes; the quantities, characteristics, and concentrations of the materials in the system; and source documents relating to the materials
- Determination of the conditions under which the hazardous materials can release or emit components in a form that may be inhaled, ingested, absorbed by living beings, or leached into the environment
- Characterization material hazards and determination of reference quantities and hazard ratings for system materials in question
- Estimation of the expected usage rate of each hazardous material for each process or component for the system and program-wide impact
- Recommendations for the disposition of each hazardous material identified. If a reference quantity is exceeded by the estimated usage rate, material substitution or altered processes may be considered to reduce risks associated with the material hazards while evaluating the impact on program costs.

For each proposed and alternative material, the assessment must provide the following data for management review:

- Material identification. Includes material identity, common or trade names, chemical name, chemical abstract service (CAS) number, national stock number (NSN), local stock number, physical state, and manufacturers and suppliers
- Material use and quantity. Includes component name, description, operations details, total system and life cycle quantities to be used, and concentrations of any mixtures
- Hazard identification. Identifies the adverse effects of the material on personnel, the system, environment, or facilities
- Toxicity assessment. Describes expected frequency, duration, and amount of exposure. References for the assessment must be provided

- Risk calculations. Includes classification of severity and probability of occurrence, acceptable levels of risk, any missing information, and discussions of uncertainties in the data or calculations.

For work performed under contract, details to be specified in the SOW include:

- Minimum risk severity and probability reporting thresholds
- Any selected hazards, hazardous areas, hazardous materials or other specific items to be examined or excluded
- Specification of desired analysis techniques and/or report formats.

## 8.5 How to Review and/or Specify a Safety Analysis

### 8.5.1 What is the Objective?

When evaluating any hazard analysis, the reviewer should place emphasis on the primary purposes for performing the analysis. They all should provide the following:

- The identification of actual hazards and risks. Hazards may occur from either simultaneous or sequential failures and from "outside" influences, such as environmental factors or operator errors.
- An assessment of each identified risk. A realistic assessment considers the risk severity (i.e., what is the worst that can happen?) and the potential frequency of occurrence (i.e., how often can the accident occur?). Risk as a function of expected loss is determined by the severity of loss and how often the loss occurs. Some hazards are present all of the time, or most of the time, but do not cause losses.
- Recommendations for resolution of the risk (i.e., what should we do about it?). Possible solutions mapped into the safety precedence of Chapter 4 are shown in Figure 8-4.

<b>HAZARD:</b> Failure to extend landing gear prior to landing an aircraft.	
<b>Resolution Method</b>	<b>Example</b>
Change design to eliminate hazard.	Use fixed (nonretractable) landing gear.
Use safety devices	Have landing gear extend automatically when certain parameters exist (e.g., airspeed, altitude).
Use warning devices	Provide a warning light, horn, or voice if the landing gear is not down when certain parameters are met (as in above).
Use special training and procedures	Instruct pilot to extend the gear prior to landing. Incorporate in flight simulators. Place a step "Landing Gear Down" in the flight manual.

**Figure 8-4: Safety Precedence Hazard Resolution Example**

### 8.5.2 Is the Analysis Timely?

The productivity of a hazard analysis is directly related to when in the development cycle of a system, the analysis is performed. A Preliminary Hazard Analysis (PHA), for example, should be completed in time to influence the safety requirements in specifications and interface documents. Therefore, the PHA

should be submitted prior to the preliminary design review. The instructions for a system request for proposal (RFP) with critical safety characteristics should include the requirements to submit a draft PHA with the proposal. This initial PHA provides a basis for evaluating the bidder's understanding of the safety issues. As detailed design specifications and details emerge, the PHA must be revised. The System Hazard Analysis and Subsystem Hazard Analyses (SHA and SSHA) are typically submitted prior to a Critical Design Review (CDR) or other similar review. They cannot be completed until the design is finalized at completion of the CDR. Finally, operating and support hazard analyses (O&SHA) are typically submitted after operating, servicing, maintenance, and overhaul procedures are written prior to initial system operation.

Analyses must be done in time to be beneficial. Determining that the timing was too late and rejecting the analysis for this reason provides little benefit. For example, if an SHA is performed near the end of the design cycle, it provides little benefit. The time to prevent this situation is during contract generation or less efficiently at a major program milestone such as design review.

When reviewing an analysis the following may provide some insight as to whether an analysis was performed in a timely manner:

- Is there a lack of detail in the reports? This lack of detail may also be due to insufficient experience or knowledge on the analyst's part, or due to lack of detailed design information at the time.
- Are hazards corrected by procedure changes, rather than through design changes? This may indicate that hazards were detected too late to impact the design or that the safety program did not receive the proper management attention.
- Are the controls for some hazards difficult to assess and therefore require verification through testing or demonstration? For example, consider an audio alarm control for minimizing the likelihood of landing an aircraft in a wheels-up condition. The analyst or the reviewer may realize that there are many potential audio alarms in the cockpit that may require marginally too much time to shift through. The lack of a planned test or test details should raise a warning flag. This may indicate poor integration between design, safety, and test personnel or an inadequate understanding of system safety impact on the test program.
- Is there a lack of specific recommendations? Some incomplete or late hazard reports may have vague recommendations such as "needs further evaluation" or "will be corrected by procedures." Recommendations that could have or should have been acted on by the contractor and closed out before the report was submitted are other clear indications of inadequate attention. Recommendations to make the design comply with contractual specifications and interface requirements are acceptable resolutions, provided the specifications address the hazard(s) identified.

Ideally, the final corrective action(s) should be stated in the analysis. In most cases, this is not possible because the design may not be finalized, or procedures have not been written. In either case, actions that control risk to acceptable levels should be identified. For example, if a hazard requires procedural corrective action, the report should state where the procedure would be found, even if it will be in a document not yet written. If the corrective action is a planned design change, the report should state that, and how the design change will be tracked (i.e., who will do what and when). In any case, the planned specific risk control actions should be included in the data submission. These risks should be listed in a hazard tracking and resolution system for monitoring.

If specific risk control implementation details are not yet known (as can happen in some cases), there are two main options:

- Keep the analysis open and periodically revise the report as risk control actions are implemented. (This will require a contract change proposal if outside the scope of the original statement of work (SOW)). For example, an SSHA might recommend adding a warning horn to the gear "not down" lamp for an aircraft. After alternatives have been evaluated and a decision made, the analysis report (and equipment specification) should be revised to include "An auditory and a visual warning will be provided to warn if the landing gear is not extended under the following conditions .....".
- Close the analysis, but indicate how to track the recommendation. (Provisions for tracking such recommendations must be within the scope of the contract's SOW.) This is usually done for a PHA, which is rarely revised. For example, a PHA may recommend a backup emergency hydraulic pump. The analysis should state something like "... recommend emergency hydraulic pump that will be tracked under Section L of the hydraulic subsystem hazard analysis." This method works fine if the contract's SOW requires the analyst to develop a tracking system to keep hazards from getting lost between one analysis and the next. The presence of a centralized hazard tracking system is a good indicator of a quality system safety program and should be a contractual requirement.

### 8.5.3 Who Should Perform the Analysis?

The analyst performing the analysis needs to be an experienced system safety person familiar with the system being analyzed. The system safety engineer should not only be familiar with the subsystem being analyzed, but should also have some prior systems safety experience. As discussed in Chapter 4, the required qualifications should match the nature of the system being evaluating. It is just as important not to over specify as under specify. These personnel qualification issues need to be resolved in the System Safety Program Plan, prior to the expenditure of assets by performing an inadequate

*Failure Modes and Effects Analysis (FMEA) / Failure Modes, Effects, and Criticality Analysis (FMECA).* Some system safety analyses get a "jump start" from FMEAs or FMECAs prepared by reliability engineers. The FMEA/FMECA data get incorporated into system safety analyses by adding a hazard category or other appropriate entries. This saves staffing and funds. An FMEA/FMECA performed by a reliability engineer will have different objectives than the safety engineer's analyses. The following cautions should be noted:

- Corrective action for hazards surfaced by these tools is the responsibility of the safety engineer(s).
- Sequential or multiple hazards may not be identified by the FMEA/FMECA.
- Some hazards may be missing. This is because many hazards are not a result of component failures (e.g., human errors, sneak circuits).
- All failure modes are not hazards. If the FMECA is blindly used as the foundation for a hazard analysis, time could be wasted on adding safety entries on non-safety critical systems.
- Human error hazards might not be identified.
- System risks will not have been identified.

### 8.5.4 What Data Sources May be Helpful to the Analysis?

The analyst should be required to include the sources of design data used in the analysis. The obvious sources are system layout and schematics diagrams, and physical inspections. Other sources include Military Standards (e.g., Mil-STD-454, Requirement 1) and analyses performed for other similar systems or programs. These generic sources often help the analyst to identify hazards that otherwise would go uncovered.

### 8.5.5 What Form Should the Analysis Take?

Formats for hazard analyses are usually found in one of three basic formats:

- The matrix format is the most widely used. This method lists the component parts of a subsystem on a reprinted form that includes several columns, the number of which can vary according to the analysis being done. As a minimum, there should be columns for each of the following:

Name of the item(s)
Function of the item(s)
Type of hazards, and risks
Category (severity) of the risks
Probability of the risks
Recommended corrective action

- Logic diagrams, particularly fault trees, are used to focus on certain risks. These are deductive analyses that begin with a defined undesired event (usually a accident condition) then branch out to organize all faults, sub-events, or conditions that can lead to the original undesired event.
- The narrative format will suffice for a few cases, such as focusing on a few easily identified risks associated with simple systems. This format is the easiest to apply (for the analyst), but is the most difficult to evaluate. There is no way to determine if a narrative report covers all risks so the evaluator is relying totally on the analyst's judgment.

### 8.5.6 What Methodology Should be Used?

Chapter 9 describes many hazard analysis approaches. The choice for a given program, however, is left up to individual managers and engineers. Some large-scale programs may require several hazard analyses, while smaller scale programs may require only one or two analyses. The selection of the types of hazard analyses to be accomplished is the most important aspect when preparing the SOW (for work to be performed by a contractor) and negotiating the system safety portion of a contract. If insufficient hazard analyses are designated, the system will not be analyzed properly and many hazards not identified. Conversely, if too many or the wrong types of analyses are selected, the system safety effort will be an overkill and will expend valuable monetary and manpower resources needlessly.

A PHA should always be performed for each separate program or project. The PHA provides an initial assessment of the overall program risk and it is used as a baseline for follow-on analyses, such as SSHAs, SHAs, and O&SHAs. It also identifies the need for safety tests and is used to establish safety requirements for inclusion in the system's specifications.

Subsequent decisions relate to the desirability of SSHA, SHA, and/or O&SHA. This decision is based upon several factors:

- The nature and use of the system being evaluated, especially safety criticality.
- The results of the PHA. If the system being analyzed has no unresolved safety concerns, then further analyses may not be necessary. If the hazards appear to be based upon training or procedural problems, then an O&SHA may be the next step. The results of the PHA will dictate the need.
- The complexity of the system being analyzed. A major system, such as an aircraft or air traffic control center would need separate analyses for different subsystems, then an overall system analysis to integrate, or find the hazards resulting from the interfaces between the different subsystems. On the other hand, an aircraft landing gear system should only need one single hazard analysis.
- The available funding.

There are a number of considerations as to whether or not to perform an O&SHA. If there is a man/machine interface (almost always the case), an O&SHA should be performed. The sources of information for this decision should include the PHA and consultations with human factors personnel knowledgeable of problems associated with operating the equipment. Note that the addition of test equipment to a system can greatly change the system, adding severe hazards. Test procedures, especially those concerning safety critical systems can contribute to accident potential.

### **8.5.7 How Should Multiple Contractors be Handled?**

If more than one contractor or organization will be performing analyses, or if one is subcontracted to another, each contract should be structured to make sure all contractors use the same formats, techniques, and definitions. Otherwise it will be difficult, if not impossible, to correlate the analyses and build higher-level analyses (e.g., SHA from SSHA generated from several contractors). In addition, the analyses should use compatible computer data formats so that interface analyses can be expedited by direct data transfer.

## **8.6 Evaluating a Preliminary Hazard Analysis**

The first analysis to be evaluated is usually the PHA, which is an initial assessment of the anticipated safety problems within a system. The PHA is not a detailed analysis. It covers the broad areas of a system, but leaves the details for future analyses. The results of the PHA provide guidance on which analyses need to be performed as the system design develops, what safety tests need to be performed, and helps define safety design requirements for inclusion in the system's specifications and interface control documents.

The tabular, or matrix, format is the most widely used format for a PHA, primarily because it provides a convenient assessment of the overall risks to a system. The basic tabular format may have entries for hazard sources, such as energy sources (i.e., electrical, pneumatic, mechanical). This PHA would list all known electrical energy sources with their initial hazard assessments, and then recommended corrective action. Another type of tabular format PHA would list key hazards (such as fire and explosion) and identify the known potential contributors for these events.

Some PHAs will be in the form of a logic diagram or Fault Tree Analysis (FTA). These are usually done to identify the major causes of a top undesired event, and are generally not done to a detailed level.

Instead, the details are added during subsequent analyses. A few PHAs will be done in a narrative format. Typically, each paragraph will cover an individual risk, its impact, and proposed resolution. Narrative analyses are preferred for covering a risk in detail, but have the drawback of not having a good tracking system unless tracking numbers are assigned. Narrative PHAs can have provisions for tracking risks, by limiting each single risk and by using the paragraph numbers for tracking.

There are two significant areas of evaluation for PHAs:

- Depth of analysis (i.e., level of detail)
- Proposed resolution of identified risks.

### **8.6.1 What is an Appropriate Depth of Analysis?**

The determination of analysis depth is one of engineering judgment, dependent upon the safety criticality of the system.

### **8.6.2 How Are Risks Resolved?**

All hazards identified in a program must be appropriately closed. Low risk hazard closure can be documented in the hazard analysis. Medium and high risk hazard tracking and closure must be documented in hazard tracking and risk resolution database. All verification and validation activities should be included in the closure documentation. When an analysis is completed, there will be hazards that have not yet been resolved. A tracking system is necessary to assure these risks are not dropped until resolved. The evaluator should ask these questions:

- Does the PHA cover all anticipated hazardous areas?
- Does it establish a baseline for defining future system safety tasks and analyses?
- Does it allow for adequate tracking of risks?
- Are the proposed hazard control actions realistic/implementable?
- Is the analysis limited to evaluation of failures or does it consider faults?

If the answer to any of the questions is "no," then revising or re-performing the PHA may be necessary. One pitfall may be timing. By the time a PHA is completed and submitted, there may be insufficient time to do much with it before the program continues on toward future milestones. In order to obtain the most benefit from the PHA process, the evaluator must work closely with the analyst to ensure the analysis is proceeding correctly. Periodic submittals of an analysis do not always provide enough time to correct inappropriate approaches before program milestones push the program beyond the point where the analysis is beneficial.

## **8.7 Evaluating a Subsystem Hazard Analysis**

The SSHA are the central parts of any system safety program. These are the detailed analyses that identify hazards and recommend solutions. The design details are known and the analyses cover all details that are necessary to identify all possible risks. When evaluating an SSHA, the five points listed for the PHA are applicable for the SSHA.

Most SSHAs are documented in the matrix format, while some are fault trees or other forms of logic diagrams. Fault trees, by themselves, are incomplete and do not directly provide useful information. The utility of fault trees come from the cut and path sets they generate and the analysis of the cut and path sets

for common cause failures and independence of failures/faults. Fault trees are good for analyzing a specific undesired event (e.g., rupture of pressure tank), and can find sequential and simultaneous failures, but are time consuming and expensive. The SSHAs are more detailed than the PHA and are intended to show that the subsystem design meets the safety requirements in the subsystem specifications(s). If hazards are not identified and corrected during the design process, they might not be identified and corrected later when the subsystem designs are frozen and the cost of making a change is significantly increased.

### 8.7.1 What Should be Found in a Subsystem Hazard Analysis?

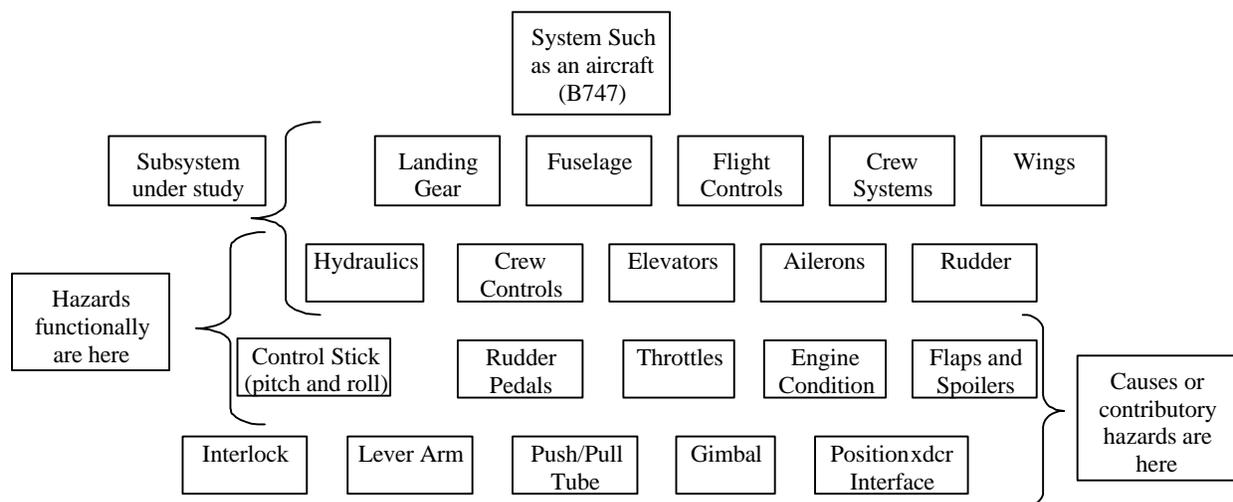
There are many variations, but virtually all of them list key items in tabular form. As a minimum, there should be information for:

- The subsystem, item, or component being analyzed
- Its function
- The hazards and risks
- The severity
- The likelihood of the risk. This likelihood should be based on existing controls.
- Controls (design, safety device, warning device, procedure, and personnel equipment). Reduction of risk (risk severity and probability), if known.
- Risk control verification method(s).
- Recommended corrective actions should include any non-existing method for the control of the risk. Corrective changes to bring the subsystem into compliance with contractual requirements should already have been made.
- Status (open or closed).

### 8.7.2 What Should be the Level of Detail?

Determining the correct level of detail is a matter of judgment. One of the most important aspects of conducting any analysis is knowing when to stop. It is not always practical to analyze all the way to the individual nut and bolt or resistor and capacitor level, which seems like an obvious answer. To illustrate, consider the following failures of an airliner fuel system:

- A fuel crossfeed valve fails partially open. This results in some uncommanded fuel crossfeed (from one tank to another) and usually is not a safety hazard. Therefore, further analysis will not be necessary.
- A fuel jettison (dump) valve fails partially open. This will result in loss of fuel during flight, so a serious hazard is present. Therefore analyzing this valve's failure modes in detail (i.e., operating mechanism, power sources, indicator lights) is appropriate.



**Figure 8-5 Level of Analysis**

Secondary (undeveloped) and environmental failures require judgment too. During most FTAs, these failures usually are not developed (i.e., pursued further) as they may be beyond the scope of the analyses. These failures are labeled by diamond symbols in a fault tree.

### 8.7.3 What Actions Were Taken on Identified Hazards?

The evaluator should focus on recommended actions, actions already taken, and planned follow-up actions. A matrix format provides good visibility of recommend changes of a design or the addition of a procedural step to control a hazard. It makes it simpler to track closing an open item based upon a recommended change. Issues should be kept open until each hazard is positively controlled or until someone documents accepting the hazard. Options include the following alternatives:

- Write the SOW so that the "final" SSHA is delivered when the production baseline design is really established.
- Require the risk to be tracked until it is really closed out.

### 8.7.4 How Are Hazards/Risks Tracked?

There are many ways to track risks and hazards. See Chapter 4: Hazard Tracking and Risk Resolution

### 8.7.5 How Can Other Sources of Data be Used to Complete the Analysis?

The FMEA or FMECA can provide SSHA data. These analyses use a matrix format partially suitable for an SSHA. It lists each component, the component function, types of failure, and the effects of the failures. Most FMEAs also include component failure rate information. An FMEA can be used as a basis for an SSHA, but several factors must be considered:

- Many FMEAs do not list hazard categories (e.g., Category I - catastrophic) necessary for hazard analyses.

- Hazards may not be resolved in a reliability analysis. These analyses emphasize failure effects and rates. They do not always lead to or document corrective action for hazards.
- Failure rate data used for reliability purposes may not be meaningful for safety analyses. Failure rates THAT meet reliability requirements (normally in the .9 or .99 range) may not be adequate to meet safety requirements (often in the .999999 range). In addition, many reliability failures such as a leaking actuator may not be hazardous although in the case it may, if undetected, become a safety issue as degradation continues. Some such as ruptured actuator may be a hazard.
- Sequential or multiple hazards might not be addressed, as well as risks.
- FMEAs address only failures and ignore such safety related faults such as human or procedural errors.

In spite of shortcomings, it is normally more cost effective to expand a reliability analysis to include Hazard Category, Hazard Resolution, and to modify reliability data that is appropriate for safety to be useful as an SSHA than starting from scratch.

An FTA is ideal for focusing on a single undesired event (e.g., failure of engine ignition) but is time consuming and can be expensive. Nevertheless, the FTA should be used for any serious risk whose causes are not immediately obvious (e.g., "O" ring failure) and that needs to be examined in detail because of the concern over the effects of multiple failures and common cause failures. The approach is to list the undesired events, then perform fault trees for each one.

## 8.8 Evaluating a System Hazard Analysis

For the most part, the comments in the previous section on SSHA apply also to the SHA. The SHA analyzes the whole system and integrates SSHAs.

Ideally, the SHA will identify hazards and risks that apply to more than a single subsystem and are not identified in the SSHAs. Most risks of this type result at interfaces between subsystems. For example, an Air Traffic Control (ATC) might have separate SSHAs on the communications and data processing systems. Assume that these SSHAs controlled all known critical and catastrophic hazards. The SHA might identify a previously undiscovered hazard (e.g., incompatible maximum data transfer rates leading to data corruption). The analysis approach is to examine the interfaces between subsystems. In addition, the SHA looks for ways in which safety-critical system level functions can be lost.

Consider, for example, an aircraft anti-skid braking SSHA. It cannot be performed comprehensively if the input information is limited to the landing gear design since there are many other subsystems that interface with the anti-skid subsystem. For instance, the cockpit contains the control panel that turns the anti-skid system on and off and notifies the crew of an anti-skid system failure. This control panel is normally not documented in the landing gear design package and potential could be missed if the analysis focuses only on the landing gear. Other brake system interfaces exist at the hydraulic and electrical power supply subsystems. The SHA is designed to cut across all interfaces.

The system and subsystem definitions are important to the evaluation of a SHA. If the overall system (and its subsystems) are not adequately defined, it is difficult to perform a successful SHA. In most cases, system definition is simple. An aircraft, for example, can be a system. In an aircraft "system" there are many subsystems, such as flight controls and landing gear.

Questions that should be considered by the evaluator:

- Are all the proper interfaces considered? It is obvious that aircraft flight control subsystems interface with hydraulic power subsystems, but not so that they interface with electrical, structural, and the display systems. The evaluator must be familiar with the system being analyzed; if not, the evaluator cannot determine whether or not all interfaces were covered.
- How were the interfaces considered? For example did the analysis consider both mechanical and electrical connections between two subsystems such as structure and hydraulic.

## 8.9 Evaluating an Operating and Support Hazard Analysis

The O&SHA identifies hazards/risks occurring during use of the system. It encompasses operating the system (primarily procedural aspects) and the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, training) that go along with operating the system. Its purpose is to evaluate the effectiveness of procedures in controlling those hazards which were identified as being controlled by procedures, instead of by design, and to ensure that procedures do not introduce new hazards.

Timing of the O&SHA is important. Generally, an Occupational Safety and Health Administration's (OSHA) output (i.e., hazard control) is safety's blessing on "procedures." In most cases, procedures aren't available for review until the system begins initial use or initial test and evaluation. As a result, the O&SHA is typically the last formal analysis to be completed. Actually, the sooner the analysis begins, the better. Even before the system is designed, an O&SHA can be started to identify hazards with the anticipated operation of the system. Ideally, the O&SHA should begin with the formulation of the system and not be completed until sometime after initial test of the system (which may identify additional hazards). This is critical because design and construction of support facilities must begin far before the system is ready for fielding, and all special safety features (e.g., fire suppression systems) must be identified early or the costs to modify the facilities may force program managers and users to accept unnecessary risks.

When evaluating an O&SHA, it is important to insure that the analysis considers not only the normal operation of the system, but abnormal, emergency operation, system installation, maintenance, servicing, storage, and other operations as well. Misuse and emergency operations must also be considered. In other words, if anyone will be doing anything with the system, planned or unplanned, the O&SHA should cover it.

The evaluator should consider the following support aspects of an O&SHA:

- Is there auxiliary equipment (e.g., loading handling, servicing, tools) that are planned to be used with the system?
- Is there a training program? Who will do the training, when, and how? What training aids will be used? Mock-ups and simulators may be needed for complex systems.
- Are there procedures and manuals? These must be reviewed and revised as needed to eliminate or control hazards. This effort requires that the analyst have good working relationships with the organization developing the procedures. If procedures are revised for any reason, the safety analyst needs to be involved.
- Are there procedures for the handling, use, storage, and disposal procedures for hazardous materials?

Human factors are an important consideration for the O&SHA. The O&SHA should be done in concert with the human factors organization since many accidents or accidents can be caused by operator error. Equipment must be user friendly and the O&SHA is an appropriate tool to ensure this takes place. Ideally, the O&SHA should be performed by both by system safety and human factors personnel.

O&SHAs are normally completed and submitted as a single document, typically in a matrix format. For a complex system, this analysis is composed of several separate analyses, such as one for operation and another for maintaining and servicing the system (sometimes called maintenance hazard analysis). The latter might be performed for several different levels of maintenance. Maintenance analyses consider actions such as disconnecting and re-applying power, use of access doors, panels, and hardstands.

The O&SHA should also include expanded operations, i.e., uses of the system for reasonable operations not explicitly specified in the equipment specification. For example, an O&SHA should normally cover the risks associated with aircraft refueling and engine maintenance. There may be some unusual operational conditions (bad weather approaching) where an O&SHA may be necessary where refueling needs to be performed simultaneously with the performance of maintenance. Early test programs are a significant source of operating and support hazards not previously identified. An observant safety monitor might notice that, for example, the proximity of an aircraft fuel vent outlet and hot engines. Corrective action would be to relocate the vent to remove fuel vapors from the vicinity of the hot engines. To benefit from test programs, and identify these "expanded operations", O&SHAs can be required to include data from by contract to use test experience as an input to the analysis.

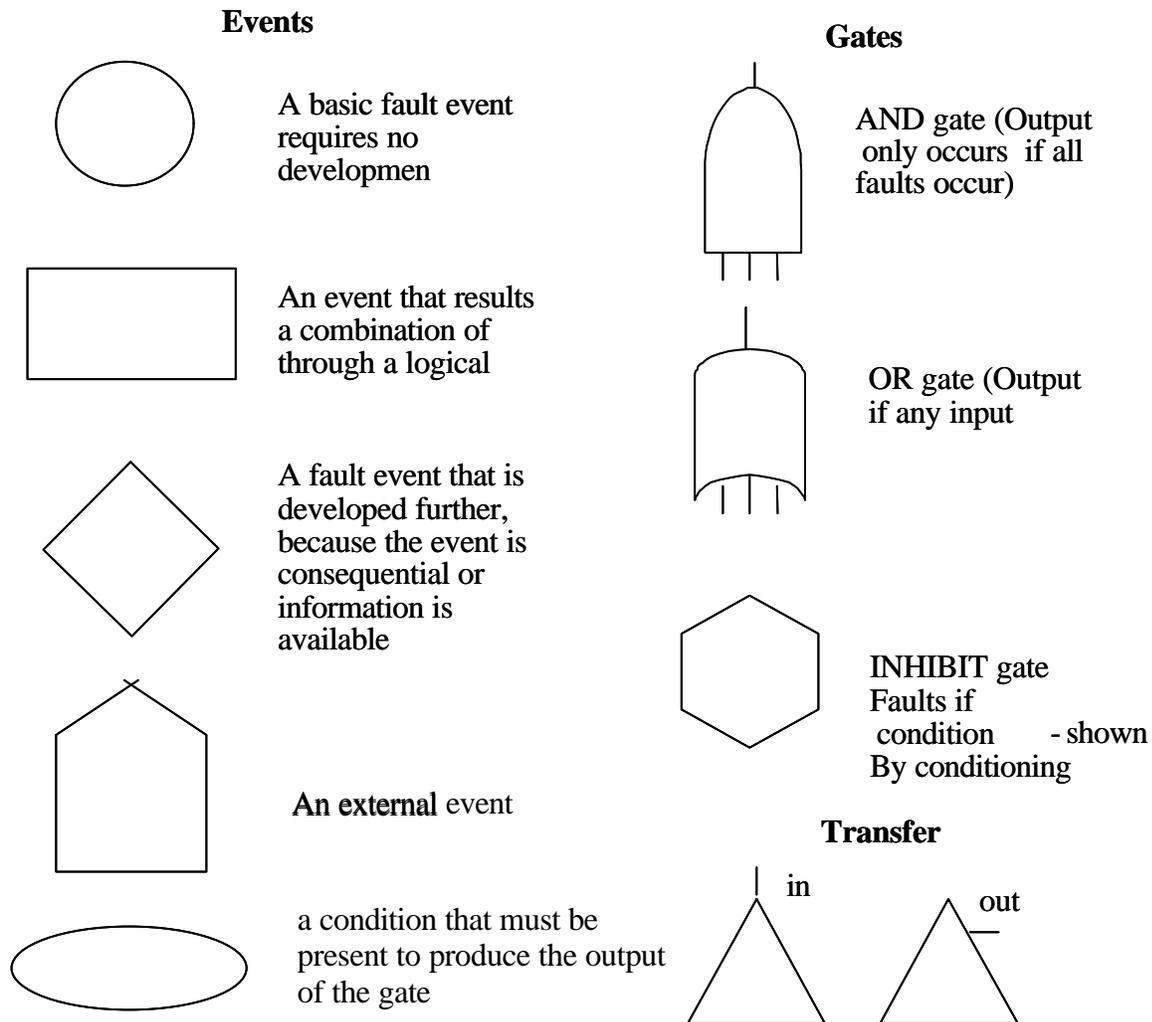
## 8.10 Evaluating a Fault Tree Analysis

FTA is a technique that can be used for any formal program analysis (PHA, SSHA, O&SHA).

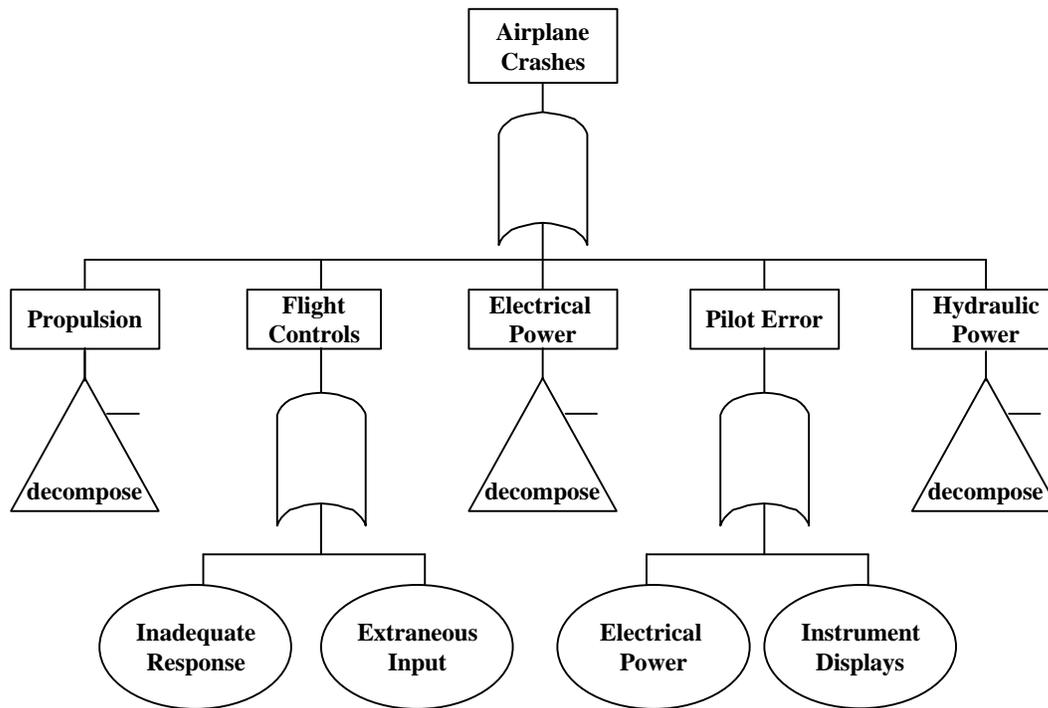
The FTA is one of several deductive logic model techniques, and is by far the most common. The FTA begins with a stated top-level hazardous/undesired event and uses logic diagrams to identify single events and combinations of events that could cause the top event. The logic diagram can then be analyzed to identify single and multiple events that can cause the top event. Probability of occurrence values are assigned to the lowest events in the tree. FTA utilizes Boolean Algebra to determine the probability of occurrence of the top (and intermediate) events. When properly done, the FTA shows all the problem areas and makes the critical areas stand out. The FTA has two drawbacks:

- Depending on the complexity of the system being analyzed, it can be time consuming, and therefore very expensive.
- It does not identify all system hazards, it only identifies failures associated with the predetermined top event being analyzed. For example, an FTA will not identify "ruptured tank" as a hazard in a home water heater. It will show all failures that lead to that event. In other words, the analyst needs to identify all hazards that cannot be identified by use of a fault tree.

The graphic symbols used in a FTA are provided in Figure 8-6.

**Figure 8-6 Fault Tree Symbols**

The first area for evaluation (and probably the most difficult) is the top event. This top event should be very carefully defined and stated. If it is too broad (e.g., aircraft crashes), the resulting FTA will be overly large. On the other hand, if the top event is too narrow (e.g., aircraft crashes due to pitch-down caused by broken bellcrank pin), then the time and expense for the FTA may not yield significant results. The top event should specify the exact hazard and define the limits of the FTA. In this example, a good top event would be "uncommanded aircraft pitch-down," which would center the fault tree around the aircraft flight control system, but would draw in other factors, such as pilot inputs and engine failures. In some cases, a broad top event may be useful to organize and tie together several fault trees. In the example, the top event would be "aircraft crash." This event would be connected to an OR-gate having several detailed top events as shown in Figure 8-5. Some fault trees do not lend themselves to quantification because the factors that tie the occurrence of a second level event to the top event are normally outside the control/influence of the operator (e.g., an aircraft that experiences loss of engine power may or may not crash depending on altitude at which the loss occurs).



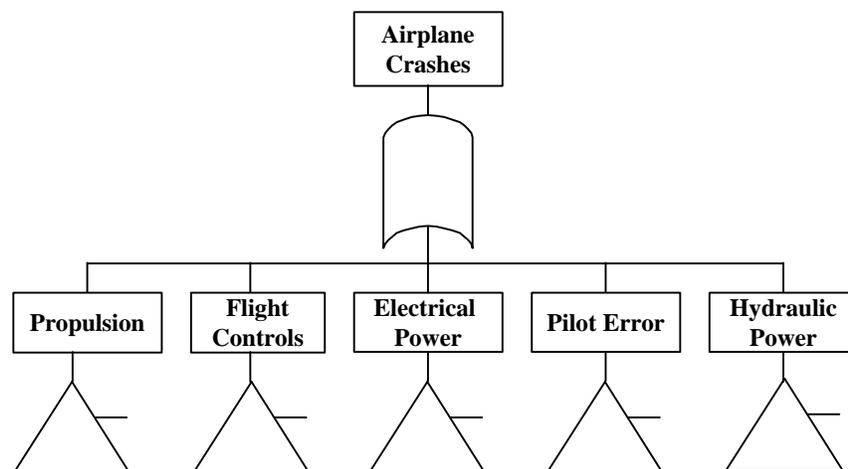
**Figure 8-6: Sample Top Level Fault Tree**

A quick evaluation of a fault tree may be possible by looking at the logic gates. Most fault trees will have a substantial majority of OR gates. If fault trees have too many OR gates, every fault of event may lead to the top event. This may not be the case, but a large majority of OR gates will certainly indicate this.

An evaluator needs to be sure that logic symbols are well defined and understood. If nonstandard symbols are used, they must not get mixed with other symbols.

Check for proper control of transfers. Transfers are reference numbers permitting linking between pages of FTA graphics. Fault trees can be extremely large, requiring the uses of many pages and clear interpage references. Occasionally, a transfer number may be changed during fault tree construction. If the corresponding sub-tree does not have the same transfer number, then improper logic will result.

Cut sets (minimum combinations of events that lead to the top event) need to be evaluated for completeness and accuracy. Establishing the correct number of cuts and their depth is a matter of engineering judgment. The fault tree in Figure 8-6 obscures some of the logic visible in Figure 8-5, preventing identification of necessary corrective action. Figure 8-7 illustrates that event Figure 8-6 was not complete.



**Figure 8-7: More Comprehensive Fault Tree**

Each fault tree should include a list of minimum cut sets. Without this list, it is difficult to identify critical faults or combinations of events. For large or complicated fault trees, a computer is necessary to catch all of the cut sets; it is nearly impossible for a single individual to find all of the cut sets.

For a large fault tree, it may be difficult to determine whether or not the failure paths were completely developed. If the evaluator is not totally familiar with the system, the evaluator may need to rely upon other means. A good indication is the shape of the symbols at the branch bottom. If the symbols are primarily circles (primary failures), the tree is likely to be complete. On the other hand, if many symbols are diamonds (secondary failures or areas needing development), then it is likely the fault tree needs expansion.

Faulty logic is probably the most difficult area to evaluate, unless the faults lie within the gates, which are relatively easy to spot. A gate-to-gate connection shows that the analyst might not completely understand the workings of the system being evaluated. Each gate must lead to a clearly defined specific event, i.e., what is the event and when does it occur? If the event consists of any component failures that can directly cause that event, an OR gate is needed to define the event. If the event does not consist of any component failures, look for an AND gate.

When reviewing an FTA with quantitative hazard probabilities of occurrence, identify the events with relatively large probability of occurrence. They should be discussed in the analysis summaries, probably as primary cause factors.

A large fault tree performed manually is susceptible to errors and omissions. There are many advantages of computer modeling relative to manual analysis (of complex systems):

- Logic errors and event (or branch) duplications can be quickly spotted.
- Cut sets (showing minimum combinations leading to the top event) can be listed.
- Numerical calculations (e.g., event probabilities) can be quickly done.
- A neat, readable, fault tree can be drawn.

### 8.10.1 Success Trees

In some cases it is appropriate to use Success Trees in modeling systems. Success Trees depict the system in its success state. The analyst considers what components or subsystems must work for the system to successfully work. Success Trees are the “inverse” of Fault Trees. For example, see figure 8-7 above. The Success Tree of the above fault tree which is represented as an “or” gate with six inputs would look like an “and” gate with six inputs. The logic is inverted from Failure State to Success State. Since a cut set is the minimum combination of events that lead to the top event, a path set represents the minimum combination of successful events for a successful top event.

### 8.11 Evaluating Quantitative Techniques

Quantitative analysis techniques are used for various purposes, including:

- Establishing overall risk levels (usually specified in terms of risk severity and risk probability).
- Determining areas that need particular attention due to their higher probabilities of a failure.

Overall risk can be expressed by looking at the combination of severity (i.e., what is the worst that can happen?) and probability (i.e., how often will it happen?). This is a realistic and widely accepted approach. A high level hazard can have a low risk of occurrence. For example, an aircraft wing separation in flight is definitely a catastrophic risk, but under normal flight conditions, it is not likely to occur, so the risk is relatively low. At the other end of the spectrum, many jet engines spill a small amount of fuel on the ground during shutdown. This is a relatively low severity with a high probability of occurrence, so the overall risk is low.

Judgment is needed for preparing an analysis and for evaluating it. An analyst might judge a "wheel down" light failure as a Severity 2 or 3 risk because its failure still gives the aircraft "get home" capability with reduced performance. On the other hand, if the wheels fail to lock in a down position and no warning is given, significant damage and injury may result. This scenario is a Severity of 1. Judgment is needed for establishing risk probabilities.

An accurate method for determining risk probabilities is to use component failure rates (e.g., valve xxx will fail to close once in  $6 \times 10^5$  operations). However, there are some pitfalls that need to be considered during evaluation:

- Where did the failure rates come from? Industry data sources? Government data sources? Others? What is their accuracy?
- If the component has a usage history on a prior system, its failure rate on the new system might be the same. However, the newer system might subject the component to a different use cycle or environment, and significantly affect the failure rate.
- For newly developed components, how was the failure rate determined?
- Does the failure rate reflect the hazard failure mode or does it represent all failure modes? For example, if a hazard is caused by capacitor shorting, the failure rate might represent all capacitor failure modes including open and value drift. The result is exaggeration of the probability of occurrence.

FAA System Safety Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks  
December 30, 2000

- System users are comprised of many contributors, human errors, software malfunctions, not just hardware failures.

Any of the above techniques can be used successfully. If more than one contractor or organization will be performing analyses, or if one is subcontracted to another contractually, all of them must be required to use the same definitions of probability levels, or some mismatching will result.

## **Chapter 9: Analysis Techniques**

<b>9.0 ANALYSIS TECHNIQUES.....</b>	<b>2</b>
<b>9.1 INTRODUCTION .....</b>	<b>2</b>
<b>9.2 FAULT HAZARD ANALYSIS .....</b>	<b>2</b>
<b>9.3 FAULT TREE ANALYSIS .....</b>	<b>4</b>
<b>9.4 COMMON CAUSE FAILURE ANALYSIS.....</b>	<b>7</b>
<b>9.5 SNEAK CIRCUIT ANALYSIS.....</b>	<b>8</b>
<b>9.6 ENERGY TRACE .....</b>	<b>10</b>
<b>9.7 FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS (FMECA) .....</b>	<b>13</b>
<b>9.8 OTHER METHODOLOGIES.....</b>	<b>14</b>

## 9.0 Analysis Techniques

### 9.1 Introduction

Many analysis tools are available to perform hazard analyses for each program. These range from the relatively simple to the complex. In general, however, they fall into two categories:

Event, e.g., What would cause an airplane crash or what will cause air space encroachment?

Consequence, e.g., What could happen if the pilot has too many tasks to do during taxi, or what could happen if a pump motor shaft bearing froze?

This chapter describes characteristics of many popular analysis approaches and, in some cases, provides procedures and examples of these techniques. The analysis techniques covered in this chapter are the following:

Fault Hazard  
Fault Tree  
Common Cause Failure  
Sneak Circuit  
Energy Trace  
Failure Modes, Effects, and Criticality Analysis (FMECA)

### 9.2 Fault Hazard Analysis

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

What can fail?  
How it can fail?  
How frequently will it fail?  
What are the effects of the failure?

How important, from a safety viewpoint, are the effects of the failure?

A Fault Hazard Analysis can be used for a number of purposes:

Aid in system design concept selection  
Support "functional mechanizing" of hardware  
"Design out" critical safety failure modes  
Assist in operational planning  
Provide inputs to management risk control efforts

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

To conduct a fault hazard analysis, it is necessary to know and understand certain system characteristics:

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

The procedural steps are:

1. The system is divided into modules (usually functional or partitioning) that can be handled effectively.
2. Functional diagrams, schematics, and drawings for the system and each subsystem are then reviewed to determine their interrelationships and the interrelationships of the component subassemblies. This review may be done by the preparation and use of block diagrams.
3. For analyses performed down to the component level, a complete component list with the specific function of each component is prepared for each module as it is to be analyzed. For those cases when the analyses are to be performed at the functional or partitioning level, this list is for the lowest analysis level.
4. Operational and environmental stresses affecting the system are reviewed for adverse effects on the system or its components.
5. Significant failure mechanisms that could occur and affect components are determined from analysis of the engineering drawings and functional diagrams. Effects of subsystem failures are then considered.
6. The failure modes of individual components that would lead to the various possible failure mechanisms of the subsystem are then identified. Basically, it is the failure of the component that produces the failure of the entire system. However, since some components may have more than

one failure mode, each mode must be analyzed for its effect on the assembly and then on the subsystem. This may be accomplished by tabulating all failure modes and listing the effects of each, e.g. a resistor that might fail open or short, high or low). An understanding of physics of failure is necessary. For example, most resistors cannot fail in a shorted mode. If the analyst does not understand this, considerable effort may be wasted on attempting to control a nonrealistic hazard.

7. All conditions that affect a component or assembly should be listed to indicate whether there are special periods of operation, stress, personnel action, or combinations of events that would increase the probabilities of failure or damage.
8. The risk category should be assigned.
9. Preventative or corrective measures to eliminate or control the risks are listed.
10. Initial probability rates are entered. These are "best judgments" and are revised as the design process goes on. Care must be taken to make sure that the probability represents that of the particular failure mode being evaluated. A single failure rate is often provided to cover all of a component's failure modes rather than separate ones for each. For example, MIL-HBK-217, a common source of failure rates, does not provide a failure rate for capacitor shorts, another for opens, and a third for changes in value. It simply provides a single failure for each operating condition (temperature, electrical stress, and so forth).
11. A preliminary criticality analysis may be performed as a final step.

The Fault Hazard analysis has some serious limitations. They include:

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

### 9.3 Fault Tree Analysis

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

This tool is used by the professional safety and reliability community to both prevent and resolve hazards and failures. Both qualitative and quantitative methods are used to identify areas in a system that are most critical to safe operation. Either approach is effective. The output is a graphical presentation providing

technical and administrative personnel with a map of "failure or hazard" paths. FTA symbols may be found in Figure 8- 5. The reviewer and the analyst must develop an insight into system behavior, particularly those aspects that might lead to the hazard under investigation.

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

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

1. Assume a system state and identify and clearly document state the top level undesired event(s). This is often accomplished by using the PHL or PHA. Alternatively, design documentation such as schematics, flow diagrams, level B & C documentation may reviewed.
2. Develop the upper levels of the trees via a top down process. That is determine the intermediate failures and combinations of failures or events that are the minimum to cause the next higher level event to occur. The logical relationships are graphically generated as described below using standardized FTA logic symbols.
3. Continue the top down process until the root causes for each branch is identified and/or until further decomposition is not considered necessary.
4. Assign probabilities of failure to the lowest level event in each branch of the tree. This may be through predictions, allocations, or historical data.
5. Establish a Boolean equation for the tree using Boolean logic and evaluate the probability of the undesired top level event.
6. Compare to the system level requirement. If it the requirement is not met, implement corrective action. Corrective actions vary from redesign to analysis refinement.

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

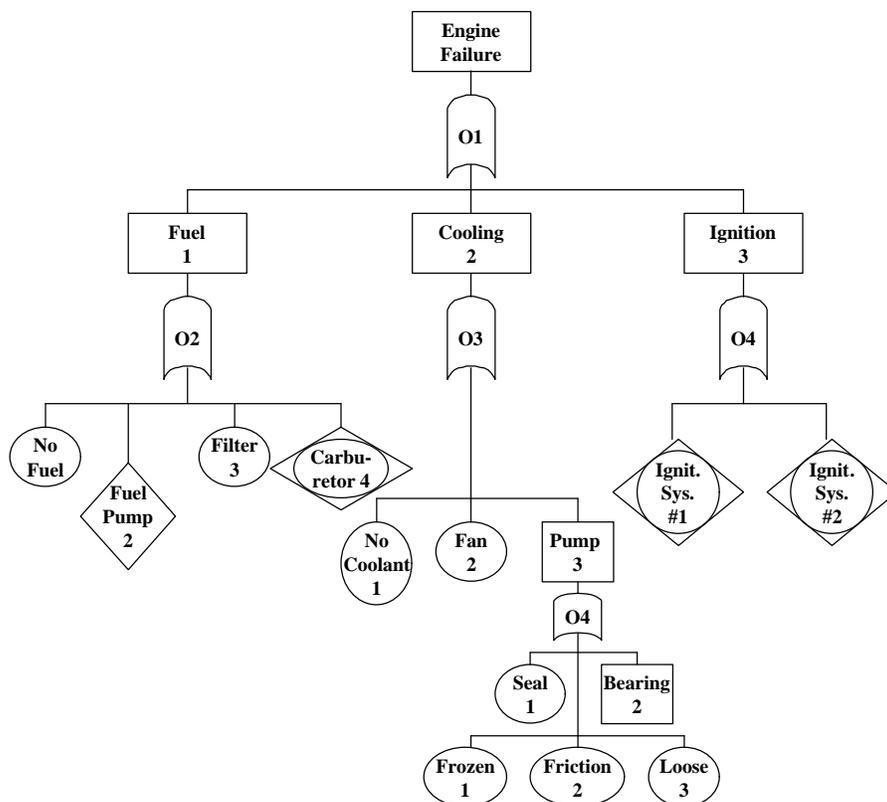


Figure 9-1: Sample Engine Failure Fault Tree

Standardized symbology is used and is shown in Figure 8-5. A non-technical person can, with minimal training, determine from the fault tree, the combination and alternatives of events that may lead to failure or a hazard. Figure 9-1 is a sample fault tree for an aircraft engine failure. In this sample there are three possible causes of engine failure: fuel flow, coolant, or ignition failure. The alternatives and combinations leading to any of these conditions may also be determined by inspection of the FTA.

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

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

In the aircraft engine example, a coolant pump failure may be caused by a seal failure. This level was not further developed. The example does not include a "house." That symbol illustrates a normal (versus failure) event. If the hazard were "unintentional stowing of the landing gear", a normal condition for the hazard would be the presence of electrical power.

FTA symbols can depict all aspects of NAS events. The example reflects a hardware based problem. More typically, software (incorrect assumptions or boundary conditions), human factors (inadequate displays), and environment conditions (ice) are also included, as appropriate.

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

Events are linked together by "AND" and "OR" logic gates. The latter is used in the example for both fuel flow and carburetor failures. For example, fuel flow failures can be caused by either a failed fuel pump or a blocked fuel filter. An "AND" gate is used for the ignition failure illustrating that the ignition systems are redundant. That is both must fail for the engine to fail. These logic gates are called Boolean gates or operators. Boolean algebra is used for the quantitative approach. The "AND" and "OR" gates are numbered sequentially A# or O# respectively in Figure 9-1.

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

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

In addition to evaluating the significance of a risk and the likelihood of occurrence, FTAs facilitate presentations of the hazards, causes, and discussions of safety issues. They can contribute to the generation of the Master Minimum Equipment List (MMEL).

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

#### **9.4 Common Cause Failure Analysis**

Common Cause Failure Analysis (CCFA) is an extension of FTA to identify "coupling factors" that can cause component failures to be potentially interdependent. Primary events of minimal cut sets from the

FTA are examined through the development of matrices to determine if failures are linked to some common cause relating to environment, location, secondary causes, human error, or quality control. A cut set is a set of basic events (e.g., a set of component failures) whose occurrence causes the system to fail. A *minimum cut set* is one that has been reduced to eliminate all redundant "fault paths." CCFA provides a better understanding of the interdependent relationship between FTA events and their causes. It analyzes safety systems for "real" redundancy. This analysis provides additional insight into system failures after development of a detailed FTA when data on components, physical layout, operators, and inspectors are available.

The procedural steps for a CCA are:

1. Establish "Critical Tree Groups." This often accomplished utilizing FMECAs, FTA, and Sneak Circuit Analyses (SCA) to limit the scope of analysis to the critical components or functions. THE FTA identifies critical functions, the FMECA critical components, and the SCA "hidden" inter-relationships.
2. Identify common components within the groups of "1." above. These might be redundant processors sharing a common power source or redundant hydraulic lines/systems being fed by a common hydraulic pump. Alternatively, it might be totally redundant hydraulic lines placed physically adjacent to each other.
3. Identify credible failure modes such as shorts, fluid leaks, defective operational procedures, etc.
4. Identify common cause credible failure modes. This requires understanding of the system/hardware involved, the use of "lessons learned", and historical data.
5. Summarize analysis results including identification of corrective action.

## 9.5 Sneak Circuit Analysis

Sneak Circuit Analysis (SCA) is a unique method of evaluating electrical circuits. SCA employs recognition of topological patterns that are characteristic of all circuits and systems. The purpose of this analysis technique is to uncover latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed. The process is convert schematic diagrams to topographical drawings and search for sneak circuits. This is a labor intensive process best performed by special purpose software. Figure 9-2 shows an automobile circuit that contains a sneak circuit. The sneak path is through the directional switch and flasher, the brake light switch, and the radio.

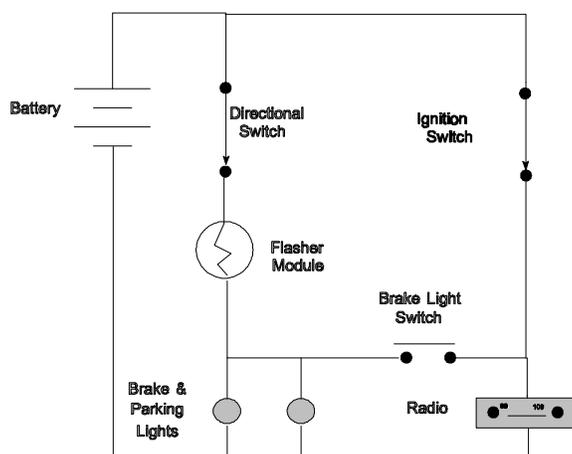


Figure 9-2: A Sneak Circuit

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

The fact that the circuits can be broken down into the patterns shown allows a series of clues to be applied for recognition of possible sneak circuit conditions. These clues help to identify combinations of controls and loads that are involved in all types of sneak circuits. Analysis of the node-topographs for sneak circuit conditions is done systematically with the application of sneak circuit clues to one node at a time. When all of the clues that apply to a particular pattern have been considered, it is assured that all possible sneak circuits that could result from that portion of the circuit have been identified. The clues help the analyst to determine the different ways a given circuit pattern can produce a "sneak." Figure 9-3 is a node topograph equivalent of Figure 9-2

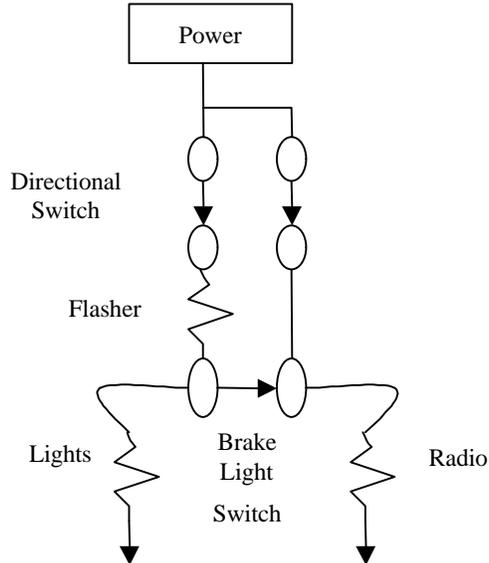


Figure 9-3: Topical Node Representation of Sneak Circuit

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

<p>Sneak Paths - allow current to flow along an unsuspected route</p> <p>Sneak Timing - causes functions to be inhibited or to occur unexpectedly</p> <p>Sneak Labels - cause incorrect stimuli to be initiated</p> <p>Sneak Indicators - cause ambiguous or false displays</p>
---

In addition to the identification of sneak circuits, results include disclosure of data errors and areas of design concern. Data errors are identified and reported incrementally on Drawing Error Reports from the time of data receipt through the analysis period. These errors generally consist of lack of agreement between or within input documents. Conditions of design concern are primarily identified during the network tree analysis. Design concern conditions include:

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

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

## 9.6 Energy Trace

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

The purpose of energy trace analysis is to ensure that all hazards and their immediate causes are identified. Once the hazards and their causes are identified, they can be used as top events in a fault tree or used to verify the completeness of a fault hazard analysis. Consequently, the energy trace analysis method complements but does not replace other analyses, such as fault trees, sneak circuit analyses, event trees, and FMEAs.

Identification of energy sources and energy transfer processes is the key element in the energy source analysis procedure. Once sources of energy have been identified, the analyst eliminates or controls the hazard using the system safety precedence described in Chapter 3, Table 3-1.

These analyses point out potential unwanted conditions that could conceivably happen. Each condition is evaluated further to assess its hazard potential. The analysis and control procedures discussed throughout this handbook are applied to the identified hazards.

Fourteen energy trace analysis procedural steps are:

1. Identify the resource being protected (personnel or equipment) to guide the direction of the analysis toward the identification of only those conditions (i.e., hazards) that would be critical or catastrophic from a mission viewpoint.
2. Identify system and subsystems, and safety critical components.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

3. Identify the operational phase(s), such as preflight, taxi, takeoff, cruise, landing, that each system/subsystem/component will experience. It is often desirable to report results of hazard analyses for each separate operational phase.
4. Identify the operating states for the subsystems/components (e.g., on/off, pressurized, hot, cooled) during each operational phase.
5. Identify the energy sources or transfer modes that are associated with each subsystem and each operating state. A list of general energy source types and energy transfer mechanisms is presented in Figure 9-4.
6. Identify the energy release mechanism for each energy source (released or transferred in an uncontrolled/unplanned manner). It is possible that a normal (i.e., as designed) energy release could interact adversely with other components in a manner not previously or adequately considered.
7. Review a generic threat checklist for each component and energy source or transfer mode. Experience has shown that certain threats are associated with specific energy sources and components.
8. Identify causal factors associated with each energy release mechanism. A hazard causal factor may have subordinate or underlying causal factors associated with it. For instance, excessive stress may be a "top level" factor. The excessive stress may, in turn, be caused by secondary factors such as inadequate design, material flaws, poor quality welds, excessive loads due to pressure or structural bending. By systematically evaluating such causal factors, an analyst may identify potential design or operating deficiencies that could lead to hazardous conditions. Causal factors are identified independent of the probability of occurrence of the factor; the main question to be answered is: Can the causal factor occur or exist?
9. Identify the potential accident that could result from energy released by a particular release mechanism.
10. Define the hazardous consequences that could result given the accident specified in the previous step.
11. Evaluate the hazard category (i.e., critical, catastrophic, or other) associated with the potential accident.
12. Identify the specific hazard associated with the component and the energy source or transfer mode relative to the resource being protected.
13. Recommend actions to control the hazardous conditions.
14. Specify verification procedures to assure that the controls have been implemented adequately.



size), immunizing against disease, or warming up by exercise

And by establishing contingency response such as early detection of energy release, first aid, emergency showers, general disaster plans, recovery of system operation procedures.

### 9.7 Failure Modes, Effects, and Criticality Analysis (FMECA)

FMECAs and FMEAs are important reliability programs tools that provide data usable by the SSP. The performance of an FMEA is the first step in generating the FMECA. Both types of analyses can serve as a final product depending on the situation. An FMECA is generated from an FMEA by adding a criticality figure of merit. These analyses are performed for reliability, safety, and supportability information. The FMECA version is more commonly used and is more suited for hazard control.

Hazard analyses typically use a top down analysis methodology (e.g., Fault Tree). The approach first identifies specific hazards and isolates all possible (or probable) causes. The FMEA/FMECA may be performed either top down or bottoms-up, usually the latter.

Hazard analyses consider failures, operating procedures, human factors, and transient conditions in the list of hazard causes. The FMECA is more limited. It only considers failures (hardware and software). It is generated from a different set of questions than the HA: “If this fails, what is the impact on the system? Can I detect it? Will it cause anything else to fail?” If so, the induced failure is called a secondary failure.

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

The procedural approach to generating an FMEA is comparable to that of the Fault Hazard Analysis. The first step is to list all components or low level functions. Then, by examining system block diagrams, schematics, etc., the function of each component is identified. Next, all reasonably possible failure modes of the lowest “component” being analyzed are identified. Using a coolant pump bearing as an example (see Figure 9-5), they might include frozen, high friction, or too much play. For each identified failure mode, the effect at the local level, an intermediate level, and the top system level are recorded. A local effect might be “the shaft won’t turn”, the intermediate “pump won’t circulate coolant”, and the system level “engine overheat and fail”. At this point in the analysis, the FMEA might identify a hazard.

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

significance of the failure is less than if the engine depends on a single pump. The severity categories used for the hazard analysis can be used as the severity class in the FMEA. A comments column is usually added to the FMEA to provide additional information that might assist the reviewer in understanding any FMEA column.

Adding a criticality figure of merit is needed to generate the FMECA, shown in Figure 9-5, from the FMEA. Assigning severity levels can not be performed without first identifying the purpose of the FMECA. For example, a component with a high failure rate would have a high severity factor for a reliability analysis: a long lead time or expensive part would be more important in a supportability analysis. Neither may be significant from a safety perspective. Therefore, a safety analysis requires a unique criticality index or equation. The assignment of a criticality index is called a criticality analysis. The Index is a mathematical combination of severity and probability of occurrence (likelihood of occurrence).

**Figure 9-5: Sample Failure Modes, Effects, and Criticality Analysis**

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

Severity Class: I-Catastrophic to IV-Incidental

Not shown are columns that may be added including frequency class, interfaces, and comments.

The FMECA and the hazard analyses provided some redundant information but more importantly some complementary information. The HA considers human factors and systems interface problems, the FMECA does not. The FMECA, however, is not more likely to identify hazards caused by component or software module failure than the HA, which considers compensating and fault detection features. These are all important safety data.

## 9.8 Other Methodologies

The System Safety Society has developed a System Safety Analysis Handbook.<sup>1</sup> The handbook describes in summary manner 106 safety methodologies and techniques that are employed by modern system safety practitioners. The following table presents the applicable methods and techniques that are appropriate for use within the FAA. The method or technique is listed, along with a brief summary, applicability and use. Further research and reference may be needed to apply a new method or technique. A reference is provided

<sup>1</sup> Stephens, Richard, A. and Talso, Warner, System safety Analysis Handbook: A Source Book for Safety Practitioners, System Safety Society, 2<sup>nd</sup> Edition, August 1999.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

for additional readings in Appendix C. The FAA's Office of System Safety can provide instruction and assistance in the applications of the listed methods and techniques.

**Table 9-1: Analysis Methods and Techniques**

No.	Methods and/or Techniques	Summary	Applicability and Use
1	Accident Analysis	The purpose of the Accident Analysis is to evaluate the effect of scenarios that develop into credible and incredible accidents.	Any accident or incident should be formally investigated to determine the contributors of the unplanned event. Many methods and techniques are applied.
2	Action Error Analysis	Action Error Analysis analyzes interactions between machine and humans. It is used to study the consequences of potential human errors in task execution related to directing automated functions.	Any automated interface between a human and automated process can be evaluated, such as pilot / cockpit controls, or controller / display, maintainer / equipment interactions.
3	Barrier Analysis	Barrier Analysis method is implemented by identifying energy flow (s) that may be hazardous and then identifying or developing the barriers that must be in place to prevent the unwanted energy flow from damaging equipment, and/or causing system damage, and/or injury.	Any system is comprised of energy, should this energy become uncontrolled accidents can result.  Barrier Analysis is an appropriate qualitative tool for systems analysis, safety reviews, and accident analysis.
4	Bent Pin Analysis	Bent Pin Analysis evaluates the effects should connectors short as a result of bent pins and mating or demating of connectors.	Any connector has the potential for bent pins to occur. Connector shorts can cause system malfunctions, anomalous operations, and other risks.
5	Cable Failure Matrix Analysis	Cable Failure Matrix Analysis identifies the risks associated with any failure condition related to cable design, routing, protection, and securing.	Should cables become damaged system malfunctions can occur. Less than adequate design of cables can result in faults, failures, and anomalies, which can result in contributory hazards and accidents.
6	Cause-Consequence Analysis	Cause-Consequence Analysis combines bottom up and top down analysis techniques of Event Trees and Fault Trees. The result is the development of potential complex accident scenarios.	Cause-Consequence Analysis is a good tool when complex system risks are evaluated.
7	Change Analysis	Change Analysis examines the effects of modifications from a starting point or baseline.	Any change to a system, equipment procedure, or operation should be evaluated from a system safety

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
			<p>view.</p> <p>Cause-Consequence Analysis is also used during accident/incident investigation.</p>
8	Checklist Analysis	<p>Checklist Analysis is a comparison to criteria, or a device to be used as a memory jogger. The analyst uses a list to identify items such as hazards, design or operational deficiencies.</p>	<p>Checklist Analysis can be used in any type of safety analysis, safety review, inspection, survey, or observation.</p> <p>Checklists enable a systematic, step by step process. They can provide formal documentation, instruction, and guidance.</p>
9	Common Cause Analysis	<p>Common Cause Analysis will identify common failures or common events that eliminate redundancy in a system, operation, or procedure.</p>	<p>Common causes are present in almost any system where there is any commonality, such as human interface, common task, and common designs, anything that has a redundancy, from a part, component, sub-system or system.</p>
10	Comparison-To-Criteria	<p>The purpose of Comparison-To-Criteria is to provide a formal and structured format that identifies safety requirements.</p>	<p>Comparison-To-Criteria is a listing of safety criteria that could be pertinent to any FAA system. This technique can be considered in a Requirements Cross-Check Analysis.</p> <p>Applicable safety-related requirements such as OSHA, NFPA, ANSI, are reviewed against an existing system or facility.</p>
11	Confined Space Safety	<p>The purpose of this analysis technique is to provide a systematic examination of confined space risks.</p>	<p>Any confined areas where there may be a hazardous atmosphere, toxic fume, or gas, the lack of oxygen, could present risks.</p> <p>Confined Space Safety should be considered at tank farms, fuel storage areas, manholes, transformer vaults, confined electrical spaces, race-ways.</p>
12	Contingency	<p>Contingency Analysis is a method of</p>	<p>Contingency Analysis should be</p>

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
	Analysis	minimizing risk in the event of an emergency. Potential accidents are identified and the adequacies of emergency measures are evaluated.	conducted for any system, procedure, task or operation where there is the potential for harm. Contingency Analysis lists the potential accident scenario and the steps taken to minimize the situation. It is an excellent formal training and reference tool.
13	Control Rating Code	Control Rating Code is a generally applicable system safety-based procedure used to produce consistent safety effectiveness ratings of candidate actions intended to control hazards found during analysis or accident analysis. Its purpose is to control recommendation quality, apply accepted safety principles, and priorities hazard controls.	Control Rating Code can be applied when there are many hazard control options available.  The technique can be applied toward any safe operating procedure, or design hazard control.
14	Critical Incident Technique <sup>2</sup>	This is a method of identifying errors and unsafe conditions that contribute to both potential and actual accidents or incidents within a given population by means of a stratified random sample of participant-observers selected from within the population.	Operational personnel can collect information on potential or past errors or unsafe conditions. Hazard controls are then developed to minimize the potential error or unsafe condition.  This technique can be universally applied in any operational environment.
15	Criticality Analysis	The purpose of the Criticality Analysis is to rank each failure mode identified in a Failure Modes and Effect Analysis.	The technique is applicable to all systems, processes, procedures, and their elements.  Once critical failures are identified they can be equated to hazards and risks. Designs can then be applied to eliminate the critical failure thereby, eliminating the hazard and associated accident risk.

<sup>2</sup> Tarrents, William, E. The Measurement of Safety Performance, Garland STPM Press, 1980.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
16	Critical Path Analysis	Critical Path Analysis identifies critical paths in a Program Evaluation graphical network. Simply it is a graph consisting of symbology and nomenclature defining tasks and activities. The critical path in a network is the longest time path between the beginning and end events.	This technique is applied in support of large system safety programs, when extensive system safety – related tasks are required.
17	Damage Modes and Effects Analysis	Damage Modes and Effects Analysis evaluates the damage potential as a result of an accident caused by <b>hazards and related failures.</b>	Risks can be minimized and their associated hazards eliminated by evaluating damage progression and severity.
18	Deactivation Safety Analysis	This analysis identifies safety concerns associated with facilities that are decommissioned/closed.	<p>The deactivation process involves placing a facility into a safe mode and stable condition that can be monitored if needed.</p> <p>Deactivation may include removal of hazardous materials, chemical contamination, spill cleanup.</p>
19	Electromagnetic Compatibility Analysis	The analysis is conducted to minimize/prevent accidental or unauthorized operation of safety-critical functions within a system.	<p>Adverse electromagnetic environmental effects can occur when there is any electromagnetic field.</p> <p>Electrical disturbances may also be generated within an electrical system from transients accompanying the sudden operations of solenoids, switches, choppers, and other electrical devices, Radar, Radio Transmission, transformers.</p>
20	Energy Analysis	The energy analysis is a means of conducting a system safety evaluation of a system that looks at the “energetics” of the system.	<p>The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionizing or non-ionizing radiation, chemical, and thermal.)</p> <p>This technique is usually conducted</p>

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
			in conjunction with Barrier Analysis.
21	Energy Trace and Barrier Analysis	<p>Energy Trace and Barrier Analysis is similar to Energy Analysis and Barrier Analysis.</p> <p>The analysis can produce a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm.</p>	The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionizing or non-ionizing radiation, chemical, and thermal.)
22	Energy Trace Checklist	<p>Similar to Energy Trace and Barrier Analysis, Energy Analysis and Barrier Analysis.</p> <p>The analysis aids in the identification of hazards associated with energetics within a system, by use of a specifically designed checklist.</p>	<p>The analysis could be used when conducting evaluation and surveys for hazard identification associated with all forms of energy.</p> <p>The use of a checklist can provide a systematic way of collecting information on many similar exposures.</p>
23	Environmental Risk Analysis	The analysis is conducted to assess the risk of environmental noncompliance that may result in hazards and associated risks.	The analysis is conducted for any system that uses or produces toxic hazardous materials that could cause harm to people and the environment.
24	Event and Casual Factor Charting	Event and Casual Factor Charting utilizes a block diagram to depict cause and effect.	The technique is effective for solving complicated problems because it provides a means to organize the data, provides a summary of what is known and unknown about the event, and results in a detailed sequence of facts and activities.
25	Event Tree Analysis	An Event Tree models the sequence of events that results from a single initiating event.	<p>The tool can be used to organize, characterize, and quantify potential accidents in a methodical manner.</p> <p>The analysis is accomplished by selecting initiating events, both desired and undesired, and develop their consequences through consideration of system/component failure-and-success alternatives.</p>
26	Explosives Safety	This method enables the safety	Explosives Safety Analysis can be

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
	Analysis	professional to identify and evaluate explosive hazards associated with facilities or operations.	used to identify hazards and risks related to any explosive potential, i.e. fuel storage, compressed gases, transformers, batteries.
27	External Events Analysis	<p>The purpose of External Events Analysis is to focus attention on those adverse events that are outside of the system under study.</p> <p>It is to further hypothesize the range of events that may have an effect on the system being examined.</p>	The occurrence of an external event such as an earthquake is evaluated and affects on structures, systems, and components in a facility are analyzed.
28	Facility System Safety Analysis	System safety analysis techniques are applied to facilities and its operations.	Facilities are analyzed to identify hazards and potential accidents associated with the facility and systems, components, equipment, or structures.
29	Failure Mode and Effects Analysis (FMEA)	The FMEA is a reliability analysis that is a bottom up approach to evaluate failures within a system.	Any electrical, electronics, avionics, or hardware system, sub-system can be analyzed to identify failures and failure modes.
30	Failure Mode and Effects Criticality Analysis (FMECA)	<p>Same as above with the addition of Criticality.</p> <p>Failure modes are classified as to their criticality.</p>	As above.
31	Fault Hazard Analysis	<p>A system safety technique that is an offshoot from FMEA.</p> <p>Similar to FMEA above however failures that could present hazards are evaluated.</p> <p>Hazards and failure are not the same. Hazards are the potential for harm, they are unsafe acts or conditions. When a failure results in an unsafe condition it is considered a hazard. Many hazards contribute to a particular risk.</p>	Any electrical, electronics, avionics, or hardware system, sub-system can be analyzed to identify failures, malfunctions, anomalies, faults, that can result is hazards.
32	Fault Isolation Methodology	<p>The method is used to determine and locate faults in large-scale ground based systems.</p> <p>Examples of specific methods applied are; Half-Step Search, Sequential Removal/Replacement, Mass</p>	Determine faults in any large-scale ground based system that is computer controlled.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
		replacement, and Lambda Search, and Point of Maximum Signal Concentration.	
33	Fault Tree Analysis	A Fault Tree Analysis is a graphical design technique that could provide an alternative to block diagrams. It is a top-down, deductive approach structured in terms of events. Faults are modeled in term of failures, anomalies, malfunctions, and human errors.	Any complex procedure, task, system, can be analyzed deductively.
34	Fire Hazards Analysis	Fire Hazards Analysis is applied to evaluate the risks associated with fire exposures. There are several fire-hazard analysis techniques, i.e. load analysis, hazard inventory, fire spread, scenario method.	Any fire risk can be evaluated.
35	Flow Analysis	The analysis evaluates confined or unconfined flow of fluids or energy, intentional or unintentional, from one component/sub-system/ system to another.	The technique is applicable to all systems which transport or which control the flow of fluids or energy.
36	Hazard Analysis	Generic and specialty techniques to identify hazards. Generally, and formal or informal study, evaluation, or analysis to identify hazards.	Multi-use technique to identify hazards within any system, sub-system, operation, task or procedure.
37	Hazard Mode Effects Analysis	Method of establishing and comparing potential effects of hazards with applicable design criteria.	Multi-use technique
38	Hardware/Software Safety Analysis	The analysis evaluates the interface between hardware and software to identify hazards within the interface.	Any complex system with hardware and software.
39	Health hazard Assessment	<p>The method is used to identify health hazards and risks associated within any system, sub-system, operation, task or procedure.</p> <p>The method evaluates routine, planned, or unplanned use and releases of hazardous materials or physical agents.</p>	The technique is applicable to all systems which transport, handle, transfer, use, or dispose of hazardous materials of physical agents.
40	Human Error	Human Error Analysis is a method to	Human Error Analysis is

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
	Analysis	<p>evaluate the human interface and error potential within the human /system and to determine human-error-related hazards.</p> <p>Many techniques can be applied in this human factors evaluation.</p> <p>Contributory hazards are the result of unsafe acts such as errors in design, procedures, and tasks.</p>	appropriate to evaluate any human/machine interface.
41	Human Factors Analysis	<p>Human Factors Analysis represents an entire discipline that considers the human engineering aspects of design.</p> <p>There are many methods and techniques to formally and informally consider the human engineering interface of the system.</p> <p>There are specialty considerations such as ergonomics, bio-machines, anthropometrics.</p>	<p>Human Factors Analysis is appropriate for all situations where the human interfaces with the system and human-related hazards and risks are present.</p> <p>The human is considered a main sub-system.</p>
42	Human Reliability Analysis	The purpose of the Human Reliability Analysis is to assess factors that may impact human reliability in the operation of the system.	The analysis is appropriate where reliable human performance is necessary for the success of the human-machine systems.
43	Interface Analysis	<p>The analysis is used to identify hazards due to interface incompatibilities.</p> <p>The methodology entails seeking those physical and functional incompatibilities between adjacent, interconnected, or interacting elements of a system which, if allowed to persist under all conditions of operation, would generate risks.</p>	<p>Interface Analysis is applicable to all systems.</p> <p>All interfaces should be investigated; machine-software, environment-human, environment-machine, human-human, machine-machine, etc.</p>
44	Job Safety Analysis	This technique is used to assess the various ways a task may be performed so that the most efficient and appropriate way to do a task is selected.	Job Safety Analysis can be applied to evaluate any job, task, human function, or operation.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
		<p>Each job is broken down into tasks, or steps, and hazards associated with each task or step are identified. Controls are then defined to decrease the risk associated with the particular hazards.</p>	
45	Laser Safety Analysis	This analysis enables the evaluation of the use of Lasers from a safety view.	The analysis is appropriate for any laser operation, i.e. construction, experimentation, and testing.
46	Management Oversight and Risk Tree (MORT)	MORT technique is used to systematically analyze an accident in order to examine and determine detailed information about the process and accident contributors.	This is an accident investigation technique that can be applied to analyze any accident.
47	Materials Compatibility Analysis	<p>Materials Compatibility Analysis provides an assessment of materials utilized within a particular design.</p> <p>Any potential degradation that can occur due to material incompatibility is evaluated.</p>	Materials Compatibility Analysis is universally appropriate throughout most systems.
48	Maximum Credible Accident/Worst Case	The technique is to determine the upper bounds on a potential environment without regard to the probability of occurrence of the particular potential accident.	<p>Similar to Scenario Analysis, this technique is used to conduct a System Hazard Analysis.</p> <p>The technique is universally appropriate.</p>
49	Modeling; Simulation	<p>There are many forms of modeling techniques that are used in system engineering.</p> <p>Failures, events, flows, functions, energy forms, random variables, hardware configuration, accident sequences, operational tasks, all can be modeled.</p>	Modeling is appropriate for any system or system safety analysis.
50	Naked Man	This technique is to evaluate a system by looking at the bare system (controls) needed for operation without any external features added in order to determine the need/value of control to decrease risk.	The technique is universally appropriate.
51	Network Logic Analysis	Network Logic Analysis is a method to examine a system in terms of mathematical representation in order	The technique is universally appropriate to complex systems.

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
		to gain insight into a system that <u>might not ordinarily be achieved.</u>	
52	Operating and Support Hazard Analysis	The analysis is performed to identify and evaluate hazards/risks associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system.	The analysis is appropriate for all operational and support efforts.
53	Petri Net Analysis	Petri Net Analysis is a method to model unique states of a complex system. Petri Nets can be used to model system components, or sub-systems at a wide range of abstraction levels; e.g., conceptual, top – down, detail design, or actual implementations of hardware, software, or combinations.	The technique is universally appropriate to complex systems.
54	Preliminary Hazard Analysis	Preliminary Hazard Analysis (PHA) is the initial analysis effort within system safety.  The PHA is an extension of a Preliminary Hazard List.  As the design matures the PHA evolved into a system of sub-system hazard analysis.	The technique is universally appropriate.
55	Preliminary Hazard List	Preliminary Hazard List (PHL) is also an initial analysis effort within system safety. Lists of initial hazards or potential accidents are listed during concept development.	The technique is universally appropriate.
56	Procedure Analysis	Procedure Analysis is a step-by-step analysis of specific procedures to identify hazards or risks associated with procedures.	The technique is universally appropriate.
57	Production System Hazard Analysis	Production System Hazard Analysis is used to identify hazards that may be introduced during the production phase of system development which could impair safety and to identify their means of control. The interface between the product and the production process is examined	The technique is appropriate during development and production of complex systems and complex subsystems.
58	Prototype Development	Prototype Development provides a Modeling/Simulation analysis the	This technique is appropriate during the early phases of pre-production

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
		constructs early pre-production products so that the developer may inspect and test an early version.	and test.
59	Risk-Based Decision Analysis	Risk-Based Decision Analysis is an efficient approach to making rational and defensible decisions in complex situations.	The technique is universally appropriate to complex systems.
60	Root Cause Analysis	This method identifies causal factors to accident or near-miss incidents. This technique goes beyond the direct causes to identify fundamental reasons for the fault or failure.	Any accident or incident should be formally investigated to determine the contributors of the unplanned event. The root cause is underlying contributing causes for observed deficiencies that should be documented in the findings of an investigation.
61	Safety Review	A Safety Review assesses a system, identify facility conditions, or evaluate operator procedures for hazards in design, the operations, or the associated maintenance.	Periodic inspections of a system, operation, procedure, or process are a valuable way to determine their safety integrity.  A Safety Review might be conducted after a significant or catastrophic event has occurred.
62	Scenario Analysis	Scenario Analysis identifies and corrects hazardous situation by postulating accident scenarios where credible and physically logical	Scenarios provide a conduit for brainstorming or to test a theory in where actual implementation could have catastrophic results.  Where system features are novel, subsequently, no historical data is available for guidance or comparison, a Scenario Analysis may provide insight.
63	The Sequentially-Timed Events Plot Investigation System (STEP)	This method is used to define systems; analyze system operations to discover, assess, and find problems; find and assess options to eliminate or control problems; monitor future performance; and investigate accidents.	In accident investigation a sequential time of events may give critical insight into documenting and determining causes of an accident. The technique is universally appropriate.
64	Single-Point Failure Analysis	This technique is to identify those failures, that would produce a catastrophic event in items of injury or monetary loss if they were to occur by themselves	This approach is applicable to hardware systems, software systems, and formalized human operator systems

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
65	Sneak-Circuit Analysis	Sneak-Circuit Analysis identifies unintended paths or control sequences that may result in undesired events or inappropriately time events.	This technique is applicable to control and energy-delivery delivery circuits of all kinds, whether electronic/electrical, pneumatic, or hydraulic.
66	Software Failure Modes and Effects Analysis	This technique identifies software related design deficiencies through analysis of process flow-charting. It also identifies areas for verification/validation and test evaluation.	Software is embedded into vital and critical systems of current as well as future aircraft, facilities, and equipment. This methodology can be used for any software process; however, application to software controlled hardware systems is the predominate application. It can be used to analyze control, sequencing, timing monitoring, and the ability to take a system from an unsafe to a safe condition.
67	Software Fault Tree Analysis	This technique is employed to identify the root cause(s) of a “top” undesired event. To assure adequate protection of safety critical functions by inhibits interlocks, and/or hardware.	Any software process at any level of development or change can be analyzed deductively. However, the predominate application is software controlled hardware systems.
68	Software Hazard Analysis	The purpose of this technique is to identify, evaluate, and eliminate or mitigate software hazards by means of a structured analytical approach that is integrated into the software development process.	This practice is universally appropriate to software systems.
69	Software Sneak Circuit Analysis	Software Sneak Circuit Analysis (SSCA) is designed to discover program logic that could cause undesired program outputs or inhibits, or incorrect sequencing/timing.	The technique is universally appropriate to any software program.
70	Structural Safety Analysis	This method is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to potential for latent design problems.	The approach is appropriate to structural design; i.e., airframe.
71	Subsystem Hazard Analysis	Subsystem Hazard Analysis (SSHA) identifies hazards and their effects that may occur as a result of design.	This protocol is appropriate to subsystems only.
72	System Hazard	System Hazard Analysis purpose is	Any closed loop hazard

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
	Analysis	to concentrate and assimilate the results of the SSHA into a single analysis to ensure the hazards of their controls or monitors are evaluated to a system level and handles as intended.	identification and tracking system for an entire program, or group of subsystems can be analyzed.
73	Systematic Inspection	This technique purpose is to perform a review or audit of a process or facility.	The technique is universally appropriate.
74	Task Analysis	Task Analysis is a method to evaluate a task performed by one or more personnel from a safety standpoint in order to identify undetected hazards, develop note/cautions/warnings for integration in order into procedures, and receive feedback from operating personnel.	Any process or system that has a logical start/stop point or intermediate segments, which lend themselves to analysis.  This methodology is universally appropriate to any operation, which there is a human input, is performed.
75	Technique For Human Error Rate Prediction (THERP)	This technique provides a quantitative measure of human operator error in a process.	This technique is the standard method for the quantifying of human error in industry.
76	Test Safety Analysis	Test Safety Analysis ensures a safe environment during the conduct of systems and prototype testing. It also provides safety lessons to be incorporated into the design, as application.	A lessons learned approach of any new systems 'or potentially hazardous subsystems' is provided.  This approach is especially applicable to the development of new systems, and particularly in the engineering/development phase.
77	Time/Loss Analysis For Emergency Response Evaluation	This technique is a system safety analysis-based process to semi-quantitatively analyze, measure and evaluate planned or actual loss outcomes resulting from the action of equipment, procedures and personnel during emergencies or accidents.	Any airport, airline and other aircraft operators should have an emergency contingency plan to handle unexpected events can be analyzed.  This approach defines organize data needed to assess the objectives, progress, and outcome of an emergency response; to identify response problems; to find and assess options to eliminate or reduce response problems and risks; to monitor future performance; and to investigate accidents.
78	Uncertainty	Uncertainty Analysis addresses.	This discipline does not typically

FAA System Safety Handbook, Chapter 9: Analysis Techniques  
December 30, 2000

No.	Methods and/or Techniques	Summary	Applicability and Use
	Analysis	quantitatively and qualitatively, those factors that cause the results of an analysis to be uncertain.	address uncertainty explicitly and there are arguments that all analyses should. This is an region of great <u>potential application</u> .
79	Walk-Trough Analysis	This technique is a systematic analysis that should be used to determine and correct root causes of unplanned occurrences related to <u>maintenance</u> .	This technique is applicable to maintenance.
80	What-If Analysis	What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence.	The technique is universally appropriate.
81	What-If/Checklist Analysis	What-If or Checklist Analysis is a simple method of applying logic in a deterministic manner.	The technique is universally appropriate.

# Chapter 10

## System Software Safety

<b>10.0 SYSTEM SOFTWARE SAFETY.....</b>	<b>2</b>
<b>10.1 INTRODUCTION .....</b>	<b>2</b>
<b>10.2 THE IMPORTANCE OF SYSTEM SAFETY .....</b>	<b>3</b>
<b>10.3 SOFTWARE SAFETY DEVELOPMENT PROCESS.....</b>	<b>5</b>
<b>10.4 SYSTEM SAFETY ASSESSMENT REPORT (SSAR) .....</b>	<b>14</b>

## 10.0 SYSTEM SOFTWARE SAFETY

### 10.1 Introduction

Much of the information in this chapter has been extracted from the JSSSC Software System Safety Handbook, December, 1999, and concepts from DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1, 1992.

Since the introduction of the digital computer, system safety practitioners have been concerned with the implications of computers performing safety-critical or safety-significant functions. In earlier years, software engineers and programmers constrained software from performing in high risk or hazardous operations where human intervention was deemed both essential and prudent from a safety perspective. Today, however, computers often autonomously control safety critical functions and operations. This is due primarily to the capability of computers to perform at speeds unmatched by its human operator counterpart. The logic of the software also allows for decisions to be implemented unemotionally and precisely. In fact, some current operations no longer include a human operator.

Software that controls safety-critical functions introduce risks that must be thoroughly addressed (assessed and mitigated?) during the program by both management and design, software, and system safety engineering. In previous years, much has been written pertaining to "Software Safety" and the problems faced by the engineering community. However, little guidance was provided to the safety practitioner that was logical, practical, or economical. This chapter introduces an approach with engineering evidence that software can be analyzed within the context of both the systems and system safety engineering principles. The approach ensures that the safety risk associated with software performing safety-significant functions is identified, documented, and mitigated while supporting design-engineering objectives along the critical path of the system acquisition life cycle.

The concepts of risk associated with software performing safety-critical functions were introduced in the 1970's. At that time, the safety community believed that traditional safety engineering methods and techniques were no longer appropriate for software safety engineering analysis. This put most safety engineers in the position of "wait and see." Useful tools, techniques, and methods for safety risk management were not available in the 1970's even though software was becoming more prevalent in system designs.

In the following two decades, it became clear that traditional safety engineering methods were indeed partially effective in performing software safety analysis by employing traditional approaches to the problem. This situation does not imply, however, that some modified techniques are not warranted. Several facts must be realized before a specific software safety approach is introduced. These basic facts must be considered by the design engineering community to successfully implement a system safety methodology that addresses the software implications.

- Software safety is a systems issue, not a software-specific issue. The hazards caused by software must be analyzed and solved within the context of good systems engineering principles.
- An isolated safety engineer may not be able to produce effective solutions to potential software-caused hazardous conditions without the assistance of supplemental expertise. The software safety "team" should consist of the safety engineer, software engineer, system engineer, software quality engineer, appropriate "ility" engineers (configuration

## FAA System Safety Handbook, Chapter 10: System Software Safety December 30, 2000

management, test & evaluation, verification & validation, reliability, and human factors), and the subsystem domain engineer.

- Today's system-level hazards, in most instances, contain multiple contributing factors from hardware, software, human error, and/or combinations of each, and,
- Finally, software safety engineering cannot be performed effectively outside the umbrella of the total system safety engineering effort. There must be an identified link between software faults, conditions, contributing factors, specific hazards and/or hazardous conditions of the system.

The safety engineer must also never lose sight of the basic, fundamental concepts of system safety engineering. The product of the system safety effort is not to produce a hazard analysis report, but to influence the design of the system to ensure that it is safe when it enters the production phase of the acquisition life cycle. This can be accomplished effectively if the following process tasks are performed:

- Identify the safety critical functions of the system.
- Identify the system and subsystem hazards/risks.
- Determine the effects of the risk occurrence.
- Analyze the risk to determine all contributing factors (i.e.. hardware, software, human error, and combinations of each.)
- Categorize the risk in terms of severity and likelihood of occurrence.
- Determine requirements for each contributing factor to eliminate, mitigate, and/or control the risk to acceptable levels. Employ the safety order of design precedence Chapter 3, Table 3-7, for hazard control.
- Determine testing requirements to prove the successful implementation of design requirements where the hazard risk index warrants.
- Determine and communicate residual safety risk after all other safety efforts are complete to the design team and program management.

### 10.2 The Importance of System Safety

Before an engineer (safety, software, or systems) can logically address the safety requirements for software, a basic understanding of how software “fails” is necessary. Although the following list may not completely address every scenario, it provides the most common failure mechanisms that should be evaluated during the safety analysis process.

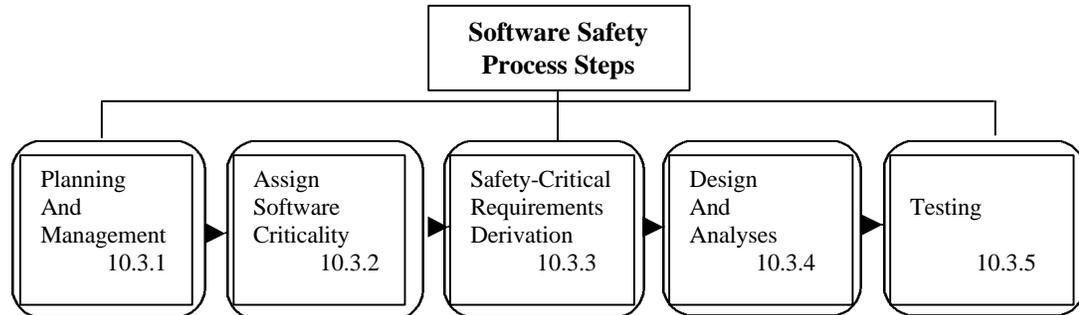
- Failure of the software to perform a required function, i.e., either the function is never executed or no answer is produced.
- The software performs a function that is not required, i.e., getting the wrong answer, issuing the wrong control instruction, or doing the right action but under inappropriate conditions.
- The software possesses timing and/or sequencing problems, i.e., failing to ensure that two things happen at the same time, at different times, or in a particular order.

FAA System Safety Handbook, Chapter 10: System Software Safety  
December 30, 2000

- The software failed to recognize that a hazardous condition occurred requiring corrective action.
- The software failed to recognize a safety-critical function and failed to initiate the appropriate fault tolerant response.
- The software produced the intended but inappropriate response to a hazardous condition.
- The specific causes most commonly associated with the software failure mechanisms listed above are:
  - Specification Errors: Specification errors include omitted, improperly stated, misunderstood, and/or incorrect specifications and requirements. Software may be developed "correctly" with regard to the specification, but wrong from a systems perspective. This is probably the single largest cause of software failures and/or errors.
  - Design and Coding Errors: These errors are usually introduced by the programmer and can result from specification errors, usually the direct result of poor structured programming techniques. These errors can consist of incomplete interfaces, timing errors, incorrect interfaces, incorrect algorithms, logic errors, lack of self-tests, overload faults, endless loops, and syntax errors. This is especially true for fault tolerant algorithms and parameters.
  - Hardware/Computer Induced Errors: Although not as common as other errors, then can exist. Possibilities include random power supply transients, computer functions that transform one or more bits in a computer word that unintentionally change the meaning of the software instruction, and hardware failure modes that are not identified and/or corrected by the software to revert the system to a safe state.
  - Documentation Errors: Poor documentation can be the cause of software errors through miscommunication. Miscommunication can introduce the software errors mentioned above. This includes inaccurate documentation pertaining to system specifications, design requirements, test requirements, source code and software architecture documents including data flow and functional flow diagrams.
  - Debugging/Software Change Induced Hazards: These errors are basically self-explanatory. The cause of these errors can be traced back to programming and coding errors, poor structured programming techniques, poor documentation, and poor specification requirements. Software change induced errors help validate the necessity for software configuration.

### 10.3 Software Safety Development Process

The process outlined below is briefly explained in this Handbook. Further guidance and specific instructions can be obtained through a careful examination of the JSSSC Software System Safety Handbook, Dec. 1999 and DO-178B, Software Considerations in Airborne Systems and Equipment Certification, Dec. 1, 1992 at a minimum.



#### 10.3.1 Software Safety Planning and Management

Software system safety planning precedes all other phases of the software systems safety program. It is perhaps the single most important step and should impose provisions for accommodating safety well before each of the software life cycle phases: requirements, design, coding, and testing starts in the cycle. Detailed planning ensures that critical program interfaces and support are identified and formal lines of communication are established between disciplines and among engineering functions. The software aspects of systems safety tend to be more problematic in this area since the risks associated with the software are often ignored or not well understood until late in the system design.

##### ***Planning Provisions***

The software system safety plan should contain provisions assuring that:

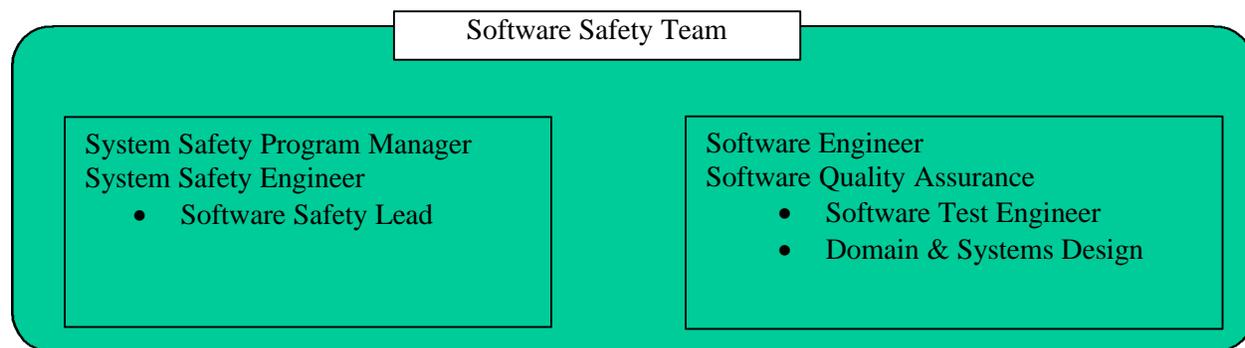
- Software safety organization is properly chartered and a safety team is commissioned at the beginning of the life cycle.
- Acceptable levels of software risk are defined consistently with risks defined for the entire system.
- Interfaces between software and the rest of the system's functions are clearly delineated and understood.
- Software application concepts are examined to identify hazards/risks within safety-critical software functions.
- Requirements and specifications are examined for hazards (e.g. identification of hazardous commands, processing limits, sequence of events, timing constraints, failure tolerance, etc.)
- Design and implementation is properly incorporated into the software safety requirements.

FAA System Safety Handbook, Chapter 10: System Software Safety  
December 30, 2000

- Appropriate verification and validation requirements are established to assure proper implementation of software system safety requirements.
- Test plans and procedures can achieve the intent of the software safety verification requirements.
- Results of software safety verification efforts are satisfactory.

### **Software Safety Team**

Software safety planning also calls for creating a software safety team. Team size and shape depends commensurately on mission size and importance (see Figure 10-1). To be effective, the team should consist of analytical individuals with sufficient system engineering background. Chapter 5 of this handbook provides a comprehensive matrix of minimum qualifications for key system safety personnel. It applies to software system safety provided professional backgrounds include sufficient experience with software development (software requirements, design, coding, testing, etc.)



**Figure 10-1: Example Membership of Software System Safety Team**

Several typical activities expected of the team range from identifying software-based hazards to tracing safety requirements, from identifying limitations in the actual code to developing software safety test plans and ultimately reviewing test results for their compliance with safety requirements.

### **Management**

Software System Safety program management begins as soon as the System Safety Program (SSP) is established and continues throughout the system development. Management of the effort requires a variety of tasks or processes from establishing the Software Safety Working Group (SwSWG) to preparing the System Safety Assessment Report (SSAR). Even after a system is placed into service, management of the software system safety effort continues to address modifications and enhancements to the software and the system. Often, changes in the use or application of a system necessitate a re-assessment of the safety of the software in the new application. Effective management of the safety program is essential to the effective reduction of the system risk. Initial efforts parallel portions of the planning process since many of the required efforts need to begin very early in the safety program. Safety management pertaining to software generally ends with the completion of the program and its associated testing; whether it is a single phase of the development process or continues throughout the development, production, deployment and maintenance phases. Management efforts end when the last safety deliverable is completed and is accepted by the FAA. Management efforts may then revert to a "caretaker" status in which the safety manager monitors the use of

## FAA System Safety Handbook, Chapter 10: System Software Safety December 30, 2000

the system in the field and identifies potential safety deficiencies based on user reports and accident/incidents reports. Even if the developer has no responsibility for the system after deployment, the safety program manager can develop a valuable database of lessons learned for future systems by identifying these safety deficiencies.

Establishing a software safety program includes establishing a SwSWG. This is normally a sub-group of the SSWG and chaired by the safety manager. The SwSWG has overall responsibility for the following:

- Monitoring and control of the software safety program
- Identifying and resolving risks with software contributory factors
- Interfacing with the other IPTs, and
- Performing final safety assessment of the system (software) design.

### **10.3.2 Assign Software Criticality**

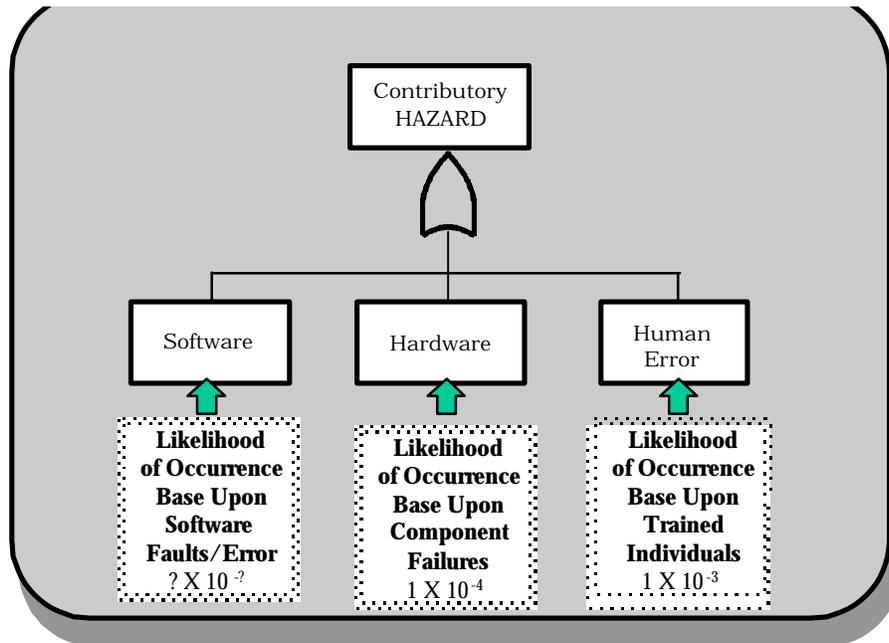
The ability to prioritize and categorize hazards is essential for the allocation of resources to the functional area possessing the highest risk potential. System safety programs have historically used the Hazard Risk Index (HRI) to categorize hazards. However, the methodology to accurately categorize hazards using this traditional HRI matrix for hazards possessing software causal factors is insufficient. The ability to use the original (hardware oriented) HRI matrix was predicated on the probability of hazard occurrence and the ability to obtain component reliability information from engineering sources. The current technologies associated with the ability to accurately predict software error occurrence, and quantify its probability, is still in its development infancy. This is due to the nature of software as opposed to hardware. Statistical data may be used for hardware to predict failure probabilities. However, software does not fail in the same manner as hardware (it does not wear out, break, or have increasing tolerances). Software errors are generally requirements errors (failure to anticipate a set of conditions that lead to a hazard, or influence of an external component failure on the software) or implementation errors (coding errors, incorrect interpretation of design requirements). Therefore, assessing the risk associated with software is somewhat more complex. Without the ability to accurately predict a software error occurrence, supplemental methods of hazard categorization must be available when the hazard possesses software causal factors. This section of the handbook presents a method of categorizing hazards that possess software influence or causal factors.

#### ***Risk Severity***

Regardless of the contributory factors (hardware, software, human error, and software influenced human error) the severity of the risk could remain constant. This is to say that the consequence of risk remains the same regardless of what actually caused the hazard to propagate within the context of the system. As the severity is the same, the severity tables presented in Chapter 3 remain applicable criteria for the determination of risk severity for those hazards possessing software causal factors.

#### ***Risk Probability***

With the difficulty of assigning accurate probabilities to faults or errors within software modules of code, a supplemental method of determining risk probability is required when software causal factors exist. Figure 10-2 demonstrates that in order to determine a risk probability, software contributory factors must be assessed in conjunction with the contributors from hardware and human error. The determination of hardware and human error contributor probabilities remain constant in terms of historical “best” practices. However, the likelihood of the software aspect of the risk's cumulative causes must be addressed.



**Figure 10-2: Likelihood of Occurrence Example**

There have been numerous methods of determining the software's influence on system-level risks. Two of the most popular software listings are presented in MIL-STD 882C and RTCA DO-178B (see Figure 10-3). These do not specifically determine software-caused risk probabilities, but instead assesses the software's "control capability" within the context of the software contributors. In doing so, each software contributors can be labeled with a software control category for the purpose of helping to determine the degree of autonomy that the software has on the hazardous event. The software safety team must review these lists and tailor them to meet the objectives of the system safety and software development programs.

FAA System Safety Handbook, Chapter 10: System Software Safety  
December 30, 2000

<b>MIL-STD 882C</b>	<b>RTCA-DO-178B</b>
<p><b>(I)</b> Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazards occurrence.</p> <p><b>(IIa)</b> Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.</p> <p><b>(IIb)</b> Software item displays information requiring immediate operator action to mitigate a hazard. Software failure will allow or fail to prevent the hazard's occurrence.</p> <p><b>(IIIa)</b> Software items issues commands over potentially hazardous hardware systems, subsystem, or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.</p> <p><b>(IIIb)</b> Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.</p> <p><b>(IV)</b> Software does not control safety critical hardware systems, subsystems, or components and does not provide safety critical information.</p>	<p><b>(A)</b> Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the aircraft.</p> <p><b>(B)</b> Software whose anomalous behavior, as shown by the System Safety assessment process, would cause or contribute to a failure of system function resulting in a hazardous/severe-major failure condition of the aircraft.</p> <p><b>(C)</b> Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a major failure condition for the aircraft.</p> <p><b>(D)</b> Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a minor failure condition for the aircraft.</p> <p><b>(E)</b> Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of function with no effect on aircraft operational capability or pilot workload. Once software has been confirmed as level E by the certification authority, no further guidelines of this document apply.</p>

**Figure 10-3: Examples of Software Control Capabilities**

Once again, the concept of labeling software contributors with control capabilities is foreign to most software developers and programmers. They must be convinced that this activity has utility in the identification and prioritization of software entities that possesses safety implication. In most instances, the software development community desires the list to be as simplistic and short as possible. The most important aspect of the activity must not be lost, that is, the ability to categorize software causal factors for the determining of both risk likelihood, and the design, code, and test activities required to mitigate the potential software cause. Autonomous software with functional links to catastrophic risks demand more coverage than software that influences low-severity risks.

### **Software Hazard Criticality Matrix**

The Software Hazard Criticality Matrix (SHCM) (see Figure 10-4 for an example matrix) assists the software safety engineering team and the subsystem and system designers in allocating the software safety requirements between software modules and resources, and across temporal boundaries (or into separate architectures). The software control measure of the SHCM also assists in the prioritization of software design and programming tasks.

FAA System Safety Handbook, Chapter 10: System Software Safety  
December 30, 2000

Control Category		Severity			
		Catastrophic	Critical	Marginal	Negligible
<p><b>(I)</b> Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazards occurrence.</p> <p><b>(IIa)</b> Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.</p> <p><b>(IIb)</b> Software item displays information requiring immediate operator action to mitigate a hazard. Software failure will allow or fail to prevent the hazard's occurrence.</p> <p><b>(IIIa)</b> Software items issues commands over potentially hazardous hardware systems, subsystem, or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.</p> <p><b>(IIIb)</b> Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.</p> <p><b>(IV)</b> Software does not control safety critical hardware systems, subsystems, or components and does not provide safety critical information.</p>	1	1	3	5	
	1	2	4	5	
	1	2	4	5	
	2	3	5	5	
	2	3	5	5	
	3	4	5	5	

	High Risk - Significant Analyses and Testing Resources
	Medium Risk - Requirements and Design Analysis and Depth Testing Required
	Moderate Risk - High Levels of Analysis and Testing Acceptable With Managing Activity Approval
	Moderate Risk - High Levels of Analysis and Testing Acceptable With Managing Activity Approval
	Low Risk - Acceptable

Figure 10-4: Software Hazard Criticality Matrix

### 10.3.3 Derivation of System Safety-Critical Software Requirements

Safety-critical software requirements are derived from known safety-critical functions, tailored generic software safety requirements and inverted contributory factors determined from previous activities. Safety requirement specifications identify the specifics and the decisions made, based upon the level of risk, desired level of safety assurance, and the visibility of software safety within the developer organization. Methods for doing so are dependent upon the quality, breadth and depth of initial hazard and failure mode analyses and on lessons-learned derived from similar systems. The generic list of requirements and guidelines establish the beginning point that initiates the system-specific requirements identification process. System-specific software safety requirements require a flow-down of hazard controls into requirements for the subsystems which provide a trace (audit trail) between the requirement, its associated risk and to the module(s) of code that are affected. Once this is achieved as a core set of requirements, design decisions are identified, assessed, implemented, and included in the hazard record database. Relationships to other risks or requirements are also determined. The identification of system-specific requirements (see Figure 10-5) is the direct result of a complete hazard analysis methodology.

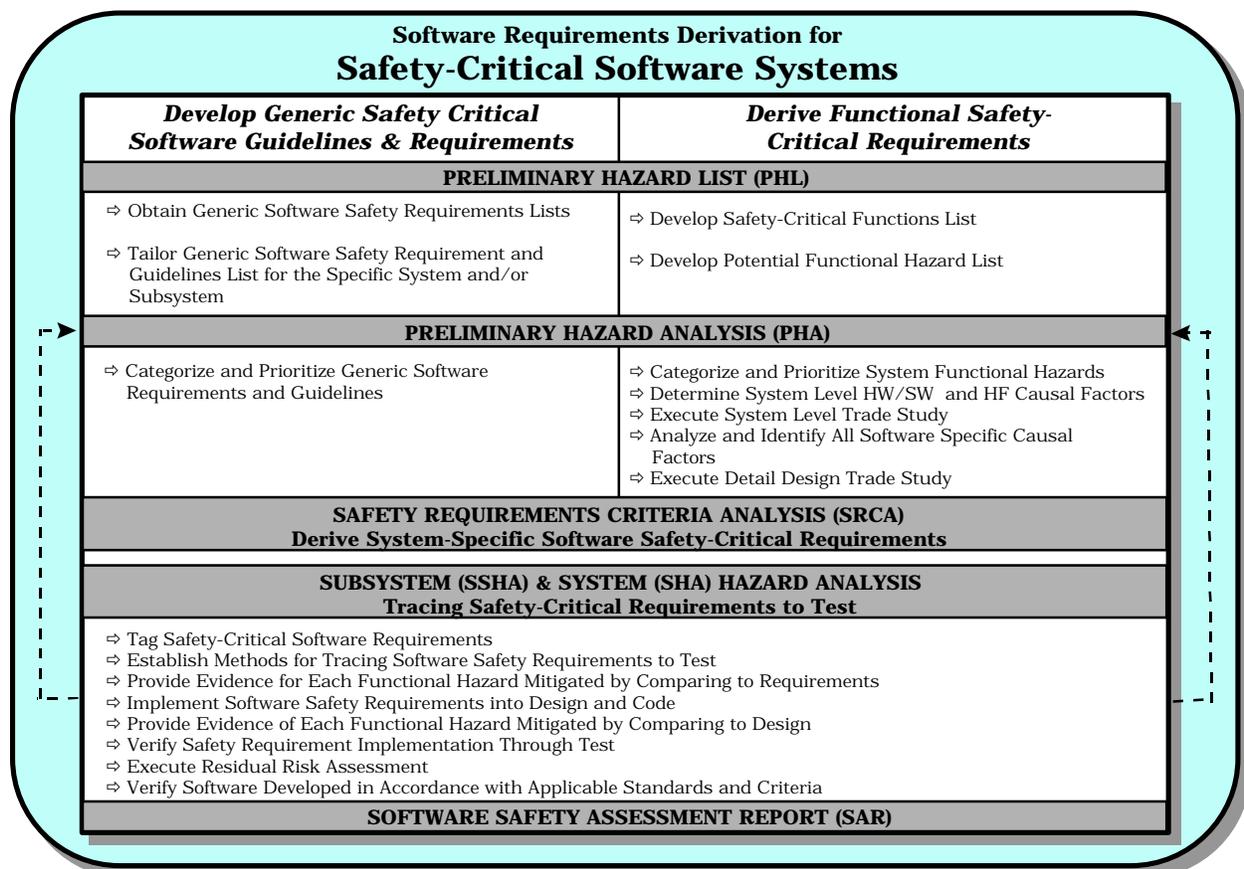


Figure 10-5: Software Safety Requirements Derivation

### **Preliminary Software Safety Requirements**

The first “cut” at system-specific software safety requirements are derived from the PHA analyses performed in the early life cycle phase of the development program. As previously discussed, the PHL/PHA hazards are a product of the information reviewed pertaining to systems specifications, lessons learned, analyses from similar systems, common sense, and preliminary design activities. Hazards that are identified during the PHA phase are analyzed and preliminary design considerations are identified to design engineering to mitigate the risk. These design considerations represent the preliminary safety requirements of the system, subsystems, and their interfaces (if known). These preliminary requirements must be accurately defined in the hazard record database for extraction when reporting of requirements to the design engineering team.

### **Matured Software Safety Requirements**

As the system and subsystem design mature, the requirements unique to each subsystem also matures via the Subsystem Hazard Analysis (SSHA). The safety engineer, during this life cycle phase of the program, attends the necessary design reviews and spends many hours with the subsystem designers for the purpose of accurately defining the subsystem hazards. Hazards/risks identified are documented in the hazard database and the hazard “causes” (hardware, software, human error, and software-influenced human error) identified and analyzed. When fault trees are used as the functional hazard analysis methodology, the contributors leading to the risk determine the derived safety-critical functional requirements. It is at this point in the design that preliminary design considerations are either formalized and defined into specific requirements, or eliminated if they no longer apply with the current design concepts. The maturation of safety requirements is accomplished by analyzing the design architecture to connect the risk to the contributors. The causal factors are analyzed to the lowest level necessary for ease of mitigation. The lower into the design the analysis progresses, the more simplistic (usually) and cost effective the mitigation requirements tend to become. The PHA phase of the program should define causes to at least the Computer Software Configuration Item (CSCI) level, whereas the SSHA and System Hazard Analysis (SHA) phases of safety analyses should analyze the causes to the algorithm level where appropriate.

#### **10.3.4 Design and Analyses**

The identification of subsystem and system hazards and failure modes inherent in the system under developed is essential to the success of a credible software safety program. The primary method of reducing the safety risk of software performing safety-significant functions is to first identify the system hazards and failure modes, and then determine which hazards and failure modes are *caused by* or *influenced by* software or lack of software. This determination includes scenarios where information produced by software could potentially influence the operator into a wrong decision resulting in a hazardous condition (design-induced human error). Moving from hazards to software contributors (and consequently design requirements to either eliminate or control the risk) is very practical, logical, and adds utility to the software development process. It can also be performed in a timelier manner as much of the analysis is accomplished to influence preliminary design activities.

The specifics of how to perform either a subsystem or system hazard analysis are briefly described in Chapters 8 and 9. The fundamental basis and foundation of a system safety (or software safety) program is a systematic and complete hazard analysis process.

One of the most helpful steps within a credible software safety program is to categorize the specific causes of the hazards and software inputs in each of the analyses (PHA, SSHA, SHA, and Operating & Support Hazard Analysis (O&SHA)). Hazard causes can be identified as those caused by; hardware, and/or hardware components; software inputs or lack of software input; human error; and/or software influenced human error or hardware or human errors propagating through the software. Hazards may result from one specific cause

## FAA System Safety Handbook, Chapter 10: System Software Safety December 30, 2000

or any combination of causes. As an example, “loss of thrust” on an aircraft may have causal factors in any of the four below listed categories.

- **Hardware:** foreign object ingestion,
- **Software:** software commands engine shutdown in the wrong operational scenario,
- **Human error:** pilot inadvertently commands engine shutdown, and,
- **Software influence pilot error:** computer provides incorrect information, insufficient or incomplete data to the pilot causing the pilot to execute a shutdown.

The safety engineer must identify and define the hazard control considerations (PHA phase) and requirements (SSHA, SHA, and O&SHA phases) for the design and development engineers. Hardware causes are communicated to the appropriate hardware design engineers; and software related causes to the software development and design team. All requirements should be reported to the systems engineering group for their understanding and necessary tracking and/or disposition.

The preliminary software design SSHA begins upon the identification of the software subsystem and uses the derived system specific safety-critical software requirements. The purpose is to analyze the system, software architecture and preliminary CSCI design. At this point, all generic and functional Software Safety Requirements (SSRs) should have been identified and it is time to begin allocating them to the identified safety-critical functions and tracing them to the design.

The allocation of the SSRs to the identified hazards can be accomplished through the development of SSR verification trees that links safety critical and safety significant SSRs to each Safety-Critical Function (SCF). The SCFs in turn are already identified and linked to each hazard. By verifying the nodes through analysis, (code/interface, logic, functional flow, algorithm and timing analysis) and/or testing (identification of specific test procedures to verify the requirement), the Software Safety Engineer (SwSE) is essentially verifying that the design requirements have been implemented successfully. The choice of analysis and/or testing to verify the SSRs is up to the individual Safety Engineer whose decision is based on the criticality of the requirement to the overall safety of the system and the nature of the SSR. Whenever possible, the Safety Engineer should use testing for verification.

Numerous methods and analytical techniques are available to plan, identify, trace and track safety-critical CSCIs and Computer Software Units (CSUs). Guidance material is available from the Institute of Electrical and Electronic Engineering (IEEE) (Standard for Software Safety Plans), the Department of Defense (DOD) Defense Standard 00-55-Annex B, DOD-STD-2167, NASA-STD-2100.91, MIL-STD-1629, the JSSSC Software System Safety Handbook and DO-178B.

### 10.3.5 Testing

Two sets of analyses should be performed during the testing phase:

- Analyses before the fact to ensure validity of tests
- Analyses of the test results

Tests are devised to verify all safety requirements where testing has been selected as appropriate verification method. This is not considered here as analysis. Analysis before the fact should, as a minimum, consider test coverage for safety critical Must-Work-Functions.

## FAA System Safety Handbook, Chapter 10: System Software Safety December 30, 2000

### ***Test Coverage***

For small pieces of code it is sometimes possible to achieve 100% test coverage (i.e., to exercise every possible state and path of the code). However, it is often not possible to achieve 100 % test coverage due to the enormous number of permutations of states in a computer program execution, versus the time it would take to exercise all those possible states. Also there is often a large indeterminate number of environmental variables, too many to completely simulate.

Some analysis is advisable to assess the optimum test coverage as part of the test planning process. There is a body of theory that attempts to calculate the probability that a system with a certain failure probability will pass a given number of tests.

“White box” testing can be performed at the modular level. Statistical methods such as Monte Carlo simulations can be useful in planning "worst case" credible scenarios to be tested.

### ***Test Results Analysis***

Test results are analyzed to verify that all safety requirements have been satisfied. The analysis also verifies that all identified risks have been either eliminated or controlled to an acceptable level of risk. The results of the test safety analysis are provided to the ongoing system safety analysis activity.

All test discrepancies of safety critical software should be evaluated and corrected in an appropriate manner.

### ***Independent Verification and Validation (IV&V)***

For high value systems with high risk software, an IV&V organization is usually involved to oversee the software development. The IV&V organization should fully participate as an independent group in the validation of test analysis.

## **10.4 System Safety Assessment Report (SSAR)**

The System Safety Assessment Report (SSAR) is generally a CDRL item for the safety analysis performed on a given system. The purpose of the report is to provide management an overall assessment of the risk associated with the system including the software executing within the system context of an operational environment. This is accomplished by providing detailed analysis and testing evidence that the software related hazards have been identified to the best of their ability and have been either eliminated or mitigated/controlled to levels acceptable to the FAA. It is paramount that this assessment report be developed as an encapsulation of all the analyses performed. The SSAR shall contain a summary of the analyses performed and their results, the tests conducted and their results, and the compliance assessment. Paragraphs within the SAR need to encompass the following items:

- The safety criteria and methodology used to classify and rank software related hazards (causal factors). This includes any assumptions made from which the criteria and methodologies were derived,
- The results of the analyses and testing performed,
- The hazards that have an identified residual risk and the assessment of that risk,
- The list of significant hazards and the specific safety recommendations or precautions required to reduce their safety risk; and
- A discussion of the engineering decisions made that affect the residual risk at a system level.

FAA System Safety Handbook, Chapter 10: System Software Safety  
December 30, 2000

The final section of the SSAR should be a statement by the program safety lead engineer describing the overall risk associated with the software in the system context and their acceptance of that risk.

## **Chapter 11: Test and Evaluation Safety**

<b>11.1 INTRODUCTION .....</b>	<b>2</b>
<b>11.2 TESTS CONDUCTED SPECIFICALLY FOR SAFETY .....</b>	<b>2</b>
<b>11.3 TESTS CONDUCTED FOR PURPOSES OTHER THAN SAFETY .....</b>	<b>2</b>
<b>11.4 TEST SAFETY ANALYSIS .....</b>	<b>2</b>
<b>11.5 OTHER TEST AND EVALUATION SAFETY CONSIDERATIONS.....</b>	<b>4</b>

## **11.0 TEST AND EVALUATION SAFETY**

### **11.1 Introduction**

Verification testing will be required at some point in the life cycle of a system and the component(s) of a system. Tests may be conducted at many hierarchical levels and involve materials, hardware, software, interfaces, processes, and procedures or combinations of these. These tests determine whether requirements have been met by the design, compatibility of personnel with equipment and operating conditions, and adequacy of design and procedures. There are two broad types of testing which may be of benefit to safety, which are discussed below.

### **11.2 Tests Conducted Specifically For Safety**

Testing can be conducted to determine the existence of hazards, effectiveness of hazard mitigation, or whether the hazard analysis is correct. This includes safe levels of stress in mechanical systems or components, severity of damage resulting from an uncontrolled hazard, or suitability and/or effectiveness of safety equipment. Examples include testing such materials as plastics, lubricants, or solvents for flammability; testing of fire extinguisher materials for effectiveness; testing the effectiveness of personnel protective equipment; testing the radiation characteristics of RF emitters.

### **11.3 Tests Conducted For Purposes Other Than Safety**

Testing is normally conducted to verify performance, i.e. verify that the system meets design requirements. The data from these tests can also be used for safety purposes. Examples include, determination of part failure rates which can be used to predict the probability of failure; testing the strength or compatibility of new materials which can be used to identify possible hazards; determination of interface problems between integrated assemblies which can also define hazards; and quality control tests performed by vendors of subcontractors. Tests performed for purposes other than safety can generate data useful to the safety process only if the proper data is collected and documented. It is the job of safety engineering to clearly define the safety program objectives so that test planners will be aware of the data which will be useful to safety.

### **11.4 Test Safety Analysis**

It is also important to consider the safety of the test itself. Safety engineers need to work closely with test planners to ensure that the 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.

### **11.4.1 Test And Evaluation Safety Tasks**

A comprehensive test and evaluation safety program will involve the following activities:

- Coordinate with test planning to determine testing milestones in order to ensure that safety activities are completed in time to support testing.
- Schedule safety analysis, evaluation and approval of test plans and other documents to ensure that safety is covered during all testing.
- Prepare safety inputs to operating and test procedures.
- Analyze test equipment, installation of test equipment and instrumentation prior to the start of testing.
- Identify any hazards unique to the test environment.
- Identify hazard control measures for hazards of testing.
- Identify test data that will be of use to safety.
- Review test documentation to ensure incorporation of safety requirements, warnings, and cautions.
- Review test results to determine if safety goals have been met or if any new hazards have been introduced by the test conditions.
- Collect data on the effectiveness of operating procedures and any safety components or controls of the system.
- Compile safety-related test data.
- Make a determination about the safety of the system. Determine if the safety features have been controlled as expected and if identified hazards have been controlled to an acceptable level of risk.
- Evaluate compatibility with existing or planned systems or equipment.
- Identify deficiencies and needs for modifications.
- Evaluate lessons-learned from previous tests of new or modified systems or tests of comparable systems to identify possible hazards or restrictions on test conditions.
- Document and track all identified hazards to ensure resolution.

### 11.4.2 Test And Evaluation Safety Results

A comprehensive test and evaluation safety program will produce the following products:

- Hazard analysis reports.
- Test safety analysis reports.
- Hazard tracking and risk resolution system.
- Safety analysis schedules.
- List of identified hazards.
- List of hazard control measures.
- List of required safety data.
- List of warnings and cautions.
- Reports of procedure and test plan reviews.
- Safety inputs to test planning reviews.
- Safety inputs to training materials.
- Safety inputs to operations manuals.

### 11.5 Other Test And Evaluation Safety Considerations

#### **11.5.1 A system whose safe operation depends upon trained personnel should not be tested without appropriately trained personnel.**

The test personnel should undergo a training program consistent with the anticipated operator training program. Testing a system in the operational environment using design engineering personnel provides limited validation data. A successful OT&E program includes training in normal operation, support, and emergency procedures. Most systems have some residual risk (i.e., high voltages, RF energy, hot surfaces, and toxic materials) that must be reflected in the training program. Personnel must receive training in how to handle the residual hazards. Also, emergency procedures are developed to minimize the impact of system failures. Personnel must be trained in these procedures. Safety must review all operations and emergency procedures to ensure the adequacy of the procedures and training.

#### **11.5.2 Adequate documentation is required for correct operation and support of a system.**

Personnel must rely on manuals to supplement their training. These manuals must be accurate and include comprehensive information on safe operation and support of the system. Manuals must be reviewed prior to the start of the test to ensure that safety portions are complete and provide adequate instructions, cautions, and warnings to protect personnel and equipment.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

## **Chapter 12: Facilities System Safety**

<b>12.1 INTRODUCTION .....</b>	<b>2</b>
<b>12.2 NEW FACILITY SYSTEM SAFETY .....</b>	<b>4</b>
<b>12.3 EXISTING FACILITIES.....</b>	<b>7</b>
<b>12.4 FACILITY SYSTEM SAFETY PROGRAM.....</b>	<b>9</b>
<b>12.5 ANALYTICAL TECHNIQUES.....</b>	<b>13</b>
<b>12.6 FACILITY RISK ANALYSIS METHODOLOGY.....</b>	<b>20</b>
<b>12.7 HAZARD TRACKING LOG EXAMPLE.....</b>	<b>31</b>
<b>12.8 EQUIPMENT EVALUATION AND APPROVAL .....</b>	<b>31</b>
<b>12.9 FACILITY AND EQUIPMENT DECOMMISSIONING .....</b>	<b>32</b>
<b>12.10 RELATED CODES .....</b>	<b>33</b>
<b>12.11 TECHNICAL REFERENCES .....</b>	<b>35</b>

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

## **12.0 Facilities System Safety**

### **12.1 Introduction**

The purpose of facility system safety is to apply system safety techniques to a facility from its initial design through its demolition. This perspective is often referred to as the Facility Acquisition Life Cycle. The term “facility” is used in this chapter to mean a physical structure or group of structures in a specific geographic site, the surrounding areas near the structures, and the operational activities in or near the structures. Some aspects that facility system safety address are: structural systems, Heating, Ventilation, and Air-conditioning (HVAC) system, electrical systems, hydraulic systems, pressure and pneumatic systems, fire protection systems, water treatment systems, equipment and material handling, and normal operations (e.g. parking garage) and unique operational activities (e.g. chemical laboratories). This Life Cycle approach also applies to all activities associated with the installation, operation, maintenance, demolition and disposal rather than focusing only on the operator.

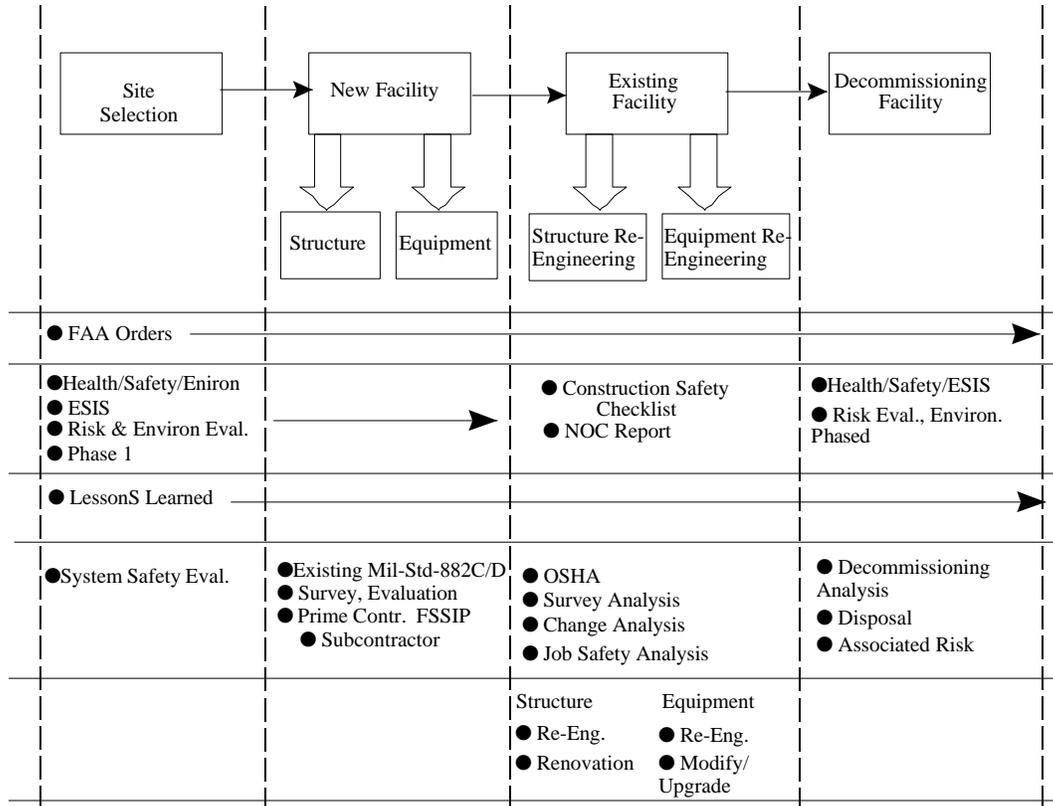
Facilities are major subsystems providing safety risks to system and facility operational and maintenance staff. Control of such risks is maintained through the timely implementation of safety processes similar to those employed for safety risk management for airborne and ground systems. MIL-STD-882, Section 4 “General Requirements” defines the minimum requirements of a safety program. These requirements define the minimum elements of a risk management process with analysis details to be tailored to the application.

#### **12.1.1 Facility Life Cycle**

System Safety techniques are applied throughout the entire Life Cycle of a facility as shown in Figure 12-1. There are four major phases of a facility's Life Cycle. They are:

- Site Selection (Pre-Construction)
- New Facility (Design and Construction)
  - Structure
  - Equipment
- Existing Facility (Design and Construction)
  - Structure Re-Engineering
  - Equipment Re-Engineering
- Facility and Equipment Decommissioning

FAA System Safety Handbook, Chapter 12: Facilities Safety  
 December 30, 2000



**Figure 12-1 Facility Life Cycle**

**12.1.2 Facility-Related Orders**

The facility system safety process starts with implementing directives such as FAA Order 1600.46 and FAA Order 3900.19, FAA Occupational Safety and Health Program. FAA Order 1600.46 applies resources for the identification and control of risks in the development of requirements, design, construction, operation and ultimately dismantling of the facility. FAA Order 3900.19, FAA Occupational Safety and Health Program, assigns requirements of the Occupational Safety and Health Act, Public Law 91-596; Executive Order 12196, Occupational Safety and Health Programs for Federal Employees; and 29 Code of Federal Regulations (CFR), Part 1960, Basic Program Elements for Federal Occupational Safety and Health Programs. The SSPP examines the specifics of applicable risks for the phase, the level of risk, and the appropriate means of control in a manner similar to that employed for hardware and software safety.

It is important to note that there is a hierarchy of safety and health directives and specifications in the FAA. All efforts should start with FAA 3900.19, Occupational Safety and Health Program rather than other related FAA Orders (e.g. FAA Order 6000.15, General Maintenance Handbook for Airway Facilities) and

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

FAA Specifications (e.g. FAA-G-2100, Electronic Equipment, General Requirements). These related documents contain only a small part of the safety and health requirements contained in FAA Order 3900.19, FAA Occupational Safety and Health Program and the Occupational Safety and Health Administration (OSHA) Standards.

The methodologies as defined in MIL-STD-882 are applicable to both construction and equipment design and re-engineering. As with all safety significant subsystems, the System Safety process for facilities should be tailored to each project in scope and complexity. The effort expended should be commensurate with the degree of risk involved. This objective is accomplished through a facility risk assessment process during the mission need and/or Demonstration and Evaluation (DEMVAL) phase(s).

## **12.2 New Facility System Safety**

It is customary to implement a facility system safety program plan that describes system safety activities and tasks from inception of the design through final decommissioning of the facility. The plan establishes the system safety organization, the initiation of a System Safety Working Group, (SSWG) and the analysis efforts conducted.

Facilities system safety involves the identification of the risks involving new facility construction and the placement of physical facilities on site. The risks associated with construction operations, the placement of hazardous facilities and materials, worker safety and facility design considerations are evaluated. Hazard analyses are conducted to identify the risks indicated above.

Consideration should be given to physical construction hazards i.e. materials handling, heavy equipment movement, fire protection during construction. Facility designs are also evaluated from a life safety perspective, fire protection view, airport traffic consideration, structural integrity and other physical hazards. The location of hazardous operations are also evaluated to determine their placement and accessibility, i.e. high hazard operations should be constructed away from general populations. Consideration should also be given to contingency planning, accident reconstruction, emergency egress/ingress, emergency equipment access and aircraft traffic flow. Line of sight considerations should be evaluated as well as factors involving electromagnetic environmental effects. Construction quality is also an important consideration, where physical designs must minimally meet existing standards, codes and regulations.

### **12.2.1 New Structures and Equipment**

Facility system safety also evaluates new structures and new equipment being installed. The hazards associated with physical structures involve: structural integrity, electrical installation, floor loading, snow loading, wind effects, earthquake and flooding. Fire protection and life safety are also important considerations. The fire protection engineering aspects are evaluated, such as automatic fire protection equipment, fire loading, and structural integrity.

System safety is also concerned with the analysis of newly installed equipment. The following generic hazards should be evaluated within formal analysis activities. Generic hazards areas are: electrical, implosion, explosion, material handling, potential energy, fire hazards, electrostatic discharge, noise, rotational energy, chemical energy, hazardous materials, floor loading, lighting and visual access, electromagnetic environmental affects, walking/working surfaces, ramp access, equipment failure/malfunction, foreign object damage, inadvertent disassembly, biological hazards, thermal non

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

ionizing radiation, pinch/nip points, system hazards, entrapment, confined spaces, and material incompatibility.

### **12.2.2 Site Selection**

The FAA carefully considers and weighs environmental amenities and values in evaluating proposed Federal actions relating to facility planning and development, utilizing a systematic interdisciplinary approach and involving local and state officials and individuals having expertise.

The environmental assessment and consultation process provides officials and decision makers, as well as members of the public, with an understanding of the potential environmental impacts of the proposed action. The final decision is to be made on the basis of a number of factors. Environmental considerations are to be weighed as fully and as fairly as non-environmental considerations. The FAA's objective is to enhance environmental quality and avoid or minimize adverse environmental impacts that might result from a proposed Federal action in a manner consistent with the FAA's principal mission to provide for the safety of aircraft operations.

In conducting site evaluations the following risks must be evaluated from a system safety perspective.

- Noise
- Environmental Site Characterization
- Compatible Land Use
- Emergency Access and existing infrastructure
- Water supply
- Local emergency facilitates
- Social Impacts
- Induced Socioeconomic Impacts
- Air & Water Quality
- Historic, Architectural, Archeological, and Cultural Resources.
- Biotic Communities
- Local Weather Phenomena (tornadoes, hurricanes and lightning)
- Physical Phenomena (e.g. mudslide and earth quakes)
- Endangered and Threatened Species of Flora and Fauna.
- Wetlands.
- Animal Migration
- Floodplains.
- Coastal Zone Management
- Coastal Barriers.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

- Wild and Scenic Rivers
- Farmland.
- Energy Supply and Natural Resources.
- Solid Waste
- Construction Impacts.

### **12.2.3 Design Phase**

The tasks to be performed during design are dependent upon the decisions made by the SSWG based on the PHL/PHA and negotiated in the contractual process. If the cost of the facility and the degree of hazard or mission criticality justify their use, analyses discussed in Chapters 8 and 9 such as Fault Tree, Failure Mode and Effects Analysis, and Operating and Support Hazard Analysis should be considered.

Besides monitoring risk analyses, there are several actions the SSWG performs during the design process. They participate in design reviews and track needed corrective actions identified in analyses for incorporation in the design.

### **12.2.4 Construction Phase**

During the construction phase, two safety related activities take place. Change orders are reviewed to ensure changes do not degrade safety features already incorporated in the design. Successful execution is dependent on disciplined configuration control.

The final step before the user takes control of the facility is the occupancy inspection. This inspection verifies the presence of critical safety features incorporated into the design. The use of a hazard tracking system can facilitate the final safety assessment. This review may identify safety features that might otherwise be overlooked during the inspection. A Hazard Tracking Log can generate a checklist for safety items that should be part of this inspection.

The results of the occupancy inspection can serve as a measure of the effectiveness of the SSPP. Any hazards discovered during the inspection will fall into one of two categories. A hazard that was previously identified and the corrective action to be taken to control the determined hazard, or a hazard not previously identified requiring further action. Items falling in this second category can be used to measure the effectiveness of the SSPP for a particular facility.

SSPP tasks appropriate for the construction phase are as follow:

- Ensure the application of all relevant building safety codes, including OSHA, National Fire Protection Association, and FAA Order 3900.19B safety requirements.
- Conduct hazard analyses to determine safety requirements at all interfaces between the facility and those systems planned for installation.
- Review equipment installation, operation, and maintenance plans to make sure all design and procedural safety requirements have been met.
- Continue updating the hazard correction tracking begun during the design phases.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

- Evaluate accidents or other losses to determine if they were the result of safety deficiencies or oversight.
- Update hazard analyses to identify any new hazards that may result from change orders.

In addition, guidance for conducting a Hazardous Material Management Program (HMMP) is provided in National Aerospace Standard (NAS) 411. The purpose of a HMMP is to provide measures for the elimination, reduction, or control of hazardous materials. A HMMP is composed of several tasks that complement an SSPP:

- HMMP Plan
- Cost analysis for material alternatives over the life cycle of the material
- Documented trade-off analyses
- Training
- HMMP Report

## **12.3 Existing Facilities**

Facility system safety is also successfully applied in the evaluation of risks associated with existing facilities. There may be a need to establish a System Safety Working Group in order to conduct hazard analysis of existing facilities. If previous analyses are not available, it will be appropriate to initiate these analysis efforts. There are benefits that can be gained by systematically reviewing physical structures, processes, and equipment. Additional safety related risks may be uncovered and enhancements provided to mitigate these risks. Secondary benefits can be enhancements and process, productivity, and design.

### **12.3.1 Re-Engineering of Structures and Equipment**

When major changes to existing facilities, equipment or structures are contemplated, a rigorous system safety activity that includes hazard analysis should be conducted.

#### ***Analysis of Existing Systems***

In order to accomplish the analysis of existing systems it is appropriate to establish a working group and to identify hazard analysis techniques that will be used. The following presents an example of such an activity. The concept of Operational Risk Management is applied. (See Chapter 15 for additional information. It is appropriate to form an Operational Risk Management Group (ORMG) in order to perform hazard analysis. Analysis examples are provided, e.g., operating and support hazard analysis, requirements cross check analysis, risk assessment, and job safety analysis.

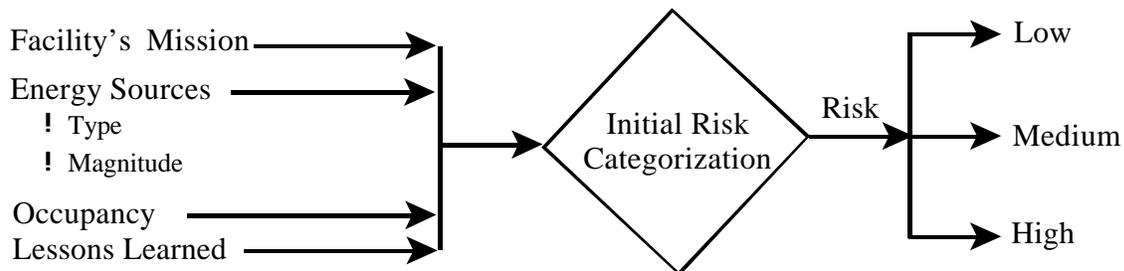
#### ***Facility Risk Categories***

The completion of the initial Preliminary Hazard List (PHL) permits categorization of the planned facility into risk categories. Categorizing is based on several factors, such as number of people exposed, type and degree of inherent hazard of operation, criticality of the facility to the National Air Space (NAS), vulnerability, and cost. Inputs include whether or not the facility is "one of a kind" or a standard design and how it impacts the rest of the installation. For example, the failure or destruction of a facility used to house emergency power or one through which communication lines run may shut down an entire airport or region. The designation should reflect the local concern for operational safety and health risks presented by the facility and its mission. It is critical that the appropriate risk categorization be applied in each instance.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

Several examples of categorization methods are presented below to illustrate their risk ranking approaches based on certain unique hazards.

The approach to facility risk categorization is summarized in Figure 12-2.



**Figure 12-2 Facility Risk Categorization**

For example, the following three risk categories can be used:

Low-risk facilities; i.e., housing, and administrative buildings. In these types of facilities, risks to building occupants are low and limited normally to those associated with everyday life. Accident experience with similar structures must be acceptable, and no additional hazards (e.g., flammable liquids, toxic materials, etc.) are to be introduced by the building occupants. Except in special cases, no further system safety hazard analysis is necessary for low risk facility programs.

Medium-risk facilities; i.e., maintenance facilities, heating plants, or benign facilities with safety critical missions such as Air Traffic Control (ATC) buildings. This group of facilities often presents industrial type safety risks to the building occupants and the loss of the facility's operation has an impact on the safety of the NAS. Accidents are generally more frequent and potentially more severe. A preliminary hazard analysis (PHA) is appropriate. System hazard Analysis (SHA) and Subsystem Hazard Analysis (SSHA) may also be appropriate. The facility design or systems engineering team members are major contributors to these analyses. User community participation is also important.

High-risk facilities; i.e., high-energy-related facilities, fuel storage, or aircraft maintenance. This category usually contains unique hazards of which only an experienced user of similar facility will have detailed knowledge. Because of this, it is appropriate for the user or someone with applicable user experience to prepare the PHA in addition to the PHL. Additional hazard analyses (e.g., system, subsystem, operating and support hazard analyses may be required).

Another example is presented in FAA Order 3900.19, FAA Occupational Safety and Health Program. This Order requires that "increased risk workplaces be inspected twice a year and all general workplaces once a year." Increased risk workplaces are based on an evaluation by an Occupational Safety and Health professional and include areas such as battery rooms and mechanical areas.

In facility system safety applications, there are many ways of classifying risk which are based on exposures, such as fire loading, or hazardous materials. The National Fire Protection Association provides details on these various risk categorization schemes. (See page 12-34 NFPA Health (hazard) Identification System).

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

## **12.4 Facility System Safety Program**

Preparation of a facility system safety program involves the same tasks detailed in Chapter 5. However, there are unique applications and facility attributes which are discussed in this section.

### **12.4.1 General Recommendations for a Facility System Safety Program**

Listed below are a number of general recommendations which are appropriate. This list is provided for example purposes only.

- A formal system safety program should be implemented. Significant benefits can be realized by initiating a system safety program. This benefit is the ability to coordinate assessments, risk resolution, and hazard tracking activities.
- Job safety analyses (JSAs) should be used to identify task-specific hazards for the purpose of informing and training maintenance staff and operators.
- The JSAs can be generated using the information provided in the O&SHA.
- Copies of the JSA should be incorporated into the procedures outlined in operating manuals for quick reference before conducting a particular analyzed task.
- First line supervisors should be trained in methods of conducting a JSA.
- Analyses should be updated by verification and validation of hazards and controls through site visits, further document review, and consultation with Subject Matter Experts (SMEs).
- The analysis of the available operating procedures can identify implied procedures that are often not analyzed or documented, such as the transport of LRUs to and from the equipment to be repaired. There may be unrecognized risks associated with these undocumented procedures.
- It is critical that all available documentation be reviewed and site visits be performed to ensure the safety of operators and maintainers of the system.
- When appropriate, site surveys will be planned to further refine the analysis and allow the analysis to be more specific. Site visits should be conducted for the purpose of data collection, hazard control validation, verification and update following a process or configuration change. The information collected during the site surveys will be used to further refine the O&SHA.
- Analyses must be revised to include new information, and a quality control review must be performed.
- Conformance to existing codes, standards, and laws are considered minimal system safety requirements.
- Hazard analysis and risk assessment are required to assure elimination and mitigation of identified risks.
- Safety, health, and environmental program activities should be conducted in conjunction with facility system safety efforts.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

The concept of operational risk management is the application of operational safety and facility system safety. More explicit information on Operational Risk management is found in Chapter 15.

#### **12.4.2 System Safety Program Plan (SSPP)**

The first task the SSWG performs is the preparation of the System Safety Program Plan (SSPP). It is customary to implement a facility system safety program plan that describes system safety activities and tasks from inception of the design through final commissioning of the facility. The plan establishes the system safety organization, the initiation of a SSWG, and the analysis efforts conducted. When approved, it becomes the road map for the project's system safety effort. This plan tailors the SSPP requirements to the needs of the specific project. The SSPP establishes management policies and responsibilities for the execution of the system safety effort. The SSPP should be written so the system safety tasks and activity outputs contribute to timely project decisions. Evaluation of system safety project progress will be in accordance with the SSPP.

Example elements of the Facility SSPP are as follows:

- Establishment of project risk acceptance criteria based on consideration of the user's recommendations. The acceptable level of risk in a facility is an expression of the severity and likelihood of an accident type that the using organization is willing to accept during the operational life of the facility. The goal is to identify all hazards and to eliminate those exceeding the defined level of acceptable risk. While this is not always possible, the analysis conducted will provide the information upon which to base risk acceptance decisions.
- A specific listing of all tasks, including hazard analyses, that are a part of the design system safety effort; designation of the responsible parties for each task. Optional tasks should be designated as such, listing the conditions which would initiate these tasks.
- Establishment of a system safety milestone schedule. Since the purpose of the hazard analysis is to beneficially impact the design, early completion of these analyses is vital. The schedule for analysis completion must complement the overall design effort.
- Establishment of procedures for hazard tracking and for obtaining and documenting residual risk acceptance decisions.
- Outline of procedures for documenting and submitting significant safety data as lessons learned.
- Establishment of procedures for evaluating proposed design changes for safety impact during the later stages of design or during construction after other safety analysis is complete.
- Establishment of a communication system that provides timely equipment requirements and hazard data to the facility design. This is necessary when equipment to be installed or utilized within the facility is being developed or procured separately from the facility.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

Other factors influencing the SSPP are overall project time constraints, manpower availability, and monetary resources. The degree of system safety effort expended depends on whether the project replaces an existing facility, creates a new facility, involves new technology, or is based on standard designs. A more detailed discussion of each of the elements of a System Safety Program Plan is in Chapter 5.

### **12.4.3 Facility System Safety Working Group (SSWG)**

The system safety process starts with the establishment of the system safety working group (SSWG). The SSWG is often tasked to oversee the system safety effort throughout the facility life cycle. The SSWG assists in monitoring the system safety effort to ensure compliance with contract requirements. Tasks included in this effort may include review of analyses, design review, review of risk acceptance documentation, construction site reviews, and participation in occupancy inspection to ensure safety measures are designed into the facility. Initially, the SSWG consists of representatives of users of the facility, facility engineering personnel (resident engineer), installation safety personnel, installation medical personnel, installation fire personnel, and project managers. As the project evolves, the makeup of the team may change to incorporate appropriate personnel. Other members with specialized expertise may be included if the type of facility so dictates. SSWG participation in design reviews is also appropriate.

The preparation of facility safety analyses is normally the responsibility of industrial/occupational/plant safety staff. However, the system safety and occupational safety disciplines complement each other in their respective spheres of influence and often work together to provide a coordinated safety program and accomplish safety tasks of mutual interest. The documents and the recommendations of the SSWG may be used to write the scope of work for additional safety efforts for subsequent contractor development and construction activities. Specialized facility system safety working groups can be formed to incorporate the concept of operational risk management.

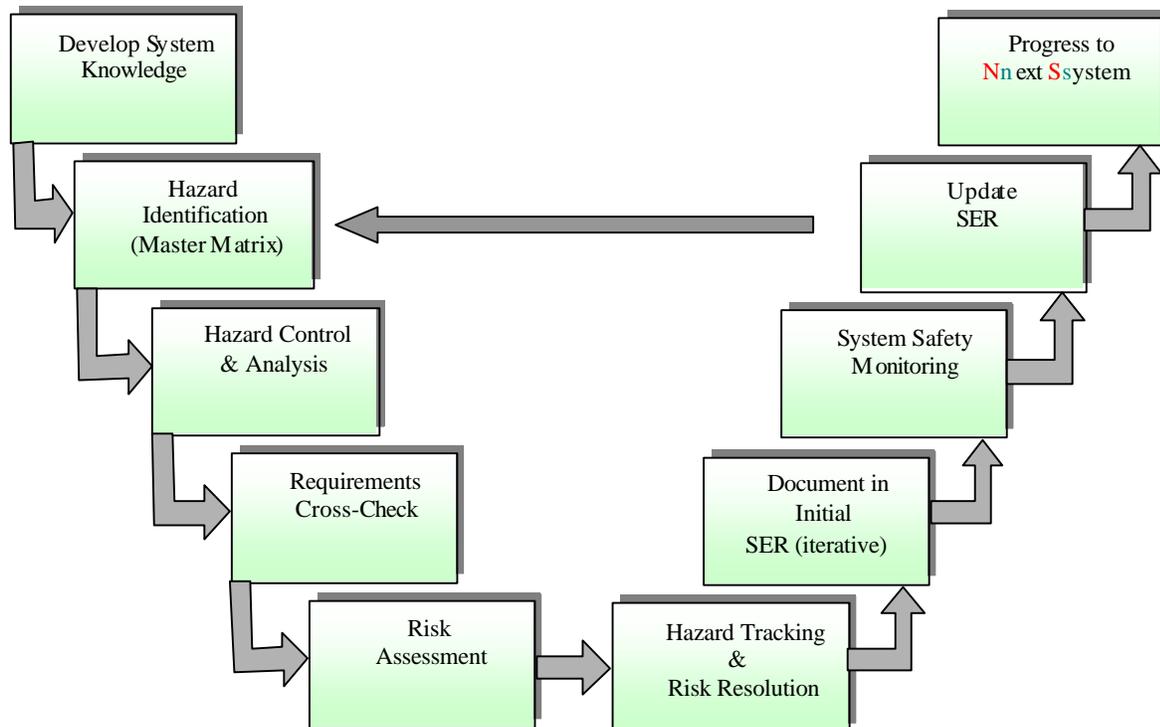
### **12.4.4 Occupational Risk Management Group (ORMG)**

The first step of the analysis should be to form the ORMG that would conduct the effort. This group should consist of appropriate representatives from various disciplines including support contractors. For example, group members should be experienced safety professionals who are recognized as experts in fire protection, system safety, environmental and industrial engineering as well as industrial hygiene and hazardous materials management. SSWG and ORMG will share data from the working group efforts.

#### ***ORMG Process***

The ORMG process consists of nine major elements, which are depicted in Figure 12-3.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000



**Figure 12-3: ORMG Process**

#### 12.4.5 Safety Engineering Report

The results of the O&SHA analysis should be presented in the SER. Updated analyses, observations, and recommendations should be provided in revisions of the SER as additional system knowledge about the hardware and procedures is collected and analyzed. The Master O&SHA\* and the requirements cross-check analysis should be refined as additional information is obtained. The contents of the SER will become more specific as more details about the system are identified and analyzed.

#### 12.4.6 System Knowledge

The ORMG's initial effort should be to acquire system knowledge. To that end, group members familiarized themselves with the system by reviewing available documentation provided by the product team. The following types of documents should be reviewed during this analysis:

- Operation and Maintenance for the system
- Maintenance of the system
- The Management of Human Factors in FAA Acquisition Programs

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

- Existing Human Factors Review documents
- Existing Computer-Human Interface Evaluations
- Safety Assessment Review documents
- Site Transition & Activation Plan (STAP)
- System Technical Manuals
- Site Transition and Activation Management Plan (STAMP)
- System/Subsystem Specification (SSS)

#### **12.4.7 Hazard Identification**

A generic list of anticipated hazards should be developed after the ORMG has become familiar with the system. The hazard list should also denote controls that could be implemented to manage the risks associated with the identified risks as well as relevant requirements from regulatory, consensus standards, and FAA documents. This information, should be presented as a tabular format which, includes a Requirements Cross-check Analysis. The generic hazards and controls should be developed from program documentation. It is anticipated that this list will lengthen as the O&SHA progresses. This list will also serve as a basis for other future analyses.

The basis of the analysis relates to generic hazards and controls to specific maintenance steps required for maintaining and repairing the system. The maintenance steps identified during the review should be integrated into a matrix. In evaluating hazards associated with the maintenance procedures, the specific procedures could fall into generic maintenance categories, which are characterized for example as listed below:

- Transporting line replaceable units (LRU)
- Processor shut down procedures
- Energizing and de-energizing procedures
- Connection and disconnection procedures
- Mounting and unmounting procedures
- Restart procedures

The anticipated hazards associated with the maintenance steps and comments could be presented in a Risk Assessment Matrix (Master Matrix). Generic hazard controls should be identified using a Requirements Cross-check Analysis. The anticipated hazards should be verified by on-site reviews.

### **12.5 Analytical Techniques**

The analytical techniques associated with facility system safety are the same techniques applied in the system safety discipline. However, discussions are provided to highlight the concepts of facility system safety, operational risk management, and safety, health, and environmental considerations.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### **12.5.1 Change Analysis<sup>1</sup>**

Change analysis examines the potential affects of modifications to existing systems from a starting point or baseline. The change analysis systematically hypothesizes worse case effects from each modification from that baseline. Consider existing, known system as a baseline. Examine the nature of all contemplated changes and analyze the potential effects of each change (singularly) and all changes (collectively) upon system risks. The process often requires the use of a system walk down, which is the method of physically examining the system or facility to identify the current configuration.

Alternatively, a change analysis could be initiated on an existing facility by comparing “as designed” with the “as built” configuration. In order to accomplish this, there would first be the need to physically identify the differences from the “as designed” configuration. The process steps are:

- Identify system baseline
- Identify changes
- Examine each baseline change by postulated effects
- Determine collective/interactive/interface effects
- Conclude system risk or deviation from baseline risk
- Report findings

### **12.5.2 Preliminary Hazard List (PHL)**

The SSWG or ORMG could be tasked with the preparation of the PHL. The purpose of the PHL is to systematically identify facility hazards. The generation of a PHL early in the development of a program is key to the success of the facility system safety effort. The Associate Administrator of the Sponsoring Organization is responsible for generating mission requirements for JRC decision points (see Section 2.1). The PHL should be included with this data. Participation by or delegation to the intended user of the facility in generating the PHL increases the quality of this initial safety risk analysis.

This PHL effort serves several important functions. It provides the FAA with an early vehicle for identifying safety, health, and environmental concerns. The results of this determination are used to size the scope of the necessary safety effort for the specification, design and construction activities. It provides the Associate Administrator with the data necessary to assess the cost of the safety effort and include it in requests for funding. By requiring the PHL to accompany the funding documentation, funding for system safety tasks becomes an integral part of the budget process.

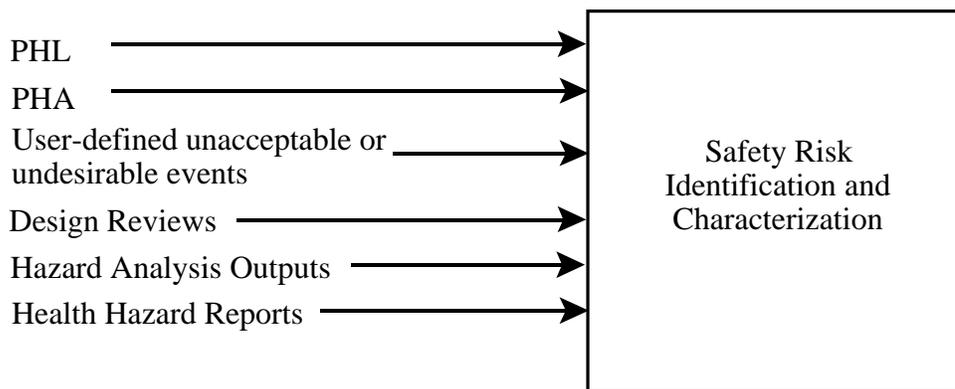
Generation of the initial PHL includes identification of safety critical areas. Areas that need special safety emphasis (e.g., walk-through risk analysis) are identified. The process for identifying hazards can be accomplished through the use of checklists, lessons learned, compliance inspections/audits, accidents/near

---

<sup>1</sup> System Safety Analysis Handbook, System Safety Society, July 1993.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

misses, regulatory developments, and brainstorming sessions. For existing facilities, the PHL can be created using information contained in the Environment and Safety Information System (ESIS). All available sources should be used for identifying, characterizing, and controlling safety risks. Examples of such inputs that may be found are in Figure 12-3. The availability of this information permits the FAA to incorporate special requirements into the detailed functional requirements and specifications. This input may be in the form of specific design features, test requirements, or SSP tasks. The resulting contract integrates system safety into the design of a facility starting with the concept exploration phase.



**Figure 12-3 Sample Inputs for Safety Risk Identification and Characterization**

The PHL also generates an initial list of risks that should initiate a Hazard Tracking Log, a database of risks, their severity and probability of occurrence, hazard mitigation, and status. New risks are identified throughout the design process, entered into and tracked by the log. As the design progresses, corrective actions are included and risks are eliminated or controlled using the system safety order of precedence (See Chapter 3, Table 3-1). Status is tracked throughout the design and construction process.

Safety risks may be logged closed in one of three ways. Those: (1) eliminated or controlled by design are simply “closed.” (2) that are to be controlled by procedures or a combination of design and procedures are marked closed but annotated to ensure that standard and operating procedures (SOPs) are developed to reduce the risk. A list of operation and maintenance procedures to be developed is generated and turned over to the user. (3) that are to be accepted as is, or with partial controls, are closed and risk acceptance documentation prepared. This process documents all risks, their status, and highlights any additional needed actions required. Thus, the hazard tracking system documents the status of safety risks throughout the life of the facility's life cycle.

### 12.5.3 Preliminary Hazard Analysis (PHA)

The preliminary hazard analysis (PHA) is an expansion of the PHL. The assessment of the facility's hazards permits classifying the facility in terms of low, medium, or high risk. It expands the PHL in three ways. It provides the following additional information:

- Details concerning necessary and planned corrective action

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

- Increased detail of hazards already identified
- More detailed analysis to identify additional hazards
- The PHA is used to determine the system safety effort for the remainder of the project

As an expanded version of the PHL, the PHA contains greater detail in three areas. First, hazard control information is added to identified hazards. Second, a more comprehensive and systematic analysis to identify additional hazards is performed. Third, greater detail on hazards previously identified in the PHL is provided.

Detailed knowledge of all operations to be conducted within the facility and any hazards presented by nearby operations is required. Based on the best available data, including lessons learned, hazards associated with the proposed facility design or functions are evaluated for risk severity and probability, together with operational constraints.

If the PHA indicates that the facility is a “low-risk” building and no further analysis is necessary, a list of applicable safety standards and codes are still required. If the facility is “medium” or “high” risk, methods to control risk must be instituted.

#### **12.5.4 Operating and Support Hazard Analysis**

The O&SHA could be performed early enough in the acquisition cycle to influence system design. However, this analysis could be initiated later in the acquisition cycle, it could be anticipated that it will not have an immediate effect on the existing design. The results of this analysis may, however, be used to initiate changes in an existing design. See Chapter 8, Operating and Support Hazard Analysis.

For existing systems the O&SHA is intended to address changing conditions through an iterative process that can include subject matter expert (SME) participation and a review of installed systems. This information could be documented in subsequent Safety Engineering Reports.

O&SHA is limited to the evaluation of risks associated with the operation and support of the system. The materials normally available to perform an O&SHA include the following:

- Engineering descriptions of the proposed system
- Draft procedures and preliminary operating manuals
- Preliminary hazard analysis, subsystem hazard analysis, and system hazard analysis reports
- Related requirements, constraints, and personnel capabilities
- Human factors engineering data and reports
- Lessons learned data.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### ***Operating and Support Hazard Analysis Approach***

This approach is based on the guidance of MIL-STD-882, *System Safety Program Plan Requirements and the International System Safety Society, Hazard Analysis Handbook*. The O&SHA evaluates hazards resulting from the implementation of operations or tasks performed by persons and considers the following:

- Planned system configuration or state at each phase of maintenance
- Facility interfaces
- Site observations
- Planned environments (or ranges thereof)
- Maintenance tools or other equipment specified for use
- Maintenance task sequence, concurrent task effects, and limitations;
- Regulatory, agency policy, or contractually specified personnel safety and health requirements including related requirements such as consensus standards
- Potential for unplanned events including hazards introduced by human errors or physical design.

Throughout the process, the human is considered an element of the total system, receiving inputs and initiating outputs during the conduct of operations and support. The O&SHA methodology identifies the safety-related requirements needed to eliminate hazards or mitigate them to an acceptable level of risk using established safety order of precedence. This precedence involves initial consideration of the elimination of the particular risk via a concept of substitution. If this is not possible, the risk should be eliminated by the application of engineering design. Further, if it is not possible to design out the risk, safety devices should be utilized. The order of progression continues and considers that if safety devices are not appropriate, design should include automatic warning capabilities. If warning devices are not possible, the risks are to be controlled via formal administrative procedures, including training.

#### **12.5.5 Job Safety Analysis**

JSAs could be presented as an output of the O&SHA. The JSA is a method used to evaluate tasks from an occupational safety and health perspective. This very basic analysis technique was known as Job Hazard Analysis (JHA) in the 1960s. The tool was generally used by industrial safety and health personnel. The JSA is a less detailed listing of basic hazards associated with a specific task and provides recommendations for following appropriate safe operating procedures. This analysis was designed to be very basic and usable by employees and their supervisors. It is appropriate for first line supervisors, operators, or maintainers to be trained in conducting JSAs. Typically, JSAs should be posted by the task site and reviewed periodically as a training tool.

The O&SHA is a more formal system safety engineering method that is designed to go beyond a JSA. System safety is concerned with any possible risk associated with the system. This includes consideration of the human/hardware/software/environmental exposures of the system. The analysis considers human factors and all associated interfaces and interactions. As an additional outcome of the O&SHA, different JSAs could be developed and presented depending on exposure and need. It is anticipated that JSAs will be

FAA System Safety Handbook, Chapter 12: Facilities Safety

December 30, 2000

utilized to conduct training associated with new systems. Specific JSAs addressing particular maintenance tasks, specific operations, and design considerations can be developed.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### 12.5.6 Physical Aviation Risk Analysis

Another objective of this chapter on facility system safety is to provide information on how to identify, eliminate and control aviation-related risks. There are unique hazards and risks associated with commercial aviation, as well as general aviation activities. Generally, a number of hazards and risks are listed for consideration. During hazard analysis activities, the analyst should consider these appropriate examples:

- Aviation fuel storage and handling.
- Airport ground handling equipment, its use, movement, and maintenance.
- Surface movement at airports
- Traffic management at airports.
- Life safety involving the general public at places of assembly in airports.
- Preventative maintenance and inspection of aircraft.
- The conduct of maintenance operations such as: use of flammables, solvents, parts cleaning, equipment accessibility, flammable materials, hangar fire protection equipment.
- Aircraft movement in and around hangars, aprons, taxiways.
- Operations during inclement weather, snow removal airport accessibility, the use of snow removal equipment.
- Accessibility of emergency equipment and emergency access of aircraft in the event of a contingency or accident.
- Accessibility of emergency personnel and security personnel in securing and accessing accident sites.
- Maintainability of airport surface equipment, such as, lighting, placarding and marking, surface runway conditions.
- Control tower visibility
- Fire protection of physical facilities, electrical installation requirements, grounding and bonding at facilities.

For further information concerning operating and support hazards and risks associated with aviation, contact the FAA Office of System Safety.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

## **12.6 Facility Risk Analysis Methodology**

After applying the various analysis techniques to identify risks, there are additional tasks involving: Risk assessment, hazard control analysis, requirements cross-check analysis, and hazard tracking and risk resolution.

### **12.6.1 Risk Assessment**

Risk assessment is the classification of relative risk associated with identified hazards. Risk has two elements, which are severity and likelihood. Severity is the degree of harm that would occur if an accident happens. Likelihood is a qualitative expression of the probability that the specific accident will occur. Criteria for severity and likelihood should be defined. When risk assessment is to be conducted, the risks should be prioritized to enable resources to be allocated consistently to the highest risks.

An example of a risk assessment matrix is provided in Table 12-1. This matrix indicates the related hazard code, hazard or scenario description, and scenario code. Both initial risk and final risk associated with the specific scenario is also indicated. There is also a section for supportive comments.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

Table 12-1: Risk Assessment Matrix Example

HAZ CODE	HAZARD DESCRIPTION	SCENARIO CODE	SCENARIO	INITIAL RISK	SUPPORT COMMENTS	RESIDUAL RISK
H1.1	Technicians may be inadvertently exposed to core high voltage when maintaining the monitor on the work bench.				This hazard is due to the “hot swap” LRU replacement philosophy.	
		S1.1.1	While accessing core a technician inadvertently contacts high voltage. This can result in possible fatality.	IC		IE
		S1.1.2	While accessing core a technician inadvertently contacts high voltage. This can result in possible major injury.	ID		IE
		S1.1.3	A technician does not follow appropriate de-energizing or grounding procedures resulting in inadvertent contact, electrical shock causing fatality.	IC		IE
		S1.1.4	A technician does not follow appropriate de-energizing or grounding procedures resulting in inadvertent contact, electrical shock causing major injury.	ID		IE



FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**Table 12-2 Hazard Tracking Log Example: LOCATION: Building 5 Paint Booth**

ITEM/FUNCTION	PHASE	HAZARD	CONTROL	CORRECTIVE ACTION & STATUS
Cranes (2) 1000 LB (top of paint booth frame)	Lifting	Loads exceed crane hoist capacity.	Rated capacity painted on both sides if Figures readable from the floor level. Ref. Operating Manual....	Closed. Use of cranes limited by procedure to loads less than 600 lbs.
Crane (1) 10,000 LB bridge (In front of paint booth)	Lifting	Loads exceed crane hoist capacity.	All bridge cranes proof loaded every 4 years. Certification tag containing date of proof load, capacity, and retest date located near grip.	Closed. No anticipated loads exceed 5000 lbs.
	Lifting	Loss of control through operator error.	All crane operators qualified and authorized by floor supervisor.  Cranes equipped with braking devices capable of stopping a load 1 1/4 X rated load.	Closed.
High Pressure Air Lines 100 LB	All operations	Pressure lines not properly identified.	Facility Safety Manual, Section ... requires all pressure lines to be coded to ANSI A.13.1 standards.	Closed. Lines identified and coded.
Facility Access	All operations	Injury to personnel due to emergency pathways blocked with dollies, cabinets, and stored hardware.	Reference Facility Safety Manual, Section ...., "Fire equipment, aisles, and exits shall be kept free of obstructions."	Closed. Area Manager is charged with instructing personnel on requirements and conducting daily audits.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### **12.6.2 Hazard Control Analysis**

To compare the generic hazards with those of a specific system, the maintenance procedures published for the system are formatted into a matrix (See Table 12 - 2). The matrix should list the detailed maintenance procedures and could serve as a method for correlating the hazards and controls with the discrete tasks to be performed on the system. Hazards specific to the system that have not included in the maintenance procedures are also to be identified during this step of the evaluation and integration.

A matrix will be used to document and assess the following:

- Changes needed to eliminate or control the hazard or reduce the associated risk
- Requirements for design enhancements, safety devices, and equipment, including personnel safety
- Warnings, cautions, and special emergency procedures (e.g., egress, escape, render safe, or back-out procedures), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication
- Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials
- Requirements for safety training.
- Potentially hazardous system states
- Federal laws regarding the storage and handling of hazardous materials.

### ***Requirements Cross-Check Analysis***

A requirements cross-check analysis should be performed in conjunction with the O&SHA (See Table 12-3). Any appropriate requirements that are applicable to specific hazard controls are to be provided as a technical reference. Any hazard control that is formally implemented becomes a specific requirement. Requirements cross-check analysis is a common technique in the system safety engineering discipline. A hazard control is considered verified when it is accepted as a formal program requirement through a process known as hazard tracking and risk resolution.

The requirement cross check analysis is a technique that relates the hazard description or risk to specific controls and related requirements. TABLE 12.-3 is an example of a requirement cross check analysis matrix. It is comprised of the following elements: hazard description code, hazard description, or accident scenario, the hazard rationale, associated with a specific exposure or piece of equipment. The matrix also displays a control code, hazard controls, and it also provides reference columns for appropriate requirement cross check. For this example, OSHA requirements, FAA requirements and National Fire Protection Association requirements are referenced.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

HAZ CODE	HAZARD DESCRIPTION	HAZARD RATIONALE	CON CODE	CONTROL	OSHA 29CFR 1900	FAA-G-2100F	HUMAN FACTORS (MIL-STD-1472)	NFPA Code
<b>1. Electrical</b>								
H1.1	Technicians may be inadvertently exposed to core high voltage when maintaining the monitor on the work bench.	This hazard is not appropriate to the system because of the LRU replacement maintenance philosophy.						
			C1.1	Technician should not access high voltage core without special authorization and training.	1910.303(h)(I)		5.10.5	70E, 2-2.1
			C1.2	Stored energy within the core must be removed via grounding prior to initiating work (suspect that manufacturers will be repairing faulty monitors)	1910.147(d)(5)	3.1.2.7 3.3.6.1.1	12.4.3	70B, 10-3.1 & 5-4.2.1 NFPA 70 460-6

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

<b>HAZ CODE</b>	<b>HAZARD DESCRIPTION</b>	<b>HAZARD RATIONALE</b>	<b>CON CODE</b>	<b>CONTROL</b>	<b>OSHA 29CFR 1900</b>	<b>FAA-G-2100F</b>	<b>HUMAN FACTORS (MIL-STD-1472)</b>	<b>NFPA Code</b>
			C1.3	Electrical safe operating procedures (e.g., LO/TO) should be implemented when any equipment is energized during bench top testing.	1910.147(c)(4)	3.3.6.1.6	4.1.7	
H1.2	Technicians could be inadvertently exposed to electrical power during removal and replacement of LRUs	This hazard is appropriate to all systems where there are voltages greater than 50 VDC.						
			C1.4	Lockout and tagout procedures must be followed and enforced prior to any system LRU replacement	1910.147(c)(4)	3.3.6.1.6		70B, 3-4.2 70E, 2-3.2 70E, 5-1.2

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

HAZ CODE	HAZARD DESCRIPTION	HAZARD RATIONALE	CON CODE	CONTROL	OSHA 29CFR 1900	FAA-G-2100F	HUMAN FACTORS (MIL-STD-1472)	NFPA Code
			C1.5	Provide guarding for each LRU associated equipment (e.g., relays, switches, bus bars, etc.) such that inadvertent contact with energized components can not occur during installation, replacement and/or removal of other LRUs.	1910.303(g)(2)		6.1.2.6	70e, 2-5 70e, 23-2
H1.3	Technicians could be inadvertently exposed to high voltages due to the lack of appropriate lockout tagout procedures.							
			C1.6	Conduct a review of existing or proposed LOTO procedures to ensure adequacy.	1910.147(z)(6)			70e, 5-1

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

HAZ CODE	HAZARD DESCRIPTION	HAZARD RATIONALE	CON CODE	CONTROL	OSHA 29CFR 1900	FAA-G-2100F	HUMAN FACTORS (MIL-STD-1472)	NFPA Code
			C1.7	Follow established LOTO procedures and incorporate them into appropriate technical manual. Provide recurring training for effected employees in appropriate procedures.	1910.147(c)(6)	3.3.6.1.6	5.10.5	70e, 5-1
			C1.8	Design console such that all power can be removed from a single console prior to performing maintenance and develop and document the procedure to accomplish this. If it is not possible to de-energize all power within a console, such power must be isolated, guarded and identified to prevent accidental contact.	1910.147(b)(2)(iii)	3.1.2.2.5	6.1.2.6	

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

HAZ CODE	HAZARD DESCRIPTION	HAZARD RATIONALE	CON CODE	CONTROL	OSHA 29CFR 1900	FAA-G-2100F	HUMAN FACTORS (MIL-STD-1472)	NFPA Code
H1.4	Technicians could be exposed to energized pins or connectors.							
			C1.9	Provide guards or other means to prevent exposed energized pins and connectors.	1910.303(g)(2)	3.3.1.3.4 .7.11/3.3 .6.4	6.8	70, 400-35 &4110-56(g)
H1.5	All electrical components are not properly grounded in their operating configuration. Should there be a fault in the rack, the technician could be inadvertently exposed to energy due to the fault (e.g., ground fault).	This hazard addresses inadvertent exposure due to inadequate grounding.						
			C1.10	Ensure proper grounding of all components (e.g., proper grounding of sliding racks moving covers and guards.)	1910.308(a)(4)(v)	3.3.6.1.1 /3.1.2.7. 1		70e, 2-6.4.44

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**TABLE 12-3 REQUIREMENTS CROSS-CHECK ANALYSIS**

<b>HAZ CODE</b>	<b>HAZARD DESCRIPTION</b>	<b>HAZARD RATIONALE</b>	<b>CON CODE</b>	<b>CONTROL</b>	<b>OSHA 29CFR 1900</b>	<b>FAA-G- 2100F</b>	<b>HUMAN FACTORS (MIL-STD- 1472)</b>	<b>NFPA Code</b>
H1.6	No single switch exists from which to de-energize the console for maintenance activities							

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### **12.7 Hazard Tracking Log Example**

Table 12-4 is an example of a page from a Hazard Tracking Log. It could also serve as a safety analysis that might be performed by design or facility safety engineering for a paint booth. As a safety analysis, it would serve as an effective design tool reflecting analysis tailoring. It does not meet the normal definition of hazard analysis as it does not include severity or probability levels.



FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

**Table 12-4 Hazard Tracking Log Example:** LOCATION: Building 5 Paint Booth

ITEM/FUNCTION	PHASE	HAZARD	CONTROL	CORRECTIVE ACTION & STATUS
Cranes (2) 1000 LB (top of paint booth frame)	Lifting	Loads exceed crane hoist capacity.	Rated capacity painted on both sides if Figures readable from the floor level. Ref. Operating Manual....	Closed. Use of cranes limited by procedure to loads less than 600 lbs.
Crane (1) 10,000 LB bridge (In front of paint booth)	Lifting	Loads exceed crane hoist capacity.	All bridge cranes proof loaded every 4 years. Certification tag containing date of proof load, capacity, and retest date located near grip.	Closed. No anticipated loads exceed 5000 lbs.
	Lifting	Loss of control through operator error.	All crane operators qualified and authorized by floor supervisor.  Cranes equipped with braking devices capable of stopping a load 1 1/4 X rated load.	Closed.
High Pressure Air Lines 100 LB	All operations	Pressure lines not properly identified.	Facility Safety Manual, Section ... requires all pressure lines to be coded to ANSI A.13.1 standards.	Closed. Lines identified and coded.
Facility Access	All operations	Injury to personnel due to emergency pathways blocked with dollies, cabinets, and stored hardware.	Reference Facility Safety Manual, Section ....., "Fire equipment, aisles, and exits shall be kept free of obstructions."	Closed. Area Manager is charged with instructing personnel on requirements and conducting daily audits.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

### **12.7.1 Matrices Construction**

Analyses matrices are designed to suit analytical needs. Matrices should be customized to enable the integration of analytical work. Matrices can be customized to present relevant information to allow continuous analysis and safety review.

### **12.7.2 Hazard Tracking and Risk Resolution**

All identified hazards should be tracked until closed out. This occurs when the hazard controls have been validated and verified. Validation is the consideration of the effectiveness and applicability of a control. System safety professionals or other designated group members conduct the validation process. Verification of a specific hazard control is the act of confirming that the control has been formally implemented. This process must also be conducted by a system safety professional or a designated group member. Each hazard control should be formally implemented as a requirement. Hazard control validation involves a detailed analysis of the particular control to determine its effectiveness, suitability, and applicability.

## **12.8 Equipment Evaluation and Approval**

A review of available Safety Assessments sometimes reveal that they focused primarily on a single Underwriters Laboratories, Inc. (UL) standard (e.g. UL 1050) instead of all of the Occupational Safety and Health Administration (OSHA) standards for the workplace. UL is an independent, not-for-profit product safety testing and certification organization whose work applies to the manufacture of products. The use of a UL standard by itself is inappropriate for comprehensive safety assessments of the workplace. OSHA's acceptance of a product certified by a nationally recognized testing laboratory (NRTL) does not mean the product is "OSHA-approved." It means that the NRTL has tested and certified the product to designate conformance to a specific product safety test standard(s) for a very specific issue.

Listing by an NRTL such as UL, does not automatically ensure that an item can be used at an acceptable level of risk. These listings are only indications that the item has been tested and listed according to the laboratory's criteria. These criteria may not reflect the actual risks associated with the particular application of the component or its use in a system. Hazard analysis techniques should be employed to identify these risks and implement controls to reduce them to acceptable levels. The hazard is related to the actual application of the product. A computer powered by 110 VAC might be very dangerous if not used as intended. For example, if it were used by a swimming pool, it would be dangerous regardless of the UL standard that it was manufactured to comply with. Therefore, the use of products manufactured to product manufacturing standards require the same system safety analysis as developmental items to ensure that they are manufactured to the correct standard and used in an acceptable manner.

Conformance to codes, requirements, and standards is no assurance of acceptable levels of risk when performing tasks. Risks should be diagnosed by hazard analysis techniques like the O&SHA. When risks are identified, they are either eliminated or controlled to an acceptable level by the application of hazard controls.

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

Commercial-off-the-shelf, non-developmental items (COTS NDI) pose risks that must be isolated by formal hazard analysis methods. The use of COTS-NDI does not ensure that the components or systems that they are used in are OSHA compliant. COTS NDI components cannot be considered as having been manufactured to any specific standards unless they have been tested by an NRTL. Therefore, the use of COTS-NDI requires the same system safety analysis as developmental items to ensure that they are manufactured and used in an acceptable manner.

## 12.9 Facility and Equipment Decommissioning

During activities associated with the decommissioning of a facility and/or equipment, hazardous materials may be found. There are numerous federal and state regulations governing the disposal of hazardous materials and hazardous waste. FAA equipment may contain numerous parts which contain hazardous materials such as:

- PCB capacitors and transformers
- Lead/acid, nickel/cadmium, and lithium batteries
- Beryllium heat sinks
- Cathode Ray Tube (CRT) displays containing lead and mercury
- Printed Circuit Boards (lead)
- Mercury switches and lights
- Lead and cadmium paint
- Asbestos

The identification of hazardous materials in facilities and equipment that have been designated for disposition. Failure to comply with these regulations can lead to fines, penalties, and other regulatory actions. As per the Federal Facilities Compliance Act of 1992, states and local authorities may fine and/or penalize federal officials for not complying with state and local environmental requirements.

Improper disposal of equipment containing hazardous materials would expose the FAA to liability in terms of regulatory actions and lawsuits (e.g. fines, penalties, and cleanup of waste sites)

There are many regulatory drivers when dealing with hazardous materials disposition. These include:

- Resource Conservation and Recovery Act (RCRA)
- Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA or Superfund)
- Superfund Reauthorization Act (SARA)

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

- National Environmental Policy Act (NEPA)
- Toxic Substance Control Act (TSCA)
- Federal Facilities Compliance Act of 1992 (FFCA)
- Community Environmental Response Facilitation Act (CERFA)
- DOT Shipping Regulations - Hazardous Materials Regulation
- OSHA Regulations (HAZCOM)
- State, local, and tribal laws
- FAA Orders
- Disposal guidance provided in FAA Order 4660.8, Real Property Management and Disposal
- Disposition guidance contained in FAA Order 4800.2C, Utilization and Disposal of Excess and Surplus Personal Property

## **12.10 Related Codes**

### **National Fire Protection Association (NFPA) Life Safety Code.**

The contents of any building or structure are classified as low, ordinary, or high. Low hazard contents are classified as those of such low combustibility that no self-perpetuating fire therein can occur. Ordinary hazard contents can be classified as those likely to burn with moderate rapidity or give off a considerable volume of smoke. High hazard contents shall be classified as those likely to burn with extreme rapidity or from which explosions are likely.

### **NFPA National Electrical Code (NEC)**

Locations are classified depending on the properties of the flammable vapors, liquids or gases, or combustible dusts or fibers that may be present in the likelihood that a flammable or combustible concentration or quantity is present period.

### **NFPA Hazard (Health) Identification System**

Materials are classified based on their potential for causing irritation, temporary health effects, minor residual injury, major residual injury and even death.

- Material that on exposure under fire conditions would offer no hazard beyond that of ordinary combustible material. (Example: peanut oil)
- Material that on exposure would cause irritation but only minor residual injury. (Example: turpentine)
- Material that on intense or continued but not chronic exposure could cause temporary incapacitation or possible residual injury. (Example: ammonia gas)

FAA System Safety Handbook, Chapter 12: Facilities Safety

December 30, 2000

- Material that on very short exposure could cause death or major residual injury.  
(Example: hydrogen cyanide)

FAA System Safety Handbook, Chapter 12: Facilities Safety  
December 30, 2000

## 12.11 Technical References

FAA Order 1600.46, Physical Security Review of New Facilities, Office Space or Operating Areas

FAA Order 3900.19, FAA Occupational Safety and Health Program.

FAA Order 8040.4, Safety Risk Management.

FAA Order 6000.15, General Maintenance Handbook for Airway Facilities

FAA-G-2100F, Electronic Equipment, General Requirements

Human Factors Design Guide. Daniel Wagner, U.S. Dept of Transportation, FAA, January 15, 1996.

National Fire Protection Association, National Fire Codes

*Code of Federal Regulations (CFR)*

Some examples:

- 29 CFR (Labor/OSHA)
- 40 CFR (Protection of Environment)
- 10 CFR (Energy)
- 49 CFR (Transportation)

Public Law 91-596; Executive Order 12196, Occupational Safety and Health Programs for Federal Employees

System Safety 2000, A Practical Guide for Planning, Managing, and Conducting System Safety Programs, J. Stephenson, 1991.

System Safety Analysis Handbook, System Safety Society (SSS), July 1993.

System Safety Engineering and Management, H. E. Roland and B. Moriarty, 1990.

## **Chapter 13:**

# **The Application of System Safety to the Commercial Launch Industry**

This chapter is intended for use as a pull-out handbook, separate from the FAA System Safety Handbook.

<b>13.1 INTRODUCTION.....</b>	<b>1</b>
<b>13.2 OFFICE OF COMMERCIAL SPACE TRANSPORTATION (AST).....</b>	<b>1</b>
<b>13.3 LICENSING PROCESS.....</b>	<b>2</b>
<b>13.4 SYSTEM SAFETY ENGINEERING PROCESS .....</b>	<b>5</b>
<b>13.5 SOFTWARE SAFETY .....</b>	<b>15</b>



## 13.0 The Application of System Safety To the Commercial Launch Industry

### 13.1 Introduction

The office of the Associate Administrator for Commercial Space Transportation (AST), under Title 49, U.S. Code, Subtitle IX, Sections 70101-70119 (formerly the Commercial Space Launch Act), exercises the FAA's responsibility to:

regulate the commercial space transportation industry, only to the extent necessary to ensure compliance with international obligations of the United State and to protect the public health and safety, safety of property, and national security and foreign policy interest of the United States, ...encourage, facilitate, and promote commercial space launches by the private sector, *recommend appropriate changes in Federal statutes, treaties, regulations, policies, plans, and procedures, and facilitate the strengthening and expansion of the United States space transportation infrastructure.* [emphasis added]

The mandated mission of the AST is "...to protect the public health and safety and the safety of property...."

AST has issued licenses for commercial launches of both sub-orbital sounding rockets and orbital expendable launch vehicles. These launches have taken place from Cape Canaveral Air Station (CCAS), Florida, Vandenburg Air Force Base (VAFB), California, White Sands Missile Range (WSMR), New Mexico, Wallops Flight Facility (WFF), Wallops Island, Virginia, overseas, and the Pacific Ocean.

AST has also issued launch site operator licenses to Space Systems International (SSI) of California, the Spaceport Florida Authority (SFA), the Virginia Commercial Space Flight Authority (VCSFA), and the Alaska Aerospace Development Corporation (AADC). SSI operates the California Spaceport located on VAFB; SFA the Florida Space Port located on CCAS; VCSFA the Virginia Space Flight Center located on WFF; and AADC the Kodiak Launch Complex, located on Kodiak Island, Alaska.

### 13.2 Office of Commercial Space Transportation (AST)

AST is divided into three functional components, the office of the Associate Administrator (AST-1), the Space Systems Development Division (SSDD), and the Licensing and Safety Division (LASD).

#### 13.2.1 The office of the Associate Administrator (AST-1)

AST-1 establishes policy, provides overall direction and guidance to ensures that the divisions function efficiently and effectively relative to the mandated mission "...to protect the public health and safety and the safety of property...."

#### 13.2.2 The Space Systems Development Division (SSDD)

The SSDD assess new and improved launch vehicle technology and their impacts upon both the existing and planned space launch infrastructures. SSDD works with the FAA and DOD Air Traffic Services to ensure full integration of space transportation flights into the Space and Air Traffic Management System. SSDD is AST's interface with the Office of Science and Technology Policy (OSTP), other Government agencies, and the aerospace industry working to create a shared 2010 space launch operations vision and in the development of the Global Positioning (Satellite) System (GPS) for the guidance of launch vehicles and tracking at ranges. SSDD is also engaged in analyzes of orbital debris and its impact to current and future space launch missions and the commercialization of outer space.

### 13.2.3 The Licensing and Safety Division (LASD)

LASD's primary objective is to carry out AST's responsibility to ensure public health and safety through the licensing of commercial space launches and launch site operations, licensing the operation of non-Federal space launch sites, and determining insurance or other financial responsibility requirements for commercial launch activities. AST/LASD looks to ensure protection of public health and safety and the safety of property through its licensing and compliance monitoring processes.

## 13.3 LICENSING PROCESS

The components of the licensing process include a pre-licensing consultation period, policy review, payload review, safety evaluation, financial responsibility determination, and an environmental review. The licensing process components most concerned with the application of system safety methodologies are the *safety evaluation*, *financial responsibility determination*, and *environmental determination*. A space launch vehicle requires the expenditure of enormous amounts of energy to develop the thrust and velocity necessary to put a payload into orbit. The accidental or inadvertent release of that energy could have equally enormous and catastrophic consequences, both near and far.

### 13.3.1 Safety Evaluation

It is the applicant's responsibility to demonstrate that they understand all hazards and risks posed by their launch operations and how they plan to mitigate them. Hazard mitigation may take the form of safety devices, protective systems, warning devices, or special procedures.

There are a number of technical analyses; some quantitative and some qualitative, that the applicant may perform in order to demonstrate that their commercial launch operations will pose no unacceptable threat to the public. The quantitative analyses tend to focus on 1) the reliability and functions of critical safety systems, and 2) the hazards associated with the hardware, and the risk those hazards pose to public property and individuals near the launch site and along the flight path, to satellites and other on-orbit spacecraft. The most common hazard analyses used for this purpose are Fault Tree Analysis, Failure Modes and Effects Analysis, and Over-flight Risk and On-Orbit Collision Risk analyses using the Poisson Probability Distribution. The qualitative analyses focus on the organizational attributes of the applicant such as launch safety policies and procedures, communications, qualifications of key individuals, and critical internal and external interfaces.

It is AST/LASD's responsibility to ensure that the hazard analyses presented by the applicant demonstrates effective management of accident risks by identifying and controlling the implicit as well as explicit hazards inherent in the launch vehicle and proposed mission. LASD must evaluate the applicant's safety data and safety related hardware/software elements and operations to ascertain that the demonstrations provided by the applicant are adequate and valid.

Specifically, the LASD evaluation is designed to determine if the applicant has:

- Identified all energy and toxic sources and implemented controls to preclude accidental or inadvertent release.
- Evaluated safety critical aspects, potential safety problems, and accident risk factors.
- Identified potential hazardous environments or events, and assessed their causes, possible effects and probable frequency of occurrence.
- Implemented effective hazard elimination, prevention or mitigation measures or techniques to minimize accident risk to acceptable levels.
- Specified the means by which hazard controls or mitigation methodology can be verified and validated.

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

### 13.3.2 Financial Responsibility Determination

Section 70112 of the Act requires that all commercial licensees demonstrate financial responsibility to compensate for the maximum probable loss from claims by:

- A third party for death, bodily injury, or property damage or loss resulting from an activity carried out under the license; and
- The U.S. Government against a person for damage or loss to government property resulting from an activity carried out under the license.

Section 70112 also requires that the Department of Transportation set the amounts of financial responsibility required of the licensee. The licensee can then elect to meet this requirement by:

- Proving it has financial reserves equal to or exceeding the amount specified, or
- Placing the required amount in escrow, or
- Purchasing liability insurance equal to the amount specified.

The most common and preferred method is via the purchase of liability insurance.

The methodology developed for setting financial responsibility requirements for commercial launch activities is called Maximum Probable Loss (MPL) analysis<sup>1</sup>. MPL analysis was developed to protect launch participants from the maximum probable loss due to claims by third parties and the loss of government property during commercial launch activities. Note that this is maximum probable loss, not maximum possible loss. Generally speaking, MPL is determined by identifying all possible accident scenarios, examining those with the highest potential losses for both government property and third party, and then estimating the level of loss that would not be exceeded at a given probability threshold. If the launch is to take place from a private licensed range and no government property is at risk, no government property financial responsibility requirement will be issued.

An integral part of, and critical input to the MPL, is the Facility Damage and Personnel\_(DAMP) Injury Analysis<sup>2</sup>: DAMP uses information about launch vehicles, trajectories, failure responses, facilities and populations in the launch area to estimate the risk and casualty expectations from impacting inert debris, secondary debris and overpressures from impact explosions. Together, the MPL and DAMP analyses are used to determine the financial responsibility determinations necessary to insure compensation for losses resulting from an activity carried out under the commercial license.

### 13.3.3 Environmental Determination

The environmental determination ensures that proposed commercial space launch activities pose no threat to the natural environment. The National Environmental Policy Act (NEPA) of 1969, as amended, requires that: Federal agencies consider the environmental consequences of major Federal actions; take actions that protect, restore, and enhance the environment; and ensure that environmental information is available to public officials and citizens before making decisions and taking action. The licensing of commercial space launch activities, either for a launch or launch site, is considered a major Federal action. Consequently, AST is responsible for analyzing the environmental impacts associated with proposed commercial space launch activities. AST is also responsible for the assessing the applicant's preparation and submittal of Environmental Assessments and Environmental Impact Statements to ensure compliance with the NEPA.

---

<sup>1</sup> Futron Corporation developed the MPL Analysis methodology employed by AST.

<sup>2</sup> Research Triangle Institute developed the DAMP Analysis methodology employed by AST.



## 13.4 SYSTEM SAFETY ENGINEERING PROCESS

### 13.4.1 Overview

The System Safety Engineering Process is the structured application of system safety engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness, time, and cost throughout all phases of a system's life cycle. The intent of the System Safety Engineering Process is to identify, eliminate, or control hazards to acceptable levels of risk throughout a system's life cycle.

This process is performed by the vehicle developer/operator. Because of the complexity and variety of vehicle concepts and operations, such a process can help ensure that all elements affecting public safety are considered and addressed. Without such a process, very detailed requirements would have to be imposed on all systems and operations, to ensure that all hazards have been addressed which could have the undesired effect of restricting design alternatives and innovation or could effectively dictate design and operations concepts.

The process (as described in Mil Std 882C) includes a System Safety Program Plan (SSPP). The SSPP (or its equivalent) provides a description of the strategy by which recognized and accepted safety standards and requirements, including organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort, are to be tailored and integrated with other system engineering functions. The SSPP lays out a disciplined, systematic methodology that ensures all risks – all events and system failures (probability and consequence) that contribute to expected casualty – are identified and eliminated, or that their probability of occurrence is reduced to acceptable levels of risk.

The SSPP should indicate the methods employed for identifying hazards, such as Preliminary Hazards Analysis (PHA), Subsystem Hazard Analysis (SSHA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis. Risk Mitigation Measures are likewise identified in the plan. These include avoidance, design/redesign, process/procedures and operational rules and constraints.

The System Safety Engineering Process identifies the safety critical systems. Safety critical systems are defined as any system or subsystem whose performance or reliability can affect public health and safety and safety of property. Such systems, whether they directly or indirectly affect the flight of the vehicle, may or may not be critical depending on other factors such as flight path and vehicle ability to reach populated areas. For this reason, it is important to analyze each system for each phase of the vehicle mission from ground operations and launch through reentry and landing operations. Examples of potentially safety critical systems that may be identified through the system safety analysis process using PHA or other hazard analysis techniques may include, but are not limited to:

- Structure/integrity of main structure
- Thermal Protection System (e.g., ablative coating)
- Temperature Control System (if needed to control environment for other critical systems)
- Main Propulsion System
- Propellant Tanks
- Power Systems
- Propellant Dumping System

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

- Landing Systems
- Reentry Propulsion System
- Guidance, Navigation and Control System(s), Critical Avionics (Hardware and Software) - includes Attitude, Thrust and Aerodynamic Control Systems
- Health Monitoring System (hardware and software)
- Flight Safety System (FSS)
- Flight Dynamics (ascent and reentry) for stability (including separation dynamics) and maneuverability
- Ground Based Flight Safety Systems (if any) including telemetry, tracking and command and control systems
- Depending on the concept, additional “systems” might include pilot and life support systems and landing systems if they materially affect public health and safety
- Others identified through hazard analysis

### 13.4.2 Validation of Safety Critical Systems

Through the system safety process, the applicant demonstrates that the proposed vehicle design and operations satisfy regulatory requirements and that the system is capable of surviving and performing safely in all operating environments including launch, orbit, reentry and recovery. Documentation must show adequate design, proper assembly, and vehicle control during all flight phases. Documentation is expected to consist of design information and drawings, analyses, test reports, previous program experience, and quality assurance plans and records.

AST uses a pre-application consultation process to help a potential applicant to understand what must be documented and to help identify potential issues with an applicant’s proposed activities that could preclude its obtaining a license. The pre-application process should be initiated by the applicant early in their system development (if possible during the operations concept definition phase) and maintained until their formal license application is completed. This pre-application process should be used to provide AST with an understanding of the safety processes to be used, the safety critical systems identified, analysis and test plan development, analysis and test results, operations planning and flight rules development.

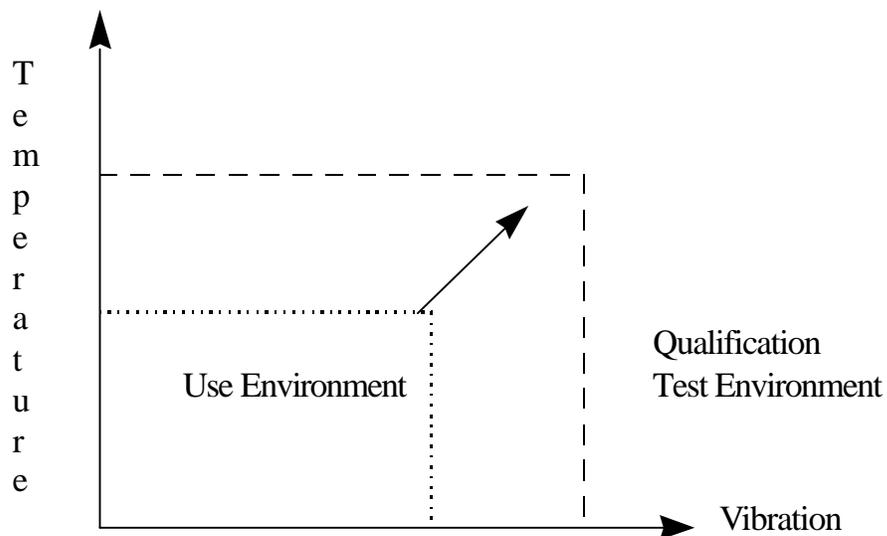
Analyses may be acceptable as the primary validation methodology in those instances where the flight regime cannot be simulated by tests, provided there is appropriate technical rationale and justification.

Qualification tests, as referenced in the safety demonstration process and the System Safety Program Plan, are normally conducted to environments higher than expected. For example, expendable launch vehicle (ELV) Flight Safety Systems (FSS) are qualified to environments a factor of two or higher than expected. (See Figure 13-2) These tests are conducted to demonstrate performance and adequate design margins and may be in the form of multi-environmental ground tests, tests to failure, and special flight tests. Such tests are normally preceded with detailed test plans and followed by test reports.<sup>3</sup>

---

<sup>3</sup> Test plans are important elements of the ground and flight test programs. Such plans define, in advance, the nature of the test (what is being tested and what the test is intended to demonstrate with respect to system functioning, system performance and system reliability). The test plan should be consistent with the claims and purpose of the test and wherever appropriate, depending on the purpose of the test, clearly defined criteria for pass and fail should be identified. A well-defined test plan and accompanying test report may replace observation by the FAA.

**Figure 13-2: Relationship of Use Environment to Qualification Test**



In addition, Quality assurance (QA) records are useful in establishing verification of both design adequacy and vehicle assembly and checkout (workmanship).

Table 13-1, Validation Acceptance Matrix, identifies sample approaches that may be employed to validate acceptance for critical systems. Examples of types of analyses, ground tests, and flight tests are provided following this matrix. (Note: Quality Assurance programs and associated records are essential where analysis or testing, covering all critical systems, are involved.)

**Table 13-1: Validation Acceptance Matrix**

Candidate Critical System	Analyses	Ground Test	Flight Test
Structure/Integrity of Main Structure	X	X	P
Thermal Protection	X	P	P
Environmental Control (temp, humidity)	X	X	X
Propulsion: Main, Auxiliary and Reentry (de-orbit)	X	P	P
Propellant Tank Pressurization	X	X	P
GN&C, Critical Avionics *; includes de-orbit targeting (e.g., star-tracker, GPS)	X	X	X
Health Monitoring *	X	X	X
Flight Safety System (FSS)*	X	X	X
Recovery and Landing*	X	P	P
Ordnance* (other than Safety)	X	X	X
Electrical and Power*	X	X	X
Telemetry and Tracking and Command*	X	X	X
Flight Control (ascent, separation, reentry) *	X	X	X
FSS Ground Support Equipment (if any) *	X	X	N/A

*P - partial; cannot satisfy all aspects*

X - If in sufficient detail when combined with test results or selected analyses

\* - Includes both hardware and software

### 13.4.3 Analyses

There are various types of analyses that may be appropriate to help validate the viability of a critical system or component. The following provides examples of some types of critical systems analysis methodologies and tools.

- Mechanical Structures and Components (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)
- Types of Analyses: Structural Loads, Thermal, Fracture Mechanics, Fatigue, Form Fit & Function
- Software Tools for Analyses: Nastran, Algor, Computational Fluid Dynamics codes, CAD/CAM
- Thermal Protection System
- Types of Analyses (for TPS and Bonding Material): Transient and Steady State Temperature Analyses, Heat Load, and Heating and Ablative Analyses.
- Software Tools for Analyses: SINDA by Network Analysis Inc.
- Electrical/Electronic Systems & Components (Electrical, Guidance, Tracking, Telemetry, Navigation, Communication, FSS, Ordnance, Flight Control and Recovery)
- Types of Analyses: Reliability, FMEA, Single Failure Point, Sneak Circuit, Fault Tree, Functional Analysis, Plume effects
- Software Tools for Analyses: MathCad, Relex, and FaultrEase
- Propulsion Systems (Propulsion, FSS, Ordnance, Flight Control)
- Types of Analyses: Analytical Simulation of nominal launch and abort sequences for Main Engines, Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; capacity analysis for consumables; Plume Flow Field Modeling
- Software Tools for Analyses: Nastran, Algor, SPF-III, and SINDA
- Aerodynamics (Structure, Thermal, Recovery)
- Types of Analyses: Lift, Drag, Stability, Heating, Performance, Dispersion, Plume effects
- Software Tools for Analyses: Post 3/6 DOF, Computational Fluid Dynamics Codes Monte Carlo Simulation Codes
- Software (Guidance, Tracking & Telemetry & Command, FSS, Flight Control and Recovery)
- Types of Analyses: Fault Tree, Fault Tolerance, Software Safety (including abort logic), Voting Protocol Dead Code, Loops, and Unnecessary Code
- Validation Methodologies, such as ISO 9000-3<sup>4</sup>

---

<sup>4</sup> ISO 9000-3 is used in the design, development, and maintenance of software. Its purpose is to help produce software products that meet the customers' needs and expectations. It does so by explaining how to control the quality of both products and the processes that produce these products. For software product quality, the standard highlights four measures: specification, code reviews, software testing and measurements.

#### 13.4.4 Ground Test

Ground tests include all testing and inspections performed by the applicant prior to flight, including qualification, acceptance and system testing. It is anticipated that an applicant will perform various types of ground tests to validate the capability of critical systems and components. The following provides examples of some types of critical systems validation ground tests. Again these are *only examples* and should not be construed as the only types of ground tests which may be used to validate a specific system for a specific operational environment, nor should it be interpreted that all of these example ground tests will be necessary to validate a specific system.

**Mechanical Systems and Components** (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)

*Types of Tests:* Load, Vibration (dynamic and modal), Shock, Thermal, Acoustic, Hydro-static, Pressure, Leak, Fatigue, X-ray, Center of Gravity, Mass Properties, Moment of Inertia, Static Firing, Bruceton Ordnance, Balance, Test to Failure (simulating non-nominal flight conditions), Non-Destructive Inspections

**Electrical/Electronic Systems** (Electrical, Guidance, Tracking, Telemetry and Command, Flight Safety System (FSS), Ordnance, Flight Control and Recovery)

*Types of Tests:* Functional, Power/Frequency Deviation, Thermal Vacuum, Vibration, Shock, Acceleration, X-ray, recovery under component failures, abort simulations, TDRSS integration testing (up to and including pre-launch testing with flight vehicle)

**Propulsion Systems** (Propulsion, FSS, Ordnance, Flight Control)

*Types of Tests:* Simulation of nominal launch and abort sequences for engines (including restart, if applicable), Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; Environmental testing (Thermal, Vibration, Shock, etc.)

**Thermal Protection System**

*Types of Tests* (for TPS and bonding material): Thermal, Vibration, Humidity, Vacuum, Shock

**Aerodynamics** (Structure, Thermal, Recovery)

*Types of Tests:* Wind Tunnel, Arc Jet, Drop Tests (Landing Systems)

**Software** (Electrical, Guidance, Tracking, Telemetry, Command, FSS, Ordnance, Flight Control and Recovery)

*Types of Tests:* Functional, Fault Tolerance, Cycle Time, Simulation, Fault Response, Independent Verification and Validation, Timing, Voting Protocol, Abort sequences (flight and in-orbit) under non-nominal conditions with multiple system failures, Integrated Systems Tests

#### 13.4.5 Flight Tests

If an applicant's System Safety Plan includes a flight test program, then a considerable amount of planning is needed to define the flight test program that will establish the performance capabilities of the vehicle for routine and repetitive commercial operations. When flight testing is indicated, a flight test plan will be needed to demonstrate that the vehicle's proposed method of operations is acceptable and will not be a hazard to the public health and safety, and safety of property.

The purpose of flight-testing is to verify the system performance, validate the design, identify system deficiencies, and demonstrate safe operations. Experience repeatedly shows that while necessary and important, analyses and ground tests cannot and do not uncover all potential safety issues associated with new launch systems. Even in circumstances where all known/identified safety critical functions can be

exercised and validated on the ground, there is still the remaining concern with unrecognized or unknown interactions (“the unknown unknowns”).

The structure of the test program will identify the flight test framework and test objectives, establish the duration and extent of testing; identify the vehicle’s critical systems, identify the data to be collected, and detail planned responses to nominal and unsatisfactory test results.

Test flight information includes verification of stability, controllability, and the proper functioning of the vehicle components throughout the planned sequence of events for the flight. All critical flight parameters should be recorded during flight. A post-flight comparative analysis of predicted versus actual test flight data is a crucial tool in validating safety critical performance. Below are examples of items from each test flight that may be needed to verify the safety of a reusable launch vehicle. Listed with each item are examples of what test-flight data should be monitored or recorded during the flight and assessed post-flight:

<p><b>Vehicle/stage launch phase:</b> Stability and controllability during powered phase of flight.</p> <ul style="list-style-type: none"> <li>• Vehicle stage individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration, mixture ratio, thrust, specific impulse (ISP)</li> <li>• Vehicle stage trajectory data (vehicle position, velocity, altitudes and attitude rates, roll, pitch, yaw attitudes)</li> <li>• Vehicle stage Attitude, Guidance and Control system activities</li> <li>• Functional performance of the Vehicle Health Monitoring System</li> <li>• Functional performance of the Flight Safety System/Safe Abort System</li> <li>• Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc...)</li> <li>• Actual thermal and vibroacoustic environment</li> <li>• Actual structural loads environment</li> </ul>
<p><b>Staging/separation phase of boost and upper stages:</b> Stable shutdown of engines, and nominal separation of the booster &amp; upper stages.</p> <ul style="list-style-type: none"> <li>• Separation activity (timestamp, i.e., separation shock loads, and dynamics between stamps)</li> <li>• Functional performance of the Vehicle Health Monitoring System</li> <li>• Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc...)</li> <li>• Functional performance of the Flight Safety System/Safe Abort System</li> </ul>
<p><b>Booster stage turn-around (re-orientation) or “loft” maneuver phase</b> (if applicable):</p> <ul style="list-style-type: none"> <li>• Rocket motor re-start (if applicable): timing, updates on propellant flow rates, chamber temperature, chamber pressure, burn duration, mixture ratio, thrust, ISP</li> <li>• Attitude, Guidance and Control system activities</li> <li>• Actual structural loads environment</li> <li>• Actual thermal and vibroacoustic environment</li> </ul>

- Functional performance of the Flight Safety System/Safe Abort System

**Booster stage flyback phase** (if applicable): Flyback engine cut-off, fuel dump or vent (if required), nominal descent to the planned impact area, proper functioning and reliability of the RLV landing systems.

- Booster stage post-separation (flyback) trajectory data
- Electrical power usage and reserves
- Booster stage landing system deployment activity (timestamp)
- Actual thermal and vibroacoustic environment
- Actual structural loads environment
- Functional performance of the Vehicle Health Monitoring System
- Functional performance of the Flight Safety System/Safe Abort System
- Attitude, Guidance and Control system activities

**Vehicle stage ascent phase** (if multistage): nominal ignition of the stage's engine, stability and controllability of the stage during engine operation, orbital insertion – simulated (for suborbital) or actual – of the vehicle.

- Vehicle individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration
- Vehicle circularization and phasing burn activities (ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration)
- Vehicle trajectory data (vehicle position, altitude, velocity, roll, pitch, yaw attitudes at a minimum)
- Attitude, guidance and control system activities
- Functional performance of the Vehicle Health Monitoring System
- Functional performance of the Flight Safety System/Safe Abort System
- Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc...)
- Actual structural loads environment
- Actual thermal and vibroacoustic environment

**Vehicle descent** (including vehicle's de-orbit burn targeting and execution phases): Function of the programmed flight of the vehicle/upper stage to maintain the capability to land (if reusable) at the planned landing site, or to reenter for disposal (if expendable), assurance of fuel dump or depletion, and proper descent and navigation to the planned or alternate landing site.

- Vehicle pre-deorbit burn trajectory data
- Vehicle deorbit burn data (ignition timing, updates on propellant flow rate, chamber temperature, chamber pressure, and burn duration)
- Vehicle descent trajectory data (position, velocity, and attitude)
- Attitude, Guidance and Control system activities

- Actual thermal and vibroacoustic environment
- Actual structural loads environment
- Functional performance of the Vehicle Health Monitoring System
- Functional performance of the Flight Safety System/Safe Abort System
- Electrical power and other critical consumables usage and reserves (i.e. gases, fluids, etc...)
- Vehicle landing system deployment activity (timestamp)

#### **13.4.6 Performance and Reliability Data**

Performance and reliability data may be supported by flight history on other vehicles with similar or comparable safety critical systems, sub-systems, and components, and by conducting both analyses and tests, at the respective levels. A flight history could mean extensive documentation might not be required if it can be shown through test results, analyses, or empirical data, that the flight regimes experienced are similar to the proposed flight regime. The degree of applicability of data depends on the degree of similarity to environmental conditions and how environmental conditions compare to the history and anticipated reactions of this system. Even when the same system, sub-system, or component is known to have an extensive (and favorable) flight history in the same or more severe environments, interfaces and integration with other systems must still be examined and tested. Another method of acquiring data is through estimating system, sub-system, and component 3-sigma performance and reliability numbers from testing evaluations and (where applicable) flight data.

The use of similarity is not new to launch operations. EWR 127-1, Paragraph. 4.14.1.2, states: as required, qualification by similarity analysis shall be performed; if qualification by similarity is not approved, then qualification testing shall be performed. For example, if component A is to be considered as a candidate for qualification by similarity to a component B that has already been qualified for use, component A shall have to be a minor variation of component B. Dissimilarities shall require understanding and evaluation in terms of weight, mechanical configuration, thermal effects, and dynamic response. Also, the environments encountered by component B during its qualification or flight history shall have to be equal to or more severe than the qualification environments intended for component A.

#### **13.4.7 Operational Controls**

There is an interrelationship between the system design capabilities and the systems operational limitations. Figure 2 depicts the relationship between the vehicle systems and the scope of operations within which the vehicle is operated. What constitutes a safety critical system may depend on the scope and nature of the vehicle design and its proposed operations. Intended operational requirements affect the proposed vehicle design requirements and vehicle capabilities/limitations and also establish the operational system constraints necessary to protect public health and safety. For example, reusable launch vehicle landing sites may have to be within some minimum cross-range distance from the orbital ground trace because of cross-range limitations of the vehicle. A vehicle operator may choose, or be required, to mitigate certain vehicle limitations through the use of operational controls rather than relieving vehicle limitations through design changes.

Test parameters and analytic assumptions will further define the limits of flight operations. The scope of the analyses and environmental tests, for example, will constitute the dimensions of the applicant's demonstration process and therefore define the limits of approved operations if a license is issued. Such testing limits, identified system and subsystem limits, and analyses also are expected to be reflected in

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

mission monitoring and mission rules addressing such aspects as commit to launch, flight abort, and commit to reentry.

Vehicle capabilities/limitations and operational factors such as launch location and flight path each affect public risk. The completion of system operation demonstrations, such as flight simulations and controlled flight tests, provide additional confidence in the vehicle systems and performance capabilities. As confidence in the systems overall operational safety performance increases, key operational constraints such as restrictions on overflight of populated areas may be relaxed.

The following are examples of the types of operations-related considerations that may need to be addressed by the applicant when establishing their operations scenarios.

Launch commit criteria/rules

Human override capability to initiate safe abort during launch and reentry

System monitoring, inspection and checkout procedures

For re-flight: inspection and maintenance

Selected primary and alternate landing sites for each stage

Surveillance/control of landing areas

Standard limits on weather

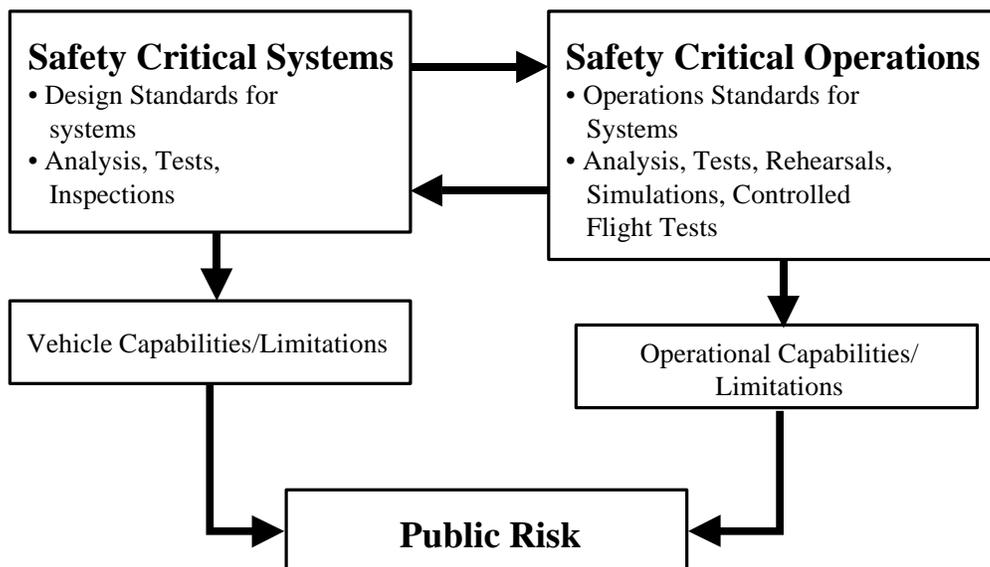
Coordination with appropriate air space authorities

Limits on flight regime (ties in with analysis, testing and demonstrating confidence in system performance and reliability)

Limits on over-flight of populated areas

Others identified through hazard analysis

**Figure 13-2: Interrelationship between Safety Critical Systems and Safety Critical Operations**



#### 13.4.8 Determination of Risk to the Public

Expected casualty is used in the space transportation industry as a measure of risk to public safety. Expected casualty is the expected average number of human casualties per mission. Human casualty is defined as a fatality or serious injury. The application of the expected casualty analysis to determine public risk is further defined in FAA Advisory Circular 431-02.

#### 13.4.9 Determination of Need for Additional Risk Mitigation

The results of the expected casualty analysis may identify the need for additional risk mitigation measures that need to be employed. These measures may include additional operational controls or may require the redesign of certain safety critical systems. These additional risk mitigation measures would be evaluated within the System Safety Process and the resultant risk to the public would be determined.

### 13.5 SOFTWARE SAFETY

#### 13.5.1 Safety Critical Software

Safety-critical software plays an ever-increasing role in Commercial Space Transportation (CST) computer systems. To preserve CST flight integrity, software-based hazards must be identified and eliminated or reduced to acceptable levels of risk. Particular concern surrounds potential software-induced accidents occurring during CST launch and reentry. Due to mission complexity, software failures manifested at these critical times can cause serious accidents. Populated areas would suffer major harm if defective software were to permit CST vehicles to violate their defined safety launch limits. Safety-critical software, relative to CST launch vehicles, payloads and ground support equipment is inherently defined as any software within a control system containing one or more hazardous or safety critical functions. Safety critical functions are usually but not always associated with safety-critical systems. Therefore, the following definition for safety –critical systems may also be applied to safety-critical functions. A safety-critical system (or function) has been inherently defined as any system or subsystem

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

(or function) whose performance or reliability can affect (i.e. malfunction or failure will endanger) public health, safety and safety of property.<sup>5</sup>

### **13.5.2 Systematic Software Safety Process**

#### ***Introduction***

The Systematic Software Safety Process (SSSP) encompasses the application of an organized periodic review and assessment of safety-critical software and software associated with safety-critical system, subsystems and functions. The Systematic Software Safety Process consist primarily of the following elements:

- Software safety planning
- The software safety organization
- A software safety team
- Application of the software safety process during all life cycle phases
- Identification and application of life cycle phase-independent software safety activities
- Identification of special provisions
- Software safety documentation

#### ***Software Safety Planning***

Software system safety planning is deemed essential early in the software life cycle. Most importantly, planning should impose provisions for accommodating safety well before each of the software design, coding, testing, deployment and maintenance phases starts in the cycle. Moreover, these provisions are to be planned carefully to impact minimally the software development process. The software system safety plan should contain provisions assuring that:

- Software safety organization is properly chartered and a safety team is commissioned in time.
- Acceptable levels of software risk are defined consistently with risks defined for the entire system.
- Interfaces between software and the rest of the system's functions are clearly delineated and understood.
- Software application concepts are examined to identify safety-critical software functions for hazards.
- Requirements and specifications are examined for safety hazards (e.g. identification of hazardous commands, processing limits, sequence of events, timing constraints, failure tolerance, etc.)
- Design and implementation is properly incorporated into the software safety requirements.
- Appropriate verification and validation requirements are established to assure proper implementation of software system safety requirements.
- Test plans and procedures can achieve the intent of the software safety verification requirements.

---

<sup>5</sup> Reference D.

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

- Results of software safety verification efforts are satisfactory.

The Institute of Electrical and Electronic Engineering (IEEE) offers a comprehensive standard (Standard for Software Safety Plans) focusing solely on planning. The Standard articulates in sufficient detail both software safety management and supporting analyses. The Standard's annex describes the kind of analyses to be performed during the software requirements, design, code, test and change phases of the traditional life cycle. Similar planning models are provided by the Department of Defense (DOD) Defense Standard 00-55-Annex B.

### ***Software Safety Organization***

Safety oversight consists of a staff function crossing several organizational boundaries. By its nature, it is meant to interact with other staff and line functions, including program or project management, software system design, quality assurance, programming, reliability, testing, human factors, and operations. Accountability-wise, the ultimate responsibility for the development and operation of a safe software system(s) rests with the CST applicant or licensed operator. Thus, the applicant's or operator's top management should be committed to supporting the software safety process across all these staff and line functions.

A software safety organization can take one of many shapes, depending on the needs of the applicant or licensed operator. However, the following requisites are recommended:

- Centralized authority and responsibility dedicated to the safety initiatives
- Safety team independence, and
- High enough safety team status relative to the rest of the organization.

Centralization allows a single organization to focus entirely on hazards and their resolutions during any life cycle phase, be it design, coding or testing. Independence prevents bias and conflicts of interest during organizationally sensitive hazard assessment and management. A high status empowers the team to conduct its mission with sufficient visibility and importance. By endorsing these requisites, CST applicants and operators will indicate they are attentive to the safety aspects of their project or mission.

### ***Software Safety Team***

Safety planning also calls for creating a software safety team. Team size and shape depends commensurately on mission size and importance. To be effective, the team should consist of analytical individuals with a sufficient system engineering background. Military Standard (MIL STD) 882C provides a comprehensive matrix of minimum qualifications for key system safety personnel. It can apply to software system safety as well, provided professional backgrounds include sufficient experience with software development (software requirements, design, coding, testing, etc.)

Several typical activities expected of the team range from identifying software-based hazards to tracing safety requirements and limitations in the actual code, to developing software safety test plans and reviewing test results for their compliance with safety requirements.

### ***Software Safety During Life Cycle Phases***

The SSSP should support a structured program life cycle model that incorporates both the system design and engineering, and software acquisition process. Prominent software life cycle models include the

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

waterfall and spiral methodologies. Although different models may carry different lifecycle emphasis, the adopted model should not affect the SSSP itself. For discussion purposes only, this enclosure adopts a waterfall model (subject to IEEE/IEA Standard for Information Technology-software life cycle processes No. 12207.) For brevity, only some phases (development, operation, maintenance and support) of the Standard are addressed in terms of their relationship to software safety activities. This relationship is summarized in Table 13-2 The table's contents partly reflect some of the guidance offered by the National Aeronautics and Space Administration (NASA) Standard 8719.13A and NASA Guidebook GB-1740.13-96.

**Table 13-2: Software Safety Activities Relative to the Software Life Cycle**

<b>Life Cycle Phase</b>	<b>Corresponding Safety Activity</b>	<b>Inputs</b>	<b>Expected Results</b>	<b>Milestones To Be Met</b>
<b>Concept/ Requirements/ Specifications</b>	<ul style="list-style-type: none"> <li>-Review software concept for safety provisions</li> <li>-Derive generic and system-specific software safety requirements.</li> <li>-Analyze software requirements for hazards.</li> <li>-Identify potential software/system interface hazards</li> <li>-Develop Functional Hazards List (FHL)</li> <li>-Develop initial Preliminary Software Hazard Analysis (PSHA)</li> </ul>	<ul style="list-style-type: none"> <li>-Preliminary Hazard Analysis (PHA) [from system safety analysis]</li> <li>-Generic and system-wide safety specs.</li> </ul>	PSHA Report PHL	<ul style="list-style-type: none"> <li>Software Concept Review (SCR)</li> <li>Software Requirements Review (SRR) and Software Specification Review (SSR)</li> </ul>
<b>Architecture/ Preliminary Software Design</b>	<ul style="list-style-type: none"> <li>At high design level:</li> <li>-Identify Safety Critical Computer Software Components (SCSCs)</li> <li>-Verify correctness &amp; completeness of architecture</li> <li>-Ensure test coverage of software safety requirements.</li> </ul>	PSHA	Software Safety Architectural Design Hazard Analysis (SSADHA) Report	Preliminary Design Review (PDR)
<b>Detailed Design</b>	<ul style="list-style-type: none"> <li>At the low design(unit) level:</li> <li>-Focus on SCSCs at the unit level.</li> <li>-Verify correctness/ completeness of detail. Design</li> </ul>	PSHA SSADHA	Software Safety Detailed Design Hazard Analysis (SSDDHA) Report	Critical Design Review (CDR)
<b>Implementation Coding</b>	<ul style="list-style-type: none"> <li>-Examine correctness &amp; completeness of code from safety requirements.</li> <li>-Identify possibly unsafe code.</li> <li>-Walk-through/audit the code</li> </ul>	PSHA, SSADHA, SSDDHA	Software Safety Implementation Hazard Analysis (SSIHA) report	Test Readiness Review (TRR)
<b>Integration and Testing</b>	<ul style="list-style-type: none"> <li>-Ensure test coverage of software safety requirements.</li> <li>-Review test documents and results for safety requirements.</li> <li>-Final SSHA</li> </ul>	Test documents	<ul style="list-style-type: none"> <li>-Software Safety Integration Testing (SSIT) Report</li> <li>-Final SSHA report</li> </ul>	Acceptance
<b>Operations and Maintenance</b>	<ul style="list-style-type: none"> <li>-Operating and Support Hazard Analysis (O&amp;SHA)</li> </ul>	All of the above plus all incidents reports	O&SHA Report(s), as required	Deployment

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

Figure 3 provides a composite overview of the entire safety process. The figure consists of three parts. The top part reflects the broader System Safety Process described in draft Advisory Circular 431.35-2. The middle part illustrates a typical waterfall Software Acquisition Process life cycle. The bottom part also partly corresponds to the Systematic Software Safety Process. In Figure 3, all processes shown in horizontal bars are subject to a hypothetical schedule with time duration not drawn to any scale.

### ***Phase-independent software safety activities***

NASA's Software Safety Standard 8719.13A mentions activities not tied to specific phases. The Standard lists the following ones meant to occur throughout the life cycle:

- Tracing safety requirements keeping track of the software safety requirements during design, coding and testing, including the correspondence between these requirements and the system hazard information.
- Tracking discrepancies between the safety and development aspects of the software.
- Tracking changes made to the software to see if they impact the safety process.
- Conducting safety program reviews to verify if safety controls are being implemented to minimize hazards.

### ***Special Provisions***

***Commercial Off the Shelf (COTS):*** COTS software targets a broad range of applications, with no specific one envisioned ahead of time. Therefore, care must be taken to ensure COTS software presence minimizes risk when it becomes embedded or coupled to specific applications. Consideration ought to be given to designing the system such that COTS software remains isolated from safety-critical functions. If isolation is not possible, then safeguards and oversight should be applied.

***Software Reuse:*** Reusable software originates from a previous or different application. Usually, developers intend to apply it to their current system, integrating it "as is" or with some minor modifications. The Software Safety Team verification/validation plan, etc.) Annex B should serve as a general model for preparing software safety documents

The results of most of the safety analyses activities usually require preparing several hazard analysis reports documenting the findings of the safety team. The team has also the responsibility of presenting their findings to decision-making management at critical milestones, like the Software Requirements Review (SRR), Preliminary Design Review (SDR), Critical Design Review (CDR), etc. Towards this end, DOD Defense Standard 00-55-Annex E describes how to prepare a software safety "case". The Standard defines a case as "a well-organized and reasoned justification, based on objective evidence, that the software does or will satisfy the safety aspects of the Software Requirement".

### **13.5.3 Software Safety Documentation**

Numerous documents are to be prepared and distributed during the SSSP. To track them, a comprehensive checklist, such as that cited in MIL STD 882 may be applied. Two highly recommended documents are the Safety Assessment Report (SAR) and the System Safety Hazard Analysis Report (SSHA). DOD Defense Standard 00-55-Annex B offers a detailed outline of the contents of numerous software safety documents (software safety plan, case or report, records log, audit plan, audit report, quality plan, risk management plan, verification/validation plan, etc.) Annex B should serve as a general model for preparing software safety documents. The results of most of the safety analyses activities usually require preparing several hazard analysis reports documenting the findings of the safety team.

The team also has the responsibility of presenting their findings to decision-making management at critical milestones, like the Software Requirements Review (SRR), Preliminary Design Review (SDR),

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

Critical Design Review (CDR), etc. Towards this end, DOD Defense Standard 00-55-Annex E describes how to prepare a software safety “case”. The Standard defines a case as “a well-organized and reasoned justification, based on objective evidence, that the software does or will satisfy the safety aspects of the Software Requirement”.

#### **13.5.4 Safety Critical Software functions**

Software can be labeled defective if it does not perform as expected. Major classes of defects are:

- Software not executing
- Software executing too late, too early, suddenly or out of sequence, or
- Software executing but producing wrong information.

In turn, defective software can be labeled hazardous if it consists of safety-critical functions that command, control and monitor sensitive CST systems. Some typical software functions considered safety-critical include:

- Ignition Control: any function that controls or directly influences the pre-arming, arming, release, launch, or detonation of a CST launch system.
- Flight Control: any function that determines, controls, or directs the instantaneous flight path of a CST vehicle.
- Navigation: any function that determines and controls the navigational direction of a CST vehicle.
- Monitoring: any function that monitors the state of CST systems for purposes of ensuring its safety.
- Hazard Sensing: any function that senses hazards and/or displays information concerning the protection of the CST system.
- Energy Control: any function that controls or regulates energy sources in the CST system.
- Fault Detection: any function that detects, prioritizes, or restores software faults with corrective logic.
- Interrupt Processing: any function that provides interrupt priority schemes and routines to enable or disable software-processing interrupts.
- Autonomous Control: any function that has autonomous control over safety-critical hardware.
- Safety Information Display: any function that generates and displays the status of safety-critical hardware or software systems.
- Computation: any function that computes safety-critical data.

### 13.5.5 Software Safety Risk and Hazard Analysis

#### ***Risk Assessment***

A key element in system safety program planning is the identification of the acceptable level of risk for the system. The basis for this is the identification of hazards. Various methodologies used in the identification of hazards are addressed in Sections 2.3 & 2.4 of draft AC 431.35-2. Once the hazards and risks are identified, they need to be prioritized and categorized so that resources can be allocated to the functional areas having an unacceptable risk potential. Risk assessment and the use of a Hazard Risk Index (HRI) Matrix as a standardized means with which to group hazards by risk are described in Attachment 2, Sections 6.1 & 6.2 of draft AC 431.35-2. This section presents specialized methods of analyzing hazards, which possess software influence or causal factors and supplements the HRI presented in draft AC 431.35-2.

The Hazard Risk Index presented in draft AC 431.35-2 is predicated on the probability of hazard occurrence and the ability to obtain component reliability information from engineering sources. Hardware reliability modeling of a system is well established; however, there is no uniform, accurate or practical approach to predicting and measuring the software reliability portion of the system. Since software does not fail in the same manner as hardware, in that it is not a physical entity, it does not wear out, break, or degrade over time; software problems are referred to as a software error. Software errors generally occur due to implementation or human failure mechanisms (such as documentation errors, coding errors, incorrect interpretation of design requirements, specification oversight, etc.) or requirement errors (failure to anticipate a set of conditions that lead to a hazard). Unlike hardware, software has many more failure paths than hardware, making it difficult to test all paths. Thus the ultimate goal of software system safety is to find and eliminate the built-in unintended and undesired hazardous functions driven by software in a CST system.

#### ***Classification of Software Safety Risk***

There are two basic steps in classifying safety risk for software. The first being the establishment of severity within the context of the CST system and then applying an acceptable methodology for determining the software's influence on system level risks. Refer to Figures 13-4 and 13-5. Regardless of the contributory factors (hardware, software, or human error) the severity of risk as present in draft AC 431.35-2 Attachment 2, Section 6.1.2, Figure 6.1.2, remain applicable criteria for the determination of hazard criticality for those risks possessing software contributory factors.

The second half of the equation for the classification of risk is applying an acceptable methodology for determining the software's influence on system level hazards. The probability factors contained in draft AC 431.35-2 has been determined for hardware based upon historical "best" practices. Data for the assignment of accurate probabilities to software error has not matured. Thus alternate methods for determining probability propagated by software causal factors need to be used. Numerous methods of determining software effects on hardware have been developed and two of the most commonly used are presented in MIL-STD 882C and RTCA DO-178 and are shown in Figure 4. These methods address the software's "control capability" within the context of the software causal factors. An applicant Software System Safety Team should review these lists and tailor them to meet the objectives of their CST system and integrated software development program.

This activity of categorizing software causal factors is for determining both likelihood, and the design, coding, and test activities required to mitigate the potential software contributor. A Software Hazard

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

Criticality (SHC) Matrix, similar to the hazard risk index (HRI)<sup>6</sup> matrix is used to determine the acceptability of risk for software hazards. Figure 3 shows an example of a typical SHC matrix using the control categories of MIL-STD 882C [Mil882C]. The SHC matrix can assist the software system safety team in allocating software safety requirements against resources and in the prioritization of software design and programming tasks.

### ***Software Hazard Analysis/Risk Mitigation***

Fault tree analysis (FTA) may be used to trace system-specific software safety-critical functional hazards<sup>7</sup>. The hazard software causal factor nodes are then traced to the appropriate mitigating CST System Requirement, design segment, and coding segment. The hazard should be tracked through the test procedure development; to assure the test procedures have been written sufficiently to demonstrate the hazard is adequately controlled (mitigated).

### ***Software Safety Analysis Methods and Tools<sup>8</sup>***

The following is not intended to be an all-inclusive or exhaustive list of software safety analysis methods and tools; nor does it represent an explicit or implicit AST recommendation thereof.

---

<sup>6</sup> See Attachment 2, Section 6.2 of AC 431.35-2 for discussion and illustration of HRI.

<sup>7</sup> The actual analysis techniques used to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how they should be met should be addressed in the applicant's System Safety Program Plan. The System Safety Society's System Safety Handbook identifies additional system safety analysis techniques that can be used.

<sup>8</sup> Reference E

<b>MIL-STD 882C</b>	<b>RTCA-DO-178B</b>
<p>(I) Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.</p> <p>II(a) Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.</p> <p>II(b) Software item displays information requiring immediate operator action to mitigate a hazard. Software failure will allow or fail to prevent the hazard's occurrence.</p> <p>III(a) Software items issues commands over potentially hazardous hardware systems, subsystem, or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.</p> <p>III(b) Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.</p> <p>(IV) Software does not control safety critical hardware systems, subsystems, or components and does not provide safety critical information.</p>	<p>(A) Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the vehicle.</p> <p>(B) Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a hazardous/severe major failure condition of the vehicle.</p> <p>(C) Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a major failure condition for the vehicle.</p> <p>(D) Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a minor failure condition for the aircraft.</p> <p>(E) Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of function with no effect on vehicle operational capability or pilot workload. Once software has been confirmed as level E by the certification authority, no further guidelines of this document apply.</p>

**Figure 13-3: Software Hazard Criticality Matrix\***

<b>CONTROL CATEGORY</b>	<b>CATASTROPHIC</b>	<b>CRITICAL</b>	<b>MARGINAL</b>	<b>NEGLIGIBLE</b>
(I) S/W without possibility of intervention- leads directly to hazard occurrence	1	1	3	5
(IIa) S/W with time for intervention- can not stand alone	1	2	4	5
(IIb) S/W displays information but requires operator to mitigate hazard - allow or fail to prevent hazard occurrence.	1	2	4	5
(IIIa) S/W issues commands requiring human action to complete control function- several redundant, independent measures for each event.	2	3	5	5
(IIIb) S/W generate information of a safety critical nature to make safety critical decisions - several redundant, independent measures for each event.	2	3	5	5
(IV) S/W does not control safety critical H/W systems or provide safety-critical information	3	4	5	5

- 1 High Risk      Significant Analyses and Testing Resources  
2 Medium Risk    Requirements and Design Analysis and Dept Test Required  
3 Moderate Risk   High Levels of Analysis and Testing Acceptable with Managing Activity Approva  
4 Moderate Risk   High Levels of Analysis and Testing Acceptable with Managing Activity Approv  
5 Low Risk        Acceptable

\*Extracted from MIL-STD 882C

It is intended to provide a limited representative sampling of those software safety analysis methods and tools available to the CST licensee or operator. General systems safety analysis have been omitted in that they are addressed in Paragraph 4.3. It is the licensee or operator's responsibility to assess the applicability and viability of a particular analysis method or tool to their CST, methods of operations, and organizational capabilities.

- **Code Inspection:** a formal review process during which a safety team checks the actual code, comparing it stepwise to a list of hazard concerns.
- **Hardware/Software Safety Analysis<sup>9</sup>:** this analysis is a derivative of the system PHA<sup>10</sup>. The PHA when integrated with the requirements leveled upon the software will identify those programs, routines, or modules that are critical to system safety and must be examined in depth.
- **Software Failure Modes and Effects Analysis (SFMEA)<sup>11</sup>:** identifies software related design deficiencies through analysis of process flow-charting. It also identifies interest areas for verification /validation and test and evaluation. Technique is used during and after the development of software specifications. The results of the PHA and SSHA, if complete, can be used as a guide for focusing the analysis.
- **Software Fault Tree Analysis (SFTA)<sup>12</sup>:** used to identify the root cause(s) of a “top” undesired event. When a branch of the hardware FTA leads to the software of the system, the SFTA is applied to that portion of software controlling that branch of the hardware FTA. The outputs from the SFMEA, Software Requirements Hazard Analysis (SRHA), Interface Analysis, and Human Factors/Man-Machine Interface Analysis can provide inputs to the SFTA. SFTA can be performed at any or all levels of system design and development.
- **Software Hazard Analysis (SHA)<sup>13</sup>:** used to identify, evaluate, and eliminate or mitigate software hazards by means of a structured analytical approach that is integrated into the software development process.
- **Software Sneak Circuit Analysis (SSCA)<sup>14</sup>:** is used to uncover program logic that could cause undesired program outputs or inhibits, or incorrect sequencing/timing. When software controls a safety critical event, an SSCA can help detect a condition that would cause a catastrophic mishap if the cause were an inadvertent enabling condition.

### ***Generic Software Safety Provisions***

Two recommended sources for the applicant of generic software safety provisions used in the design and development of CST systems that have safety-critical applications are the Joint Software System Safety Committee Software System Safety Handbook and Eastern and Western Range Safety Requirements, (EWR 127-1). Using the generic software safety provision previously discussed and other available software safety “best practices” the applicant should be able to develop system software safety requirements. This should be done early in the software engineering process, in order for software design features to be specified that will eliminate, mitigate, or control hazards/risks at an acceptable level with minimal program impact.

---

<sup>9</sup> Alternate Names: Software Hazard Analysis (SHA) and Follow-On Software Hazard Analysis.

<sup>10</sup> See Paragraph 4.3.

<sup>11</sup> Alternate Names: Also known as Software Fault Hazard Analysis (SFHA) and Software Hazardous Effects Analysis (SHEA).

<sup>12</sup> Alternate Name: Also known as Soft Tree Analysis (STA).

<sup>13</sup> Alternate Name: Software Safety Analysis (SSA).

<sup>14</sup> Should be cross-referenced to system SCA.

***Design and Development Process Guidelines***

The following guidelines should be applied to the software design and development process:

- A software quality assurance program should be established for systems having safety-critical functions.
- At least two people should be thoroughly familiar with the design, coding, testing and operation of each software module in the CST system.
- The software should be analyzed throughout the design, development, and maintenance processes by a software system safety team to verify and validate the safety design requirements have been correctly and completely implemented.
- The processes as described in the software development plan should be enforceable and auditable. Specific coding standards or testing strategies should be enforced and they should be independently audited.
- Desk audits, peer reviews, static and dynamic analysis tools and techniques, and debugging tools should be used to verify implementation of identified safety-critical computing system functions.

***System Design Requirements and Guidelines***

The following system design requirements and guidelines should apply:

- The CST system should have at least one safe state identified for each operation phase.
- Software should return hardware systems under the control of software to a designed safe state when unsafe conditions are detected.
- Where practical, safety-critical functions should be performed on a standalone computer. If this is not practical, safety-critical functions should be isolated to the maximum extent practical from non-critical functions.
- Personnel not associated with the original design team should design the CST system and its software for ease of maintenance.
- The software should be designed to detect safety-critical failures in external hardware input or output hardware devices and revert to a safe state upon their occurrence.
- The software should make provisions for logging all system errors detected.
- Software control of safety-critical functions should have feedback mechanisms that give positive indications of the function's occurrence.
- The system and software should be designed to ensure that design safety requirements are not violated under peak load conditions.
- Applicant should clearly identify an overall policy for error handling. Specific error detection and recovery situations should be identified.
- When redundancy is used to reduce the vulnerability of a software system to a single mechanical or logic failure, the additional failure modes from the redundancy scheme should be identified and mitigated.
- The CST system should be designed to ensure that the system is in a safe state during power-up.

- The CST system should not enter an unsafe or hazardous state after an intermittent power transient or fluctuation.
- The CST system should gracefully degrade to a secondary mode of operation or shutdown in the event of a total power loss so that potentially unsafe states are not created.
- The CST system should be designed such that a failure of the primary control computer will be detected and the CST system returned to a safe state.
- The software should be designed to perform a system level check at power-up to verify that the system is safe and functioning properly prior to application of power to safety-critical functions.
- When read-only memories are used, positive measures, such as operational software instructions, should be taken to ensure that the data is not corrupted or destroyed.
- Periodic checks of memory, instruction, and data buss(es) should be performed.
- Fault detection and isolation programs should be written for safety-critical subsystems of the computing system.
- Operational checks of testable safety-critical system elements should be made immediately prior to performance of a related safety-critical operation.
- The software should be designed to prevent unauthorized system or subsystem interaction from initiating or sustaining a safety-critical sequence.
- The system design should prevent unauthorized or inadvertent access to or modification of the software and object coding.
- The executive program or operating system should ensure the integrity of data or programs loaded into memory prior to their execution.
- The executive program or operating system should ensure the integrity of data and program during operational reconfiguration.
- Safety-critical computing system functions and their interfaces to safety-critical hardware should be controlled at all times. The interfaces should be monitored to ensure that erroneous or spurious data does not adversely affect the system, that interface failures are detected, and that the state of the interface is safe during power-up, power fluctuations & interruptions, in the event of system errors or hardware failure.
- Safety-critical operator display legends and other interface functions should be clear, concise and unambiguous and, where possible, be duplicated using separate display devices.
- The software should be capable of detecting improper operator entries or sequences of entries or operations and prevent execution of safety-critical functions as a result.
- The system should alert the operator to an erroneous entry or operation.
- Alerts should be designed such that routine alerts are readily distinguished from safety-critical alerts.
- Safety-critical computing system functions should have one and only one possible path leading to their execution.
- Files used to store safety-critical data should be unique and should have a single purpose.

FAA System Safety Handbook, Chapter 13: Launch Safety  
December 30, 2000

- The software should be annotated, designed, and documented for ease of analysis, maintenance, and testing of future changes to the software. Safety-critical variables should be identified in such a manner that they can be readily distinguished from non-safety-critical variables.

### ***Configuration Control***

The overall System Configuration Management Plan should provide for the establishment of a Software Configuration Control Board (SCCB) prior to the establishment of the initial baseline. The SCCB should review and approve all software changes (modifications and updates) occurring after the initial baseline is established.

The software system safety program plan should provide for a thorough configuration management process that includes version identification, access control, change audits, and the ability to restore previous revisions of the system.

Modified software or firmware should be clearly identified with the version of the modification, including configuration control information. Both physical and electronic “fingerprinting” of the version are encouraged.

### ***Testing***

Systematic and thorough testing should provide evidence for critical software assurance. Software test results should be analyzed to identify potential safety anomalies that may occur. The applicant should use independent test planning, execution, and review for critical software. Software system testing should exercise a realistic sample of expected operational inputs. Software testing should include boundary, out-of-bounds and boundary crossing test conditions. At a minimum, software testing should include minimum and maximum input data rates in worst case configurations to determine the system capabilities and responses to these conditions. Software testing should include duration stress testing. The stress test time should be continued for at least the maximum expected operation time for the system. Testing should be conducted under simulated operational environments. Software qualification and acceptance testing should be conducted for safety-critical functions.

### **References:**

AST Licensing And Safety Division Directive No. 001, Licensing Process and Procedures dated March 15, 1996.

FAA Advisory Circular AC 431-01, Reusable Launch Vehicle System Safety Process, dated April 1999 (Draft)

Code of Federal Regulations, Commercial Space Transportation, Department of Transportation Title 14, Federal Aviation Administration, Chapter III, Part 415 – Launch Licenses, and Part 431 – Launch and Reentry of a Reusable Launch Vehicle (RLV)

FAA Advisory Circular AC 431-03, Software System Safety (Draft)

System Safety Society, System Safety Handbook, 2<sup>nd</sup> Edition, dated July 1997

Joint Software System Safety Committee Software System Safety Handbook

Eastern and Western Range Safety Requirements, EWR 127-1.

The Application of System Safety to the Commercial Launch Industry Licensing Process, FAA/ASY Safety Risk Assessment News Reports No. 97-4 and 97-5

## Chapter 14: System Safety Training

<b>14.1</b>	<b>TRAINING NEEDS ANALYSIS .....</b>	<b>2</b>
<b>14.2</b>	<b>TASK ANALYSIS .....</b>	<b>4</b>
<b>14.3</b>	<b>LEARNING OBJECTIVES.....</b>	<b>5</b>
<b>14.4</b>	<b>DELIVERING EFFECTIVE SAFETY TRAINING.....</b>	<b>13</b>
<b>14.5</b>	<b>LEARNING STYLES .....</b>	<b>14</b>
<b>14.6</b>	<b>SOURCES FOR SYSTEM SAFETY TRAINING .....</b>	<b>15</b>

## 14.0 System Safety Training<sup>1</sup>

System Safety Training is one of the key elements within a System Safety Program. To conduct a successful program participants should be trained in appropriate concepts, duties, and responsibilities associated with system safety. Specific training is required for management, system safety working group members, safety teams, inspectors, controllers, technicians, engineers, anyone conducting activities within the program. Training will also be required as an administrative control to eliminate or control risk to an acceptable level.

This section provides guidance to a system safety trainer to successfully conduct a systematic safety training activity. Specific topics discussed include Training Needs Analysis, Task Analysis, Learning Objectives, Learning Behaviors, and Delivering Effective Safety Training.

### 14.1 Training Needs Analysis

The first step in preparing to train a group is to perform a training needs analysis. A training needs analysis is a thorough study of an organization to determine how training can help the organization to improve its safety, effectiveness, and efficiency and/or meet legal obligations. It is essential to the success of training programs. Many trainers who do not perform a training needs analysis find that sometimes their program is quite successful, but other times the same program delivered in the same way by the same trainer is vaguely unsuccessful. The reason is that no two training groups are exactly alike. Training needs, level of motivation, educational background, and many other factors can affect the training environment. Therefore, the trainer must be able to assess training needs and adapt the training accordingly. Some of the crucial factors are discussed below.

Safety training plays a vital role in a system safety program. The trainer must assess the needs in which he/she is going to provide training with the following questions in mind (all of which are important):

<p>What is the extent of system safety knowledge of the participants within the organization?</p> <p>What are the participant's tasks that involve system safety knowledge?</p> <p>What are the background, experience, and education of the participants?</p> <p>What training has been provided in the past?</p> <p>What is the management's attitude toward system safety and training?</p> <p>Is training being provided to management, or system safety working group participants?</p> <p>Will participants be trained in hazard analysis?</p>
--

#### 14.1.1 Training Standards

Often trainers are overwhelmed by what seems to be a maze of interrelated regulations pertaining to system safety, occupational safety, and environmental training requirements. The regulations may change. Amid the confusion, it is often difficult to know how to get started.

---

<sup>1</sup> Bob Thornburgh, President of Environmental Services, Inc.; Presentation at 15th International Systems Safety Conference, Wash. D.C., Aug. 1997

Here are some guidelines for bringing the organization into compliance with safety training requirements:

- ***Read the pertinent regulations.*** The regulations are often difficult to comprehend, and it may be necessary to read them several times. However, whoever has primary responsibility for safety training should read them rather than rely solely on other people for interpretation.
- ***Attend professional development workshops and talk to colleagues.*** In addition to reading the regulations, the trainer should attend professional development workshops and talk with colleagues and regulatory personnel to stay current and to share implementation strategies.
- ***Work with management to set training priorities.*** After analyzing requirements and safety training needs, management and the training unit must meet to set safety training priorities and to develop a training calendar.
- ***Design, deliver, and evaluate systematic instruction.*** Most regulations state training requirements in terms of hour requirements and topics. The trainer must translate the requirements into a systematic plan of instruction, including learning objectives, instructional strategies, and evaluation methods. This Chapter provides the fundamentals for designing safety-training programs, but does not cover basic information on delivering or evaluating safety-training programs.
- ***Document training.*** Documentation of training is an essential ingredient of all training, and is especially crucial for safety training. Inspectors usually review documentation, and documentation is often used as evidence of good intent on the industry's behalf. With easy storage of information available through computers, many companies are maintaining safety-training records over the life spans of their personnel. They are also asking employees to verify with a signature that safety training has been delivered.

### 14.1.2 Expectations from Training

Take some time “up front” to pinpoint the expectations of the organization you are going to train. Determine how much support there is from the management team. Determine their training objectives. Then, talk with representatives from the target audience, the group you will be training, to determine their objectives and expectations. Also, survey representatives from the subordinates the target audience supervises; in order to gain another perspective on safety training needs. This part of the needs analysis does not have to be formal. Often a tour provides an opportunity to ask questions, listen, and assess expectations. The ability to listen is very important, because people will often volunteer information to a skilled listener.

Once you have determined the training expectations, put down the training objectives in writing and secure consensus from the organization. If the expectations are unrealistic, then they should be discussed.

Unrealistic expectations are usually a result of a failure to understand what constitutes effective training. A common example is a request to train 200 people with a wide variation in knowledge of background information and need-to-know. Look for creative solutions to this problem, such as several safety-training

sessions for different groups, the use of several safety trainers, the use of multiple teaching strategies, and/or multi-media, etc.

Another example of an unrealistic expectation might be a request to have training at 7:00 a.m. on Saturday with no additional pay for workers who have just worked a shift from 11:00 p.m. to 7:00 a.m. It is easy to anticipate a problem in motivating the group. Be sure to set appropriate times and dates.

Another type of unrealistic expectation that is even more serious, results from a request to minimize dangers, encourages shortcuts, or overlook hazards. Deliberately misinforming trainees could result in liability for the trainer. Therefore, the trainer should feel comfortable with the philosophy and practices of the organization. On rare occasions, trainers elect to walk away from training opportunities rather than compromise their personal training standards. Normally, however, organizations are supportive when the trainer explains how the training will promote effectiveness, efficiency, and safety.

### **14.1.3 Problem Analysis**

There are several types of problems that can affect the performance of an organization and the safety training environment. The trainer should try to determine the causes of the deficiencies and tailor the training to the needs of the organization. For example, when workers and/or managers are motivated to perform well but lack skills or knowledge, an ideal training opportunity exists. Safety training usually can fill the gap of knowledge that exists if learners have pre-requisite skills and knowledge and are given sufficient instruction.

### **14.1.4 Audience Analysis**

A crucial step in a safety training needs analysis is to analyze the target audience. The safety trainer should determine the general educational background of the audience, their job duties, their previous training history, their length of employment, the general emotional climate of the organization, behavioral norms, and attitudes toward training. It is vital to determine whether trainees have mastered pre-requisite skills and knowledge in order to target training appropriately.

## **14.2 Task Analysis**

Once the safety training needs analysis has been completed, management and the trainer should have agreed on overall training objectives - the skill or knowledge areas where training is needed. The next step in the process of designing safety training is to perform a task analysis. The primary purpose of a task analysis is to prepare a sequential listing of all the steps necessary to perform a specific job skill. A task analysis is important for several reasons:

- It helps the trainer to be methodical and to organize training in a logical sequence.
- Not all steps in the task will necessarily require training. However, the safety trainer and trainee in context of the “big picture” can see those steps that do require training.
- The safety trainer becomes familiar with the task, can incorporate graphic examples into safety training, can relate better to the trainees, and can enhance credibility as a knowledge expert.
- Trainers who are already very familiar with the task benefit from performing a task analysis because they think through “common sense” steps they might overlook otherwise, but which need to be included in safety and environmental training.

- During the task analysis, the safety trainer often identifies environmental constraints and/or motivational problems as well as problems with lack of skills and knowledge. If the trainer can assist management in resolving environmental constraints and/or motivational problems, barriers to effective training will be reduced.
- The safety trainer determines pre-requisite skills and knowledge needed to perform the task so that training can begin at the appropriate level.

There are several ways to begin a task analysis, depending upon the safety-training situation:

- The safety trainer can observe the task being performed. This is an excellent method for analyzing routine tasks. It may not work as well for tasks such as emergency procedures that are rarely, if ever, performed under normal circumstances.
- The safety trainer can interview one or more workers who perform or supervise the task. ***Once a task inventory has been developed, it should always be reviewed and validated by job incumbents.***
- The safety trainer may be able to perform the task, develop a task inventory, and submit it for review and validation by job incumbents.
- Some tasks have prescribed steps that are outlined by the policies and procedures manual. It is always important to review this manual so that the training and the written policy and procedures are properly aligned. However, the safety trainer should be alert to situations where actual practice varies from written policy.

### 14.3 Learning Objectives

A learning objective is a brief, clear statement of what the participant should be able to do as a result of the safety training. The groundwork for the learning objective has already been laid once a thorough task analysis has been completed. A task analysis describes all the steps involved in a skill. The learning objectives focus just on the steps to be included in the training session. Sometimes an entire task needs to be learned; sometimes only a portion of the task needs to be learned. A task analysis lists the behavior to be learned, a learning objective goes a step further by defining how well and under what conditions the task must be performed in order to verify that the task has been learned. Learning objectives are important because instructional strategies and evaluation techniques are an outgrowth of the learning objectives.

#### 14.3.1 Guidelines for Writing Learning Objectives

Objectives are always written from the viewpoint of what the trainee or participant will do, not what the trainer will do.

*Right:* Participants will be able to repair a generator.

*Wrong:* Instructor will cover unit on repairing generators.

Verbs or action words used to describe behavior are as specific as possible. Words to avoid include popular but vague terms such as “know,” “learn,” “comprehend,” “study,” “cover,” and “understand.”

*Right:* Participants will be able to measure and record the concentration of Volatile Organic Compound (VOC) in a sample of ground water.

*Wrong:* Participants will learn about ground water sampling.

The desired behavior must be *observable and measurable* so that the trainer can determine if it has been learned.

*Right:* Participants will demonstrate the ability to don a respirator properly.

*Wrong:* Participant will know about respirators.

Objectives should be given orally and in writing to the participants, so that they understand the purpose of the training session.

### 14.3.2 Components of Learning Objectives

There are four components that need to be considered each time a learning objective is developed: Target audience, behavior, conditions, and standards.

#### Target Audience

The target audience (participants or trainees) must be considered because the same topic may be approached differently based on the background of the groups to be trained. The following examples of learning objectives describe the audience. In each learning objective, the target audience is highlighted.

*New employees* will identify evacuation routes from the facility.

*System safety personnel* will develop an emergency response plan.

When an entire training course is designed for a particular audience, often the audience is described only once in a blanket statement, such as the following: “This course is designed as a safety orientation for new personnel.” Once the audience is established, then the audience component does not have to be repeated each time.

#### Behavior

The behavior component of the objective is the action component. It is the most crucial component of the objective in that it pinpoints the way in which trainees will demonstrate they have gained knowledge. Learning is measured by a change in behavior. How will trainees prove what they have learned? Will they **explain...**? Will they **calculate...**? Will they **operate...**? Will they **repair...**? Will they **troubleshoot...**? The highlighted verbs in the following examples indicate the behavior required.

- The emergency response team will **build** a decontamination chamber.
- Trainees will **interpret** the meaning of colors and numbers on Material Safety Data Sheet (MSDS) labels.
- System safety personnel with a minimum of five years’ experience will **develop** an emergency response plan.

The behavior component should be easy to determine based on the task analysis, which was written in behavioral terms.

#### Conditions

The **condition** component of the objective describes special conditions (constraints, limitations, environment, or resources) under which the behavior must be demonstrated. If trainees are expected to demonstrate how to don a respirator in a room filled with tear gas rather than in a normal classroom environment, that would constitute a special condition. Please note that the condition component indicates the condition under which the behavior will be tested, not the condition under which the behavior was learned. Examples:

Right: ***Given a list of chemical symbols and their atomic structure***, participants in beginning chemistry course will construct a Periodic Table of Elements. (This condition is correct; participants will be able to refer to symbols and atomic structure while they are being tested.)

Right: ***From memory***, participants in an advanced course will construct a Periodic Table of Elements. (This condition is also correct; it outlines a testing condition.)

Wrong: ***Given a unit of instruction on the Periodic Table***, participants will then construct a Periodic Table of Elements. (This tells something about how the knowledge was learned, not a condition under which the knowledge will be tested.)

The condition component does not have to be included if the condition is obvious, such as the one in the following example:

***Given paper and pencil***, trainees will list the safety rules regarding facility areas. (The condition is obvious and does not need to be stated.)

### Standards of Acceptable Performance

The standard of acceptable performance indicates the minimum acceptable level of performance - how well the trainee must perform the behavior indicated in the objective. Examples include percentages of right responses, time limitations, tolerances, correct sequences without error, etc. Examples:

The hazardous waste supervisor will calculate required statistics ***with an accuracy of plus or minus 0.001***.

Given a facility layout, the employees will circle the location of fire extinguishers ***with a minimum of 80% accuracy***.

Given a scenario of an emergency situation, employees will respond ***in less than three minutes***.

### 14.3.3 Types of Behavior in Learning Objectives

The next step is to identify the **domains of learning** - the types of behavior that can be described within objectives. Behaviors are categorized in one of these domains of learning: *cognitive, psychomotor, or affective*.

**Cognitive behaviors** describe observable, measurable ways the trainees demonstrate that they have gained the knowledge and/or skill necessary to perform a safety task. Most learning objectives describe cognitive behaviors. Some cognitive behaviors are easy to master; others are much more difficult. In designing safety and environmental instruction, trainers move from the simple to the complex in order to verify that trainees have the basic foundation they need before moving on to higher level skills. It is crucial to identify the level of knowledge required because knowledge-level objectives can be taught in a lecture session, and comprehension-level objectives can be taught with a guided discussion format. However, most training sessions are designed for trainees to apply the information and to solve problems. Therefore, participants need to achieve by doing; they need to be drilled on actual safety case problems.

This does not mean that the basic skills have to be re-taught if the trainer can verify through observations, pretests, training records, etc., that pre-requisite skills have been mastered. However, many training sessions have turned into a disaster because the trainer made the assumption that the trainees had mastered basic skills and began the training at too high a level. In contrast, some training sessions have bored the participants by being too basic. Therefore, it is important for safety trainers to be able to label learning objectives and design safety training sessions appropriate to the level of cognitive behavior required to perform a task. Following are descriptions and examples of types of cognitive behaviors.

**Knowledge-level cognitive behaviors** are the easiest to teach, learn, and evaluate. They often refer to rote memorization or identification. Trainees often “parrot” information or memorize lists or name objects. Common knowledge-level behaviors include action words such as these: identify, name, list, repeat, recognize, state, match, and define. Examples:

Given containers of sample chemicals, the participants will **identify** the chemicals by name.

Given a list of chemicals, health and safety personnel will **state** the properties of each.

**Comprehension-level cognitive behaviors** have a higher level of difficulty than knowledge-level cognitive behaviors, because they require learners to process and interpret information; however, learners are not required to actually apply/demonstrate the behavior. Commonly used action words at this level include verbs such as these: explain, discuss, interpret, classify, categorize, cite evidence for, compare, contrast, illustrate, give examples of, differentiate, and distinguish between. Examples:

Participants will **contrast** the properties of acids and alkalis.

All employees will be able to **discuss** the hazard communications training they have received.

**Application-level cognitive behaviors** move beyond the realm of explaining concepts orally or in writing; they deal with putting ideas into practice and involve a routine process. Trainees apply the knowledge they have learned. Some examples of action words commonly used in application-level cognitive behaviors include the following: demonstrate, calculate, do, operate, implement, compute, construct, measure, prepare, and produce. Examples:

The emergency response team will **perform** evacuation management.

Beginning machinists will **measure** stock with a micrometer within a tolerance of +/-0.001.

Workshop trainees will accurately **complete** an MSDS.

**Problem-solving cognitive behaviors** involve a higher level of cognitive skills than application-level cognitive behaviors. The easiest way to differentiate between application-level and problem-solving level is to apply application-level to a routine activity and problem-solving level to non-routine activities which require **analysis** (breaking a problem into parts), **synthesis** (looking at parts of a problem and formulating a generalization or conclusion), or **evaluation** (judging the appropriateness, effectiveness, and/or efficiency of a decision or process and choosing among alternatives). Some examples of action words commonly used in problem-solving cognitive behaviors include the following: troubleshoot, analyze, create, develop, devise, evaluate, formulate, generalize, infer, integrate, invent, plan, predict, reorganize, solve, and synthesize. Examples:

System safety personnel will **develop** an emergency response plan.

Given a pump with “bugs” built in, maintenance personnel will **troubleshoot** the problems with the pump.

Quality circle team will **analyze** the flow of production and **devise** ways to reduce work-in-process inventory.

There is no way to prepare a list stating that an action word is always on a certain level. The lists of example action words included in the discussion above are suggestions and are not all-inclusive. Safety trainers must use professional judgement to determine the level of cognitive behavior indicated. The same action word can be used on different levels. Example:

Photographers will develop film in a dark room using a three-step process.  
(**Application level**)

R and D Department will *develop* a new process to coat film. (*Problem-solving level*)

### ***Psychomotor Behaviors***

Learning new behaviors *always* includes cognitive skills (knowledge, comprehension, application and/or, problem solving). In addition, the trainer needs to be cognizant of psychomotor skills that may be required in the application phase of learning. *Psychomotor* behaviors pertain to the proper and skillful use of body mechanics and may involve gross and/or fine motor skills. Examples:

Warehouse personnel will *lift* heavy boxes appropriately.  
Inventory personnel will *enter* data into computer at 40 words per minute.

Safety training sessions for psychomotor skills should involve as many of the senses as possible. The safety trainer should adapt the format of training to match the skill level of the learner and the difficulty of the task. Following is an example of a sound process for teaching psychomotor skills:

#### **Example: How to Don a Respirator**

- Step 1:** The safety instructor shows a respirator and explains its function and importance. (Lecture)
- Step 2:** The trainees explain the function and importance of the respirator. (Cognitive - comprehension level)
- Step 3:** The safety instructor holds up the respirator, names the parts, and explains functions. (Lecture/demonstration)
- Step 4:** The trainees hold up respirators, name the parts, and explain the functions. (Cognitive - knowledge and comprehension levels)
- Step 5:** The instructor explains and demonstrates how to don a respirator. (Lecture/demonstration)
- Step 6:** The trainees explain how to don a respirator while the safety instructor follows trainees' instructions. (Cognitive - comprehension level)

**Important Note:** Step 6 allows the safety instructor an opportunity to check for understanding and would be especially useful when one is teaching a task that could be potentially dangerous to the trainee or others or that involves expensive tools or equipment that could be damaged.

FAA System Safety Handbook, Chapter 14: System Safety Training  
December 30, 2000

**Step 7:** The trainees don a respirator properly. (Cognitive - application level and psychomotor)

**Step 8:** Explain and practice; explain and practice; EXPLAIN AND PRACTICE. (Cognitive - comprehension and application levels and psychomotor)

The key to teaching psychomotor skills is that the more the learner *observes* the task, *explains* the task, and *practices* the task correctly, the better he/she performs the task.

### ***Affective Behaviors***

*Affective behaviors pertain to attitudes, feelings, beliefs, values, and emotions.* The safety trainer must recognize that affective behaviors influence how efficiently and effectively learners acquire cognitive and psychomotor behaviors. Learning can be influenced by positive factors (success, rewards, reinforcement, perceived value, etc.) and by negative factors (failure, disinterest, punishments, fears, etc.) Examples:

Supervisors resent training time and tell employees they must make up time lost. Employees develop negative attitude toward training.

**OR**

Supervisors explain the training could save lives, attend training with employees, and reinforce training on the job.

Employees are afraid of chemical spills and are anxious to learn how to avoid them.

**OR**

Employees have been told through the grapevine that the safety and training is boring and a waste of time. Employees have a negative attitude toward training.

Employees have just received a bonus for 365 accident-free days and have a positive attitude toward the company and toward safety training.

**OR**

The company announces 30 minutes before the safety training session begins that there will be a massive layoff. Training will probably not be a priority for employees today.

Other affective behaviors (attitudes and emotions) that must be considered go beyond positive or negative motivations toward learning. Examples:

An employee may have the knowledge and skills to repair an air conditioning system, but fear of heights causes him/her not to be able to repair a unit located on the roof.

An employee may know how to don a self-contained breathing apparatus, but panics when he/she does so.

Training objectives which state affective behaviors are usually much more difficult to observe and measure than cognitive behaviors. Nevertheless, they are crucial to the ultimate success of the safety-training program. Following are some examples of affective objectives:

Employees will demonstrate safety awareness by leaving guards on equipment and wearing safety glasses in designated areas.

Employees will demonstrate awareness of chemical flammability by smoking only in designated areas.

Employees will state in a survey that they appreciate safety-training sessions.

A critical factor to remember is that while training can stress the importance of affective behaviors, people are most influenced by the *behavioral norms* of an organization. Remember: Before attempting to make changes in an organization, it is first important to identify existing norms and their effects on employees. Behavioral norms refer to the peer pressure that results from the attitudes and actions of the employees/management as a group. Behavioral norms are the behaviors a group expects its members to display. Examples:

Although training may emphasize the importance of wearing a face mask and helmet in a “clean” room, if most employees ignore the rule, new employees will “learn” to ignore the rule as well.

Although smoking and non-smoking areas may be clearly labeled in the plant, if new employees observe supervisors and “old-timers” breaking the rules, they will tend to perceive the non-smoking rule as not very important, despite what was stated in an orientation session.

Although a new employee learns to perform a task well in safety training sessions, he/she will quickly change performance if the supervisor undermines the safety training and insists there is a better, faster way to do the job.

For safety training to be successful, it must have the support of all levels of management. Safety training does not occur in a vacuum. The organizational climate and behavioral norms, in fact, are likely to be more powerful than the behavior taught in safety training sessions, because the group can enforce its norms with continual rewards, encouragement, and pressure. Supervisors should see themselves as coaches who continue to reinforce safety training. Otherwise, the safety training is unlikely to have a long-term impact on the organization.

## 14.4 Delivering Effective Safety Training

One of the easiest and most fatal mistakes for a trainer to make is to approach the trainer-learner relationship as a teacher-child relationship. Certainly, most of the role models trainers have observed have been adults teaching children. However, it is essential for trainers to view themselves as facilitators of the adult learning process. Although no generalizations apply to every adult learner, it is helpful in planning training sessions to keep the following characteristics of adult learners in mind:

- Despite the cliché that “old dogs can’t learn new tricks,” healthy adults are capable of lifelong learning. At some point, rote memorization may take more time, but purposeful learning can be assimilated as fast or faster by an older adult as by high school students.
- Most adults want satisfactory answers to these questions before they begin to learn: “Why is it important?” and “How can I apply it?”
- Adults are used to functioning in adult roles, which means they are capable of and desirous of participating in decision making about learning.
- Adults have specific objectives for learning and generally know how they learn best. Delegation of decisions on setting objectives may help learners, especially managers, gain the knowledge and skills they really need.
- Adults do not like to be treated “like children” (neither do children) and especially do not appreciate being reprimanded in front of others.
- Adults like organization and like to know the “big picture.”
- Adults have experienced learning situations before and have positive and/or negative preconceptions about learning and about their own abilities.
- Adults have had a wealth of unique individual experiences to invest in learning and can transfer knowledge when new learning is related to old learning.
- Adults recognize good training and bad training when they see it.

There are several guidelines to remember when one is designing adult training sessions:

- Early in the safety training session, explain the purpose and importance of the session.
- Share the framework (organization) of the safety learning session with the participants.
- Demonstrate a fundamental respect for the learners. Ask questions and really listen to their responses. Never reprimand anyone in front of others, even if it means taking an unscheduled break to resolve a problem.
- Acknowledge the learners’ experience and expertise when appropriate. Draw out their ideas, and try not to tell them anything they could tell you. Do not embarrass them when they make mistakes.
- Allow choices when possible within a structured framework. Example: “For this exercise, would you rather work in pairs or individually?”

- Avoid body language that is reminiscent of an elementary school teacher, such as hands on hips, wagging a pointed index finger, etc.
- Do not “talk down” to participants; “talking down” results more from tone of voice and expression rather than from vocabulary.
- Maintain a certain degree of decorum within a classroom environment and mutual respect among learners.
- Should a mistake in information or judgment occur, admit it.
- Make sure everyone can see and hear properly and has comfortable seating.

## 14.5 Learning Styles

One of the pitfalls of instruction is that trainers tend to develop safety-training programs that accommodate the way the trainer learns best, not the way the participants learn best. For example, if the trainer learns best by reading, he/she tends to give a manual to the new employees and expects them to master the procedure by reading the manual. If the trainer learns best through experimentation, he/she tends to throw employees into a new situation with little guidance. It is important to emphasize individual growth rather than competition and to remember that individuals have different learning styles with which they are most comfortable. Every trainee is different and must be treated as an individual. Here are some examples:

### Passive Learners learn best by:

Reading manuals/books
Watching audio-visual presentations
Hearing a lecture
Observing demonstrations

### Active Learners learn best by:

Participating in discussions
Role-playing
Performing an experiment
Taking a field trip
Hands-on learning
Responding to a scenario
Making a presentation

FAA System Safety Handbook, Chapter 14: System Safety Training  
December 30, 2000

Some learners prefer to learn by themselves; others prefer to work in-groups. Some people need a lot of organization and learn small steps sequentially; others assimilate whole concepts with a flash of insight or intuition.

Some people are very visual and learn best through drawings, pictorial transparencies, slides, demonstrations, etc.; others learn best through words and enjoy reading transparencies and slides with words, and lectures.

Increased retention results from what we know of split hemisphere learning. Just as different sides of the brain control opposite sides of the body, so does the brain absorb and record different types of information:

- |  |
|--|
| <p>a. Left side — Linear functions, logic, time, reasoning, language, and writing.</p> <p>b. Right side — Space, movement, emotion, facial recognition, music, depth perception.</p> |
|--|

It is the combination of the effects of both sides that allows us to think and react to information.

Although various tests have been developed to try to identify how people learn best, they are not practical for most safety training sessions. Rather, the trainer needs to be aware that differences in learning styles exist and try to combine as many types of activities and media as possible so that learners can have access to the way they learn best and also learn to adapt to other learning styles as well. That means that a safety training session might include a handout for readers, a lecture for listeners, and an experiment for doers, depending on the objective.

The key to accommodating learning styles is that instructional strategies and media be selected as a means to help the learner and not as a convenience for the instructor. For example, a new employee orientation pamphlet and videotape should be selected if they prove to be an excellent instructional strategy for teaching new employees; they should not be selected just because they are a convenient means of orientation. Also, the safety trainer should constantly look for alternate strategies and media so that if one strategy or type of media is ineffective, the safety trainer has multiple strategies from which to select.

## **14.6 Sources for System Safety Training**

FAA Academy

FAA Training Office

FAA Office of System Safety, System Safety Engineering and Analysis Division

International System Safety Society

## **Chapter 15: Operational Risk Management (ORM)**

<b>15.1 DEFINING RISK AND RISK MANAGEMENT .....</b>	<b>2</b>
<b>15.2 ORM PRINCIPLES .....</b>	<b>3</b>
<b>15.3 THE ORM PROCESS SUMMARY.....</b>	<b>4</b>
<b>15.4 IMPLEMENTING THE ORM PROCESS.....</b>	<b>6</b>
<b>15.5 RISK VERSUS BENEFIT .....</b>	<b>6</b>
<b>15.6 ACCEPTABILITY OF RISK.....</b>	<b>7</b>
<b>15.7 GENERAL RISK MANAGEMENT GUIDELINES .....</b>	<b>8</b>
<b>15.8 RISK MANAGEMENT RESPONSIBILITIES.....</b>	<b>9</b>
<b>15.9 SYSTEMATIC RISK MANAGEMENT: THE 5-M MODEL .....</b>	<b>9</b>
<b>15.10 LEVELS OF RISK MANAGEMENT.....</b>	<b>12</b>
<b>15.11 ORM PROCESS EXPANSION.....</b>	<b>12</b>
<b>15.12 CONCLUSION .....</b>	<b>23</b>

## **15.0 Operational Risk Management (ORM)**

### **15.1 Defining Risk and Risk Management**

ORM is a decision-making tool to systematically help identify operational risks and benefits and determine the best courses of action for any given situation. In contrast to an Operational and Support Hazard Analysis (O&SHA), which is performed during development, ORM is performed during operational use. For example, an ORM might be performed before each flight. This risk management process, as other safety risk management processes is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare.

Risk management, as discussed throughout this handbook is pre-emptive, rather than reactive. The approach is based on the philosophy that it is irresponsible and wasteful to wait for an accident to happen, then figuring out how to prevent it from happening again. We manage risk whenever we modify the way we do something to make our chances of success as great as possible, while making our chances of failure, injury or loss as small as possible. It's a common-sense approach to balancing the risks against the benefits to be gained in a situation and then choosing the most effective course of action.

Often, the approach to risk management is highly dependent on individual methods and experience levels and is usually highly reactive. It is natural to focus on those hazards that have caused problems in the past. In the FAA's operational environment where there is a continual chance of something going wrong, it helps to have a well-defined process for looking at tasks to prevent problems. Operational Risk Management, or ORM, is a decision-making tool that helps to systematically identify risks and benefits and determine the best courses of action for any given situation. ORM is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare.

Risk is defined as the probability and severity of accident or loss from exposure to various hazards, including injury to people and loss of resources. All FAA operations in the United States, and indeed even our personal daily activities involve risk, and require decisions that include risk assessment and risk management. Operational Risk Management (ORM) is simply a formalized way of thinking about these things. ORM is a simple six-step process, which identifies operational hazards and takes reasonable measures to reduce risk to personnel, equipment and the mission.

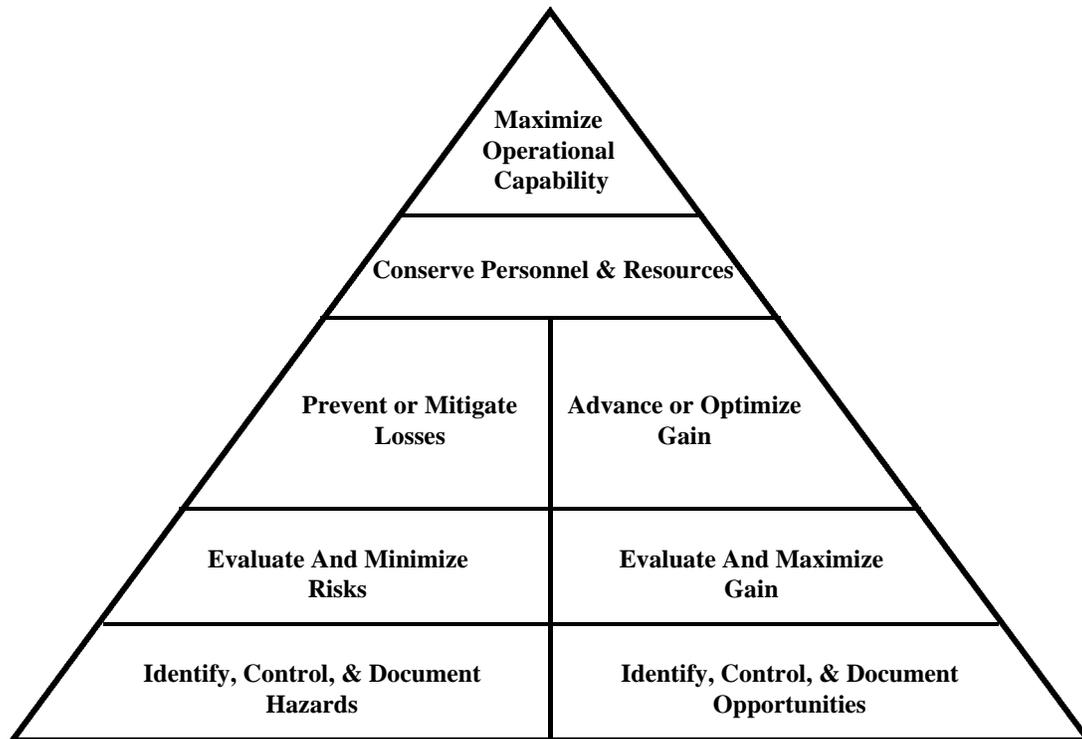
In FAA operations, decisions need to take into account the significance of the operation, the timeliness of the decision required, and what level of management is empowered to make the decision. Risk should be identified and managed using the same disciplined process that governs other aspects of the Agency's endeavors, with the aim of reducing risk to personnel and resources to the lowest practical level.

Risk management must be a fully integrated part of planning and executing any operation, routinely applied by management, not a way of reacting when some unforeseen problem occurs. Careful determination of risks, along with analysis and control of the hazards they create results in a plan of action that anticipates difficulties that might arise under varying conditions, and pre-

determines ways of dealing with these difficulties. Managers are responsible for the routine use of risk management at every level of activity, starting with the planning of that activity and continuing through its completion.

Figure 15-1 illustrates the objectives of the ORM process: protecting people, equipment and other resources, while making the most effective use of them. Preventing accidents, and in turn reducing losses, is an important aspect of meeting this objective. In turn, by minimizing the risk of injury and loss, we ultimately reduce costs and stay on schedule. Thus, the fundamental goal of risk management is to enhance the effectiveness of people and equipment by determining how they are most efficiently to be used.

**Figure 15-1: Risk management Goal**



## 15.2 ORM Principles

Four principles govern all actions associated with operational risk management. These continuously employed principles are applicable before, during and after all tasks and operations, by individuals at all levels of responsibility.

**Accept No Unnecessary Risk:**

Unnecessary risk is that which carries no commensurate return in terms of benefits or opportunities. Everything involves risk. The most logical choices for accomplishing an operation are those that meet all requirements with the minimum acceptable risk. The corollary to this axiom is “accept necessary risk,” required to successfully complete the operation or task.

**Make Risk Decisions at the Appropriate Level:**

Anyone can make a risk decision. However, the appropriate decision-maker is the person who can allocate the resources to reduce or eliminate the risk and implement controls. The decision-maker must be authorized to accept levels of risk typical of the planned operation (i.e., loss of operational effectiveness, normal wear and tear on materiel). He should elevate decisions to the next level in the chain of management upon determining that those controls available to him will not reduce residual risk to an acceptable level.

**Accept Risk When Benefits Outweigh the Costs:**

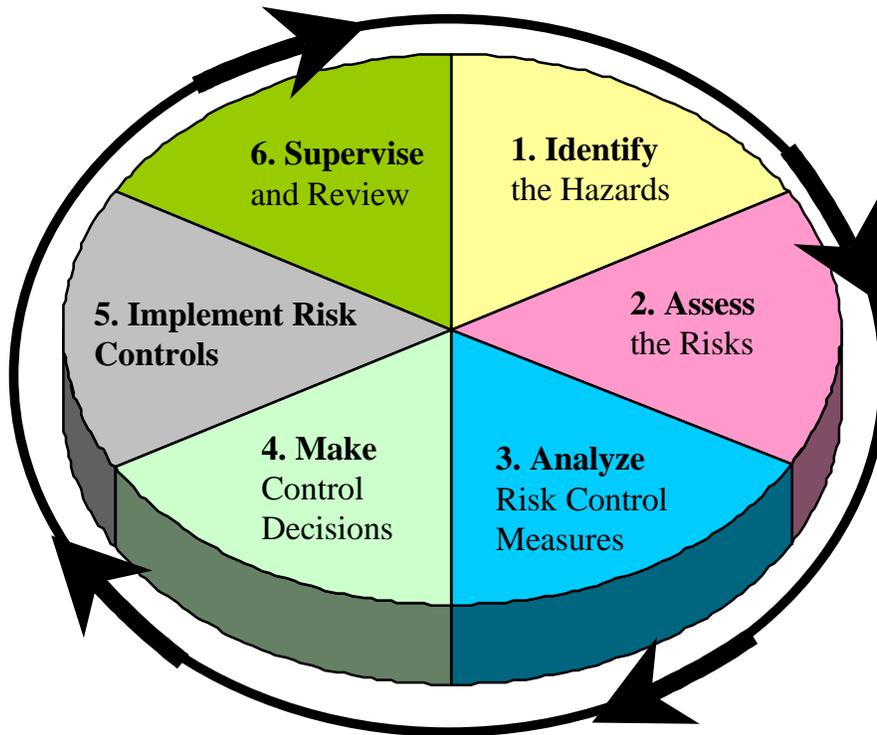
All identified benefits should be compared against all identified costs. Even high-risk endeavors may be undertaken when there is clear knowledge that the sum of the benefits exceeds the sum of the costs. Balancing costs and benefits is a subjective process, and ultimately the balance may have to be arbitrarily determined by the appropriate decision-maker.

**Integrate ORM into Planning at all Levels:**

Risks are more easily assessed and managed in the planning stages of an operation. The later changes are made in the process of planning and executing an operation, the more expensive and time-consuming they will become.

**15.3 The ORM Process Summary**

The ORM process comprises six steps, each of which is equally important. Figure 15-2 illustrates the process.



**Figure 15-2: ORM's 6 Process Steps**

### **Step 1: Identify the Hazard**

A hazard is defined as any real or potential condition that can cause degradation, injury, illness, death or damage to or loss of equipment or property. Experience, common sense, and specific analytical tools help identify risks.

### **Step 2: Assess the Risk**

The assessment step is the application of quantitative and qualitative measures to determine the level of risk associated with specific hazards. This process defines the probability and severity of an accident that could result from the hazards based upon the exposure of humans or assets to the hazards.

### **Step 3: Analyze Risk Control Measures**

Investigate specific strategies and tools that reduce, mitigate, or eliminate the risk. All risks have three components: probability of occurrence, severity of the hazard, and the exposure of people and equipment to the risk. Effective control measures reduce or eliminate at least one of these. The analysis must take into account the overall costs and benefits of remedial actions, providing alternative choices if possible.

#### **Step 4: Make Control Decisions**

Identify the appropriate decision-maker. That decision-maker must choose the best control or combination of controls, based on the analysis of step 3.

#### **Step 5: Implement Risk Controls**

Management must formulate a plan for applying the controls that have been selected, then provide the time, materials and personnel needed to put these measures in place.

#### **Step 6: Supervise and Review**

Once controls are in place, the process must be periodically reevaluated to ensure their effectiveness. Workers and managers at every level must fulfill their respective roles to assure that the controls are maintained over time. The risk management process continues throughout the life cycle of the system, mission or activity.

### **15.4 Implementing the ORM Process**

To derive maximum benefit from this powerful tool, it must be used properly. The following principles are essential.

#### **Apply the steps in sequence**

Each step is a building block for the next, and must be completed before proceeding to the next. If a hazard identification step is interrupted to focus upon the control of a particular hazard, other, more important hazards may be overlooked. Until all hazards are identified, the remainder of the process is not effective.

#### **Maintain a balance in the process**

All six steps are important. Allocate the time and resources to perform them all.

#### **Apply the process in a cycle**

The “supervise and review” step should include a brand-new look at the operation being analyzed, to see whether new hazards can be identified.

#### **Involve people in the process**

Be sure that the risk controls are mission supportive, and that the people who must do the work see them as positive actions. The people who are actually exposed to risks usually know best what works and what does not.

### **15.5 Risk versus Benefit**

Risk management is the logical process of weighing the potential costs of risks against the possible benefits of allowing those risks to stand uncontrolled.

#### **15.5.1 Types of Risk Defined**

*Identified risk:* That risk that has been determined to exist using analytical tools. The time and costs of analysis efforts, the quality of the risk management program, and the state of the technology involved affect the amount of risk that can be identified.

*Unidentified risk:* That risk that has not yet been identified. Some risk is not identifiable or measurable, but is no less important for that. Mishap investigations may reveal some previously unidentified risks.

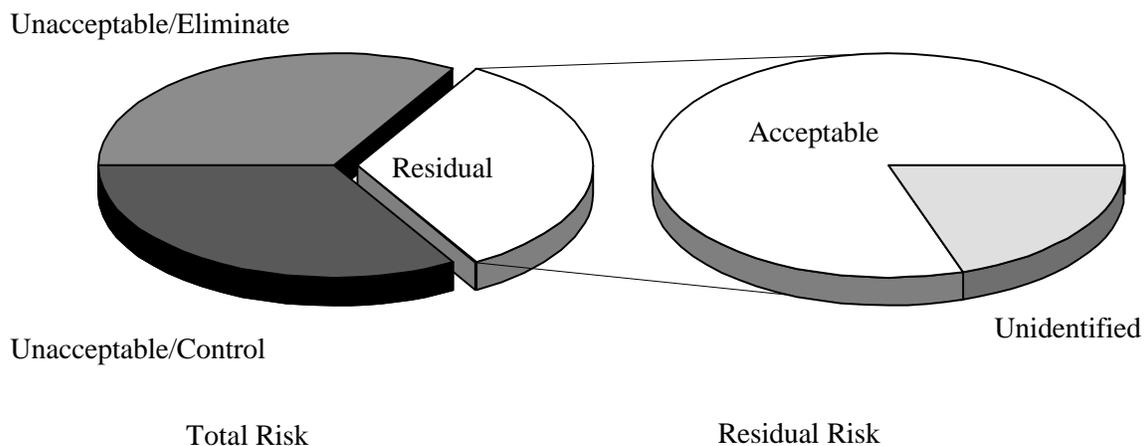
*Total risk:* The sum of identified and unidentified risk. Ideally, identified risk will comprise the larger proportion of the two.

*Acceptable risk:* The part of identified risk that is allowed to persist after controls are applied. Risk can be determined acceptable when further efforts to reduce it would cause degradation of the probability of success of the operation, or when a point of diminishing returns has been reached.

*Unacceptable risk:* That portion of identified risk that cannot be tolerated, but must be either eliminated or controlled.

*Residual risk:* The portion of total risk that remains after management efforts have been employed. Residual risk comprises acceptable risk and unidentified risk.

**Figure 15-3: Types of Risk**



### 15.5.2 Benefits Defined

Benefits are not limited to reduced mishap rates or decreased injuries, but may also be realized as increases in efficiency or mission effectiveness. Benefits are realized through prudent risk-taking. Risk management provides a reasoned and repeatable process that reduces the reliance on intuition.

### 15.6 Acceptability of Risk

Risk management requires a clear understanding of what constitutes unnecessary risk, i.e., when benefits actually outweigh costs. Accepting risk is a function of both risk assessment and risk management, and is not as simple a matter as it may first appear. Several principles apply:

- Some degree of risk is a fundamental reality
- Risk management is a process of tradeoffs
- Quantifying risk does not in itself ensure safety
- Risk is often a matter of perspective
- Realistically, some risk must be accepted. How much is accepted, or not accepted, is the prerogative of the defined decision authority. That decision is affected by many inputs. As tradeoffs are considered and operation planning progresses, it may become evident that some of the safety parameters are forcing higher risk to successful operation completion. When a manager decides to accept risk, the decision should be coordinated whenever practical with the affected personnel and organizations, and then documented so that in the future everyone will know and understand the elements of the decision and why it was made.

### **15.7 General Risk Management Guidelines**

- All human activity involving technical devices or complex processes entails some element of risk.
- Hazards can be controlled; they are not a cause for panic.
- Problems should be kept in perspective.
- Judgments should be based upon knowledge, experience and mission requirements.
- Encouraging all participants in an operation to adopt risk management principles both reduces risk and makes the task of reducing it easier.
- Good analysis tilts the odds in favor of safe and successful operation.
- Hazard analysis and risk assessment do not replace good judgment: they improve it.
- Establishing clear objectives and parameters in risk management works better than using a cookbook approach.
- No one best solution may exist. Normally, there are a variety of alternatives, each of which may produce a different degree of risk reduction.
- Tact is essential. It is more productive to show a mission planner how he can better manage risk than to condemn his approach as unworkable, risky, unsafe or unsound.
- Seldom can complete safety be achieved.
- There are no “safety problems” in planning or design, only management problems that may cause accidents, if left unresolved.

## **15.8 Risk Management Responsibilities**

### **15.8.1 Managers**

- Are responsible for effective management of risk.
- Select from risk reduction options recommended by staff.
- Accept or reject risk based upon the benefit to be derived.
- Train and motivate personnel to use risk management techniques.
- Elevate decisions to a higher level when it is appropriate.

### **15.8.2 Staff**

- Assess risks and develop risk reduction alternatives.
- Integrate risk controls into plans and orders.
- Identify unnecessary risk controls.

### **15.8.3 Supervisors**

- Apply the risk management process
- Consistently apply effective risk management concepts and methods to operations and tasks.
- Elevate risk issues beyond their control or authority to superiors for resolution.

### **15.8.4 Individuals**

- Understand, accept and implement risk management processes.
- Maintain a constant awareness of the changing risks associated with the operation or task.
- Make supervisors immediately aware of any unrealistic risk reduction measures or high-risk procedures.

## **15.9 Systematic Risk Management: The 5-M Model**

Successful operations do not just happen; they are indicators of how well a system is functioning. The basic cause factors for accidents fall into the same categories as the contributors to successful operations—Human, Media, Machine, Mission, and Management.

Risk management is the systematic application of management and engineering principles, criteria and tools to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all operational phases. To apply the systematic risk management process, the composite of hardware, procedures, and people that accomplish the objective, must be viewed as a system.

The 5-M model, depicted in Figure 15-4, is adapted from military ORM. In this model, “Man” is used to indicate the human participation in the activity, irrespective of the gender of the human involved. “Mission” is the military term that corresponds to what we in civil aviation call “operation.” This model provides a framework for analyzing systems and determining the relationships between the elements that work together to perform the task.

The 5-M's are Man, Machine, Media, Management, and Mission. Man, Machine, and Media interact to produce a successful Mission (or, sometimes, an unsuccessful one). The amount of overlap or interaction between the individual components is a characteristic of each system and evolves as the system develops. Management provides the procedures and rules governing the interactions between the other elements.

When an operation is unsuccessful or an accident occurs, the system must be analyzed; the inputs and interaction among the 5-Ms must be thoroughly reassessed. Management is often the controlling factor in operational success or failure. The National Safety Council cites the management processes in as many as 80 percent of reported accidents.

### 15.9.1 Man

The human factor is the area of greatest variability, and thus the source of the majority of risks.

*Selection:* The right person psychologically and physically, trained in event proficiency, procedures and habit patterns.

*Performance:* Awareness, perceptions, task saturation, distraction, channeled attention, stress, peer pressure, confidence, insight, adaptive skills, pressure/workload, fatigue (physical, motivational, sleep deprivation, circadian rhythm).

*Personal Factors:* Expectancies, job satisfaction, values, families/friends, command/control, perceived pressure (over tasking) and communication skills.

### 15.9.2 Media

Media are defined as external, and largely environmental and operational conditions. For example:

*Climatic:* Ceiling, visibility, temperature, humidity, wind, precipitation.

*Operational:* Terrain, wildlife, vegetation, human made obstructions, daylight, and darkness.

*Hygienic:* Ventilation/air quality, noise/vibration, dust, and contaminants.

*Vehicular/Pedestrian:* Pavement, gravel, dirt, ice, mud, dust, snow, sand, hills, curves.

### 15.9.3 Machine

Hardware and software used as intended, limitations interface with man.

*Design:* Engineering reliability and performance, ergonomics.

*Maintenance:* Availability of time, tools, and parts, ease of access.

*Logistics:* Supply, upkeep, and repair.

*Technical data:* Clear, accurate, useable, and available.

#### 15.9.4 Management

Directs the process by defining standards, procedures, and controls. Although management provides procedures and rules to govern interactions, it cannot completely control the system elements. For example: weather is not under management control and individual decisions affect personnel far more than management policies.

*Standards:* FAA Policy and Orders.

*Procedures:* Checklists, work cards, and manuals.

*Controls:* Crew rest, altitude/airspeed/speed limits, restrictions, training rules/limitations.

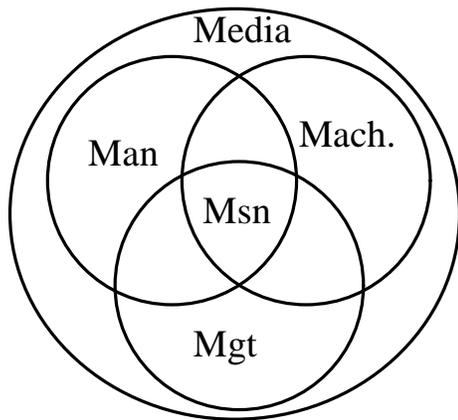
*Operation.* The desired outcome.

#### 15.9.5 Mission (Operation)

*Objectives:* Complexity understood, well defined, obtainable. The results of the interactions of the other -M's (Man, Media, Machine, and Management).

Figure 15-4: The 5-M Model

## 5M model of System Engineering



- Msn - Mission: central purpose or functions
- Man - Human element
- Mach - Machine: hardware and software
- Media - Environment: ambient and operational environment
- Mgt- Management: procedures, policies, and regulations

## **15.10 Levels of Risk Management**

The risk management process operates on three levels. Although it would be preferable to perform an in-depth application of risk management for every operation or task, the time and resources may not always be available. The three levels are as follow:

### **15.10.1 Time-Critical**

Time-critical risk management is an "on the run" mental or verbal review of the situation using the basic risk management process without necessarily recording the information. This time-critical process of risk management is employed by personnel to consider risk while making decisions in a time-compressed situation. This level of risk management is used during the execution phase of training or operations as well as in planning and execution during crisis responses. It is also the most easily applied level of risk management in off-duty situations. It is particularly helpful for choosing the appropriate course of action when an unplanned event occurs during execution of a planned operation or daily routine.

### **15.10.2 Deliberate**

Deliberate Risk Management is the application of the complete process. It primarily uses experience and brainstorming to identify risks, hazards and develops controls and is therefore most effective when done in a group. Examples of deliberate applications include the planning of upcoming operations, review of standard operating, maintenance, or training procedures, and damage control or disaster response planning.

### **15.10.3 Strategic**

This is the deliberate process with more thorough hazard identification and risk assessment involving research of available data, use of diagram and analysis tools, formal testing, or long term tracking of the risks associated with the system or operation (normally with assistance from technical experts). It is used to study the hazards and their associated risks in a complex operation or system, or one in which the hazards are not well understood. Examples of strategic applications include the long-term planning of complex operations, introduction of new equipment, materials and operational, development of tactics and training curricula, high risk facility construction, and major system overhaul or repair. Strategic risk management should be used on high priority or high visibility risks.

## **15.11 ORM Process Expansion**

Many aspects of the ORM process utilize the same risk management tools described throughout this handbook. There are some unique contributions and issues in the ORM process which are expanded in this section.

### **15.11.1 Hazard identification expansion**

Hazard identification, the foundation of the entire ORM process, and an analysis of control measures require further expansion. Figure 15-3 depicts the actions necessary to identify hazards. Specifically, identify hazards associated with these three categories:

Operational or System Degradation.
------------------------------------

Injury or Death.
------------------

Property Damage.
------------------

**Action 1—Task Analysis**

The 5-M's are examined. This is accomplished by reviewing current and planned operations. Management defines requirements and conditions to accomplish the tasks. Construct a list or chart depicting the major phases of the operation or steps in the job process, normally in time sequence. Break the operation down into 'bite size' chunks.

Some tools that will help perform operation/task analysis are:

Operations Analysis/Flow Diagram
----------------------------------

Preliminary Hazard Analysis (PHA)
-----------------------------------

Multi-linear Events Sequence (MES)
------------------------------------

**Action 2—List Hazards**

Hazards are identified based on the deficiency to be corrected and the definition of the operation and system requirements. The output of the identification phase is a listing of inherent hazards or adverse conditions and the accidents, which could result. Examples of inherent hazards in any one of the elements include fire, explosion, and collision with ground, wind, or electrocution. The analysis must also search for factors that can lead to hazards such as alertness, ambiguity, or escape route. In addition to a hazard list for the elements above, interfaces between or among these elements should be investigated for hazards. Make a list of the hazards associated with each phase of the operation or step in the job process. Stay focused on the specific steps in the operation being analyzed. Try to limit your list to "big picture" hazards. Hazards should be tracked on paper or in a computer spreadsheet/database system to organize ideas and serve as a record of the analysis for future use. Tools that help list hazards are:

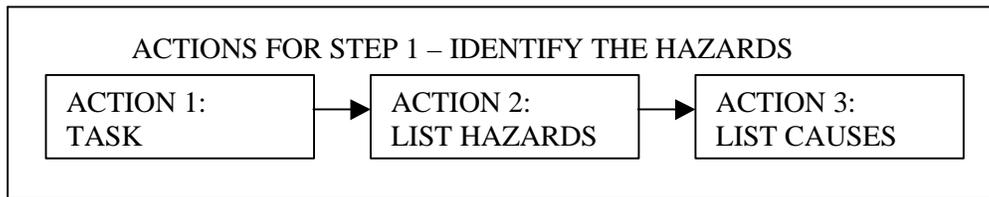
Preliminary Hazard Analysis
-----------------------------

“What if” Tool
----------------

Scenario Process Tool
-----------------------

Logic Diagram  
Change Analysis Tool  
Opportunity Assessment  
Training Realism Assessment.

**Figure 15-3. Identify Hazards Actions**



### **Action 3—List Causes**

Make a list of the causes associated with each hazard identified in the hazard list. A hazard may have multiple causes related to each of the 5-M's. In each case, try to identify the root cause (the first link in the chain of events leading to operational degradation, personnel injury, death, or property damage). Risk controls can be effectively applied to root causes. Causes should be annotated with the associated hazards in the same paper or computer record mentioned in the previous action. The same tools for Action 2 can be used here.

### **Strategic Tools**

If time and resources permit, and additional hazard information is required, use strategic hazard analysis tools. These are normally used for medium and long term planning, complex operations, or operations in which the hazards are not well understood.

The first step of in-depth analysis should be to examine existing databases or available historical and hazard information regarding the operation. Suggested tools are:

Accident analysis  
Cause and effect diagrams

The following tools are particularly useful for complex, coordinated operations in which multiple units, participants, and system components and simultaneous events are involved:

Multi-linear event sequence (MES).  
Interface analysis.  
Failure mode and effect analysis.

The following tools are particularly useful for analyzing the hazards associated with physical position and movement of assets:

Mapping tool.

Energy trace and barrier analysis.

Interface analysis.

## **SEVEN PRIMARY HAZARD IDENTIFICATION TOOLS**

- **THE OPERATIONS ANALYSIS**
- **THE PRELIMINARY HAZARD ANALYSIS**
- **THE WHAT IF TOOL**
- **THE SENARIO PROCESS TOOL**
- **THE LOGIC DIAGRAM**
- **THE CHANGE ANALYSIS**
- **THE CAUSE AND EFFECT TOOL**

### **Figure 15-4: The Primary Family of Hazard Identification Tools**

There are many additional tools that can help identify hazards. One of the best is through a group process involving representatives directly from the workplace. Most people want to talk about their jobs, therefore a simple brainstorming process with a facilitator is often very productive. The following is a partial list of other sources of hazard identification information:

*Accident/Incident Reports:* These can come from within the organization, for it represents memory applicable to the local workplace, cockpit, flight, etc. Other sources might be NTSB reports, medical reports, maintenance records, and fire and police reports.

*Operational Personnel:* Relevant experience is arguably the best source of hazard identification. Reinventing the wheel each time an operation is proposed is neither desired nor efficient. Seek out those with whom you work who have participated in similar operations and solicit their input.

*Outside Experts:* Look to those outside your organization for expert opinions or advice.

*Current Guidance:* A wealth of relevant direction can always be found in the guidance that governs our operations. Consider regulations, operating instructions, checklists, briefing guides, SOPs, NOTAMs, and policy letters.

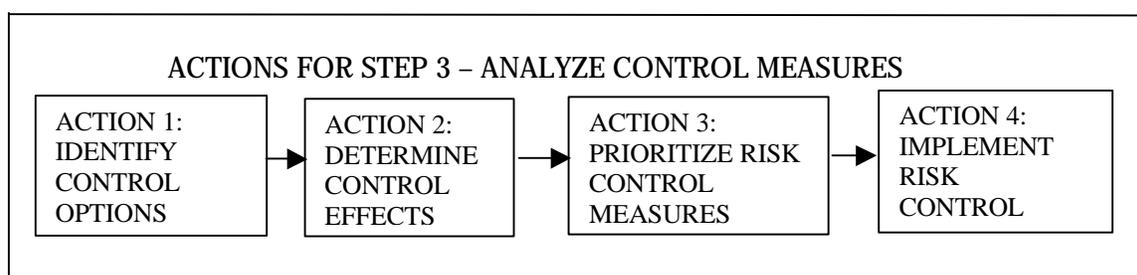
*Surveys:* The survey can be a powerful tool because it pinpoints people in the operation with first hand knowledge. Often, first line supervisors in the same facility do not have as good an understanding of risk as those who confront it every day.

*Inspections:* Inspections can consist of spot checks, walk-through, checklist inspections, site surveys, and mandatory inspections. Utilize staff personnel to provide input beyond the standard third-party inspection.

### 15.11.2 Analyze Control Measures

Hazard control is accomplished in several ways. Figure 15-5 depicts the actions necessary to analyze the alternatives.

**Figure 15-5. Analyze Control Measures Actions**



#### **Action 1—Identify Control Options**

Starting with the highest-risk assessed, identify as many risk control options as possible for all hazards. Refer to the list of possible causes from Step 1 for control ideas. The Control Options Matrix and “What-If” analyses are excellent tools to identify control options. Risk control options include: **rejection, avoidance, delay, transference, spreading, compensation, and reduction.**

#### **Action 2—Determine Control Effects**

Determine the effect of each control on the risk associated with the hazards. A computer spread sheet or data form may be used to list control ideas and indicate control effects. The estimated value(s) for severity and/or probability after implementation of control measures and the change in overall risk assessed from the Risk Assessment Matrix should be recorded. Scenario building and next accident assessment provides the greatest ability to determine control effects.

#### **Action 3—Prioritize Risk Controls/ Measures**

For each risk, prioritize those risk controls that will reduce the risk to an acceptable level. The best controls will be consistent with objectives and optimize use of available resources (manpower, material, and equipment, money, time). Priorities should be recorded in some standardized format for future reference. Opportunity assessment, cost versus benefit analysis and computer modeling provide excellent aids to prioritize risk controls. If the control is already implemented in an established instruction, document, or procedure, that too should be documented.

The "standard order of precedence" indicates that the ideal action is to "plan or design for minimum risk" with less desirable options being, in order, to add safety devices, add warning devices, or change procedures and training. This order of preference makes perfect sense while the system is still being designed, but once the system is fielded this approach is frequently not cost effective. Redesigning to eliminate a risk or add safety or warning devices is both expensive and time consuming and, until the retrofit is complete, the risk remains unabated.

Normally, revising operational or support procedures may be the lowest cost alternative. While this does not eliminate the risk, it may significantly reduce the likelihood of an accident or the severity of the outcome (risk) and the change can usually be implemented quickly. Even when a redesign is planned, interim changes in procedures or maintenance requirements are usually required. In general, these changes may be as simple as improving training, posting warnings, or improving operator or technician qualifications. Other options include preferred parts substitutes, instituting or changing time change requirements, or increased inspections.

The feasible alternatives must be evaluated, balancing their costs and expected benefits in terms of operational performance, dollars and continued risk exposure during implementation. A completed risk assessment should clearly define these tradeoffs for the decision-maker.

**Some Special Considerations in Risk Control.** The following factors should be considered when applying the third step of ORM.

Try to apply risk controls only in those activities and to those who are actually at risk. Too often risk controls are applied indiscriminately across an organization leading to wasted resources and unnecessary irritation of busy operational personnel.

Apply redundant risk controls when practical and cost effective. If the first line of defense fails, the back up risk control(s) may prevent loss.

Involve operational personnel, especially those likely to be directly impacted by a risk control, in the selection and development of risk controls whenever possible. This involvement will result in better risk controls and in general a more positive risk control process.

Benchmark (find best practices in other organizations) as extensively as possible to reduce the cost associated with the development of risk controls. Why expend the time and resources necessary to develop a risk control and then have to test it in application when you may be able to find an already complete, validated approach in another organization?

Establish a timeline to guide the integration of the risk control into operational processes.

#### ***Action 4 — Implement Risk Controls***

Once the risk control decision is made, assets must be made available to implement the specific controls. Part of implementing control measures is informing the personnel in the system of the risk management process results and subsequent decisions. If there is a disagreement, then the decision-makers should provide a rational explanation. Careful documentation of each step in the risk management process facilitates risk communication and the rational processes behind risk management decisions. Figure 15-6 depicts the actions necessary to complete this step.

**Figure 15-6: Actions to Implement Risk Controls**

## ACTIONS FOR STEP 4—IMPLEMENT RISK CONTROLS

**Step 1—Make Implementation Clear**

To make the implementation directive clear, consider using examples, providing pictures or charts, including job aids, etc. Provide a roadmap for implementation, a vision of the end-state, and describe successful implementation. The control measure must be deployed in a method that insures it will be received positively by the intended audience. This can best be achieved by designing in user ownership.

**Step 2—Establish Accountability**

Accountability is an important area of ORM. The accountable person is the one who makes the decision (approves the control measures), and hence, the right person (appropriate level) must make the decision. Also, be clear on who is responsible at the unit level for implementation of the risk control.

**Step 3—Provide Support**

To be successful, management must be behind the control measures put in place. Prior to implementing a control measure, get approval at the appropriate level. Then, explore appropriate ways to demonstrate commitment. Provide the personnel and resources necessary to implement the control measures. Design in sustainability from the beginning and be sure to deploy the control measure along with a feedback mechanism that will provide information on whether the control measure is achieving the intended purpose.

**Common Problems in Implementing Risk Controls**

A review of the historical record of risk controls indicates that many never achieve their full potential. The primary reason for shortfalls is failure to effectively involve the personnel who are actually impacted by a risk control. Note that virtually all these factors are driven by the failure to properly involve personnel impacted by risk controls in the development and implementation of the risk controls. Shortfalls include:

- The control is inappropriate for the problem.
- Operators dislike it.
- Managers dislike it.
- It turns out to be too costly (unsustainable).
- It is overmatched by other priorities.
- It is misunderstood.

- Nobody measures progress until it is too late.

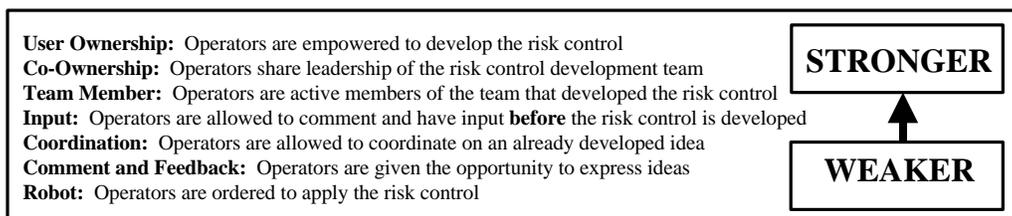
### Procedures for Implementing Risk Controls within an Organizational Culture

The following procedures provide useful guidance for shaping a risk control within an organizational culture. Followed carefully they will significantly improve the impact and duration of the effectiveness of risk controls.

Develop the risk control within the organization's culture. Every organization has a style or a culture. While the culture changes over time due to the impact of managers and other modifications, the personnel in the organization know the culture at any given time. It is important to develop risk controls, which are consistent with this culture. For example, a rigid, centrally directed risk control would be incompatible with an organizational culture that emphasizes decentralized flexibility. Conversely, a decentralized risk control may not be effective in an organization accustomed to top down direction and control. If you have any doubts about the compatibility of a risk control within your organization, ask some personnel in the organization what they think. People are the culture and their reactions will tell you what you need to know.

Generate maximum possible involvement of personnel impacted by a risk control in the implementation of the risk control. Figure 15-7 provides a tool to assist in assessing this "involvement factor." The key to making ORM a fully integrated part of the organization culture, is to achieve user ownership in a significant percentage of all risk controls that are developed and implemented by the personnel directly impacted by the risk..

**Figure 15-7: Levels of User Involvement in Risk Controls**



Develop the best possible supporting tools and guides (infrastructure) to aid operating personnel in implementing the risk control. Examples include standard operating procedures (SOPs), model applications, job aids, checklists, training materials, decision guides, help lines, and similar items. The more support that is provided, the easier the task for the affected personnel. The easier the task, the greater the chances for success.

Develop a time line for implementing the risk control. Identify major milestones, being careful to allow reasonable timeframes and assuring that plans are compatible with the realities of organizational resource constraints.

### Procedures for Generating Management Involvement in Implementing Risk Controls

Manager and supervisor's influence behind a risk control can greatly increase its chances of success. It is usually a good idea to signal clearly to an organization that there is interest in a risk control if the manager in fact has some interest. Figure 15-8 illustrates actions in order of priority that can be taken to signal leader support. Most managers are interested in risk control and are willing to do anything reasonable to support the process. Take the time as you develop a risk control to visualize a role for organization leaders.



**Figure 15-8. Levels of Command Involvement**

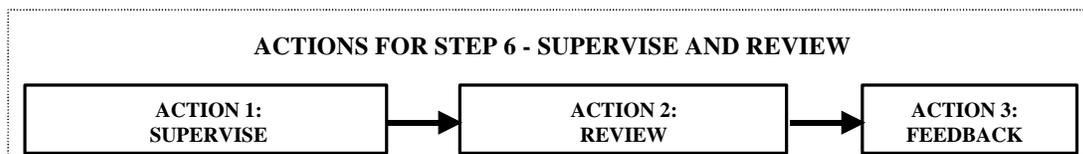
### Procedures for Sustaining Risk Control Effectiveness

To be fully effective, risk controls must be sustained. This means maintaining the responsibility and accountability for the long haul. If the risk control has been well designed for compatibility with the organization operation and culture this should not be difficult. Managers must maintain accountability and yet provide a reasonable level of positive reinforcement as appropriate.

### Supervise and Review

The sixth step of ORM, Supervise and Review, involves the determination of the effectiveness of risk controls throughout the operation. This step involves three aspects. The first is monitoring the effectiveness of risk controls. The second is determining the need for further assessment of either all or a portion of the operation due to an unanticipated change as an example. The last is the need to capture lessons-learned, both positive and negative, so that they may be a part of future activities of the same or similar type. Figure 15-9 depicts the actions necessary to complete this step.

**Figure 15-9: Supervise and Review Actions**



### **Action 1—Supervise**

Monitor the operation to ensure:

- The controls are effective and remain in place.
- Changes, which require further risk management, are identified.
- Action is taken when necessary to correct ineffective risk controls and reinitiate the
- Risk management steps in response to new hazards.

Any time the personnel, equipment, or tasking change or new operations are anticipated in an environment not covered in the initial risk management analysis, the risks and control measures should be reevaluated. The best tool for accomplishing this is change analysis.

Successful performance is achieved by shifting the cost versus benefit balance more in favor of benefit through controlling risks. By using ORM whenever anything changes, we consistently control risks, those known before an operation and those that develop during an operation. Being proactive and addressing the risks before they get in the way of operation accomplishment saves resources, enhances operational performance, and prevents the accident chain from ever forming.

### ***Action 2—Review***

The process review must be systematic. After assets are expended to control risks, then a cost benefit review must be accomplished to see if risk and cost are in balance. Any changes in the system (the 5-M model, and the flow charts from the earlier steps provide convenient benchmarks to compare the present system to the original) are recognized and appropriate risk management controls are applied.

To accomplish an effective review, supervisors need to identify whether the actual cost is in line with expectations. Also the supervisor will need to see what effect the control measure has had on operational performance. It will be difficult to evaluate the control measure by itself so focus on the aspect of operational performance the control measure was designed to improve.

A review by itself is not enough, a feedback system must be established to ensure that the corrective or preventative action taken was effective and that any newly discovered hazards identified during the operation are analyzed and corrective action taken. When a decision is made to assume risk, the factors (cost versus benefit information) involved in this decision should be recorded. When an accident or negative consequences occur, proper documentation allows for the review of the risk decision process to see where errors might have occurred or if changes in the procedures and tools lead to the consequences. Secondly, it is unlikely that every risk analysis will be perfect the first time. When risk analyses contain errors of omission or commission, it is important that those errors be identified and corrected. Without this feedback loop, we lack the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

Measurements are necessary to ensure accurate evaluations of how effectively controls eliminated hazards or reduced risks. After action reports, surveys, and in progress reviews provide great starting places for measurements. To be meaningful, measurements must quantitatively or qualitatively identify reductions of risk, improvements in operational success, or enhancement of capabilities.

**Action 3—Feedback**

A review by itself is not enough: a feedback system must be established to ensure that the corrective or preventative action taken was effective and that any newly discovered hazards identified during the operation are analyzed and corrective action taken. Feedback informs all involved as to how the implementation process is working, and whether or not the controls were effective. Whenever a control process is changed without providing the reasons, co-ownership at the lower levels is lost. The overall effectiveness of these implemented controls must also be shared with other organizations that might have similar risks to ensure the greatest possible number of people benefit. Feedback can be in the form of briefings, lessons learned, cross-tell reports, benchmarking, database reports, etc. Without this feedback loop, we lack the benefit of knowing if the previous forecasts were accurate, contained minor errors, or were completely incorrect.

**Monitoring the Effectiveness of Implementation**

This aspect of the supervise and review step should be routine. Periodically monitor the progress of implementation against the planned implementation schedule that should have been developed during the third and fifth ORM steps. Take action as necessary to maintain the planned implementation schedule or make adjustments as necessary.

**Monitoring the Effectiveness of Risk Controls**

If the risk control has been well designed, it will favorably change either physical conditions or personnel behavior during the conduct of an operation. The challenge is to determine the extent to which this change is taking place. If there has been no change or only minor change, the risk control is possibly not worth the resources expended on it. It may be necessary to modify it or even rescind it. At first thought it may seem obvious that we need only determine if the number of accidents or other losses has decreased. This is only practical at higher levels of management. Even at those levels of management where we have sufficient exposure to validly assess actual losses, it may be a year or more before significant changes actually occur. This is too long to wait to assess the effectiveness of risk controls. Too much effort may have been invested before we can determine the impact of our proposals. We need to know how we are doing much sooner. If we can't efficiently measure effectiveness using accident rates, how can we do it? The answer is to directly measure the degree of risk present in the system.

**Direct Measures of Behavior.** When the target of a risk control is behavior, it is possible to actually sample behavior changes in the target group. Making a number of observations of the use of restraints before initiating the seat belt program and a similar sample after, for example, can assess the results of an effort to get personnel to wear seat belts. The change, if any, is a direct measure of the effectiveness of the risk control. The sample would establish the percent of personnel using belts as a percentage of total observations. Subsequent samples would indicate our success in sustaining the impact of the risk control.

**Direct Measures of Conditions.** It is possible to assess the changes in physical conditions in the workplace. For example, the amount of foreign objects found on the flight line can be assessed before and after a risk control initiative aimed at reducing foreign object damage.

**Measures of Attitudes.** Surveys can also assess the attitudes of personnel toward risk-related issues. While constructing survey questions is technical and must be done right, the FAA often conducts surveys and it may be possible to integrate questions in these surveys, taking advantage of the experts who manage these survey processes. Nevertheless, even informal surveys taken verbally in very small organizations will quickly indicate the views of personnel.

**Measures of Knowledge.** Some risk controls are designed to increase knowledge of some hazard or of hazard control procedures. A short quiz, perhaps administered during a safety meeting before and after a training risk control is initiated.

**Safety and Other Loss Control Reviews Procedures.** Programmatic and procedural risk control initiatives (such as revisions to standard operating procedures) can be assessed through various kinds of reviews. The typical review involves a standard set of questions or statements reflecting desirable standards of performance against which actual operating situations are compared.

## **15.12 Conclusion**

Operational risk management provides a logical and systematic means of identifying and controlling risk. Operational risk management is not a complex process, but does require individuals to support and implement the basic principles on a continuing basis. Operational risk management offers individuals and organizations a powerful tool for increasing effectiveness and reducing accidents. The ORM process is accessible to and usable by everyone in every conceivable setting or scenario. It ensures that all FAA personnel will have a voice in the critical decisions that determine success or failure in all our operations and activities. Properly implemented, ORM will always enhance performance.

## Chapter 16: Operational Safety in Aviation

<b>16.1</b>	<b>GLOBAL AVIATION INFORMATION NETWORK (GAIN)</b> .....	<b>1</b>
<b>16.2</b>	<b>FLIGHT OPERATIONS QUALITY ASSURANCE PROGRAM (FOQA)</b> .....	<b>4</b>
<b>16.3</b>	<b>SPECIAL SAFETY STUDIES AND DATA ANALYSIS</b> .....	<b>5</b>
<b>16.4</b>	<b>OPERATOR'S FLIGHT SAFETY HANDBOOK (OFSH)</b> .....	<b>6</b>

## 16.0 Operational Safety in Aviation

This chapter summarizes recent initiatives and other related activities appropriate to operational safety in aviation. The Global Aviation Information Network (GAIN) program is discussed. Special safety studies and data analyses directed to aircraft performance risk assessment are presented, and the Operator's Flight Safety Handbook (OFSH) is summarized and discussed.

Many years ago Heinrich conducted a statistical study of accidents and determined that out of 300 incidents, one fatal accident may occur. This provided a general analogy of a ratio of 1 to 300. Years later, Frank Byrd conducted a similar study and noted that out of 600 incidents, one fatal accident occurred, indicating a ratio of 1 to 600. Figure 16-1 illustrates the concept that for every accident or incident that is reported, there may be a much larger number that are not reported.

It is important to identify incidents that could have resulted in accidents. An incident is any occurrence that could have resulted in an accident, i.e., fatal harm. But since the harm did not occur, it is considered an incident. The point is that all incidents that could have resulted in an accident should be reported to determine the relevant factors associated with that incident.

### Heinrich Pyramid

---

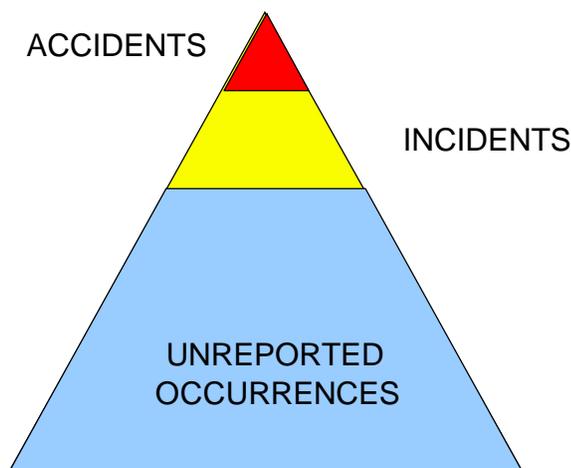


Figure 16-1

## 16.1 Global Aviation Information Network (GAIN)

The Federal Aviation Administration (FAA) first proposed a Global Analysis and Information Network (GAIN) in May 1996 for the worldwide collection, analysis, and dissemination of safety information to help the aviation community reach the goal of zero accidents. GAIN was envisioned by the FAA as a

FAA System Safety Handbook, Chapter 16: Operational Safety in Aviation  
December 30, 2000

privately owned and operated international information infrastructure that would use a broad variety of worldwide aviation data sources together with comprehensive analytical techniques to assist in identifying emerging safety concerns.



As the aviation community exchanged ideas on the GAIN concept over the first 2 ½ years after its announcement, a variety of descriptions were applied to GAIN by various segments of the aviation community. The GAIN Steering Committee considered various comments and recommendations on GAIN and agreed upon the following description of GAIN in January 1999:

“GAIN promotes and facilitates the voluntary collection and sharing of safety information by and among users in the international aviation community to improve safety.”

The Steering Committee also changed the meaning of the GAIN acronym to “Global Aviation Information Network” to better define the program.

The GAIN organization consists of the Steering Committee, Working Groups, Program Office, and a planned Government Support Team.

The **Steering Committee** consists of industry stakeholders (airlines, manufacturers, employee groups and their trade associations) that set high-level GAIN policy, issue charters to direct the Working Groups, and guide the Program Office. Represented on the GAIN Steering Committee are Airbus Industrie, Air France, Air Line Pilots Association (ALPA), Air Transport Association (ATA), Boeing Commercial Airplane Group, British Airways, Continental Airlines, Flight Safety Foundation, International Association of Machinists (IAM), Japan Airlines, National Air Traffic Controller Association (NATCA), National Business Aviation Association (NBAA), Northwest Airlines, and the U.S. military. The Steering Committee meets on a quarterly basis.

The **Executive Committee** is comprised of several Steering Committee members and acts on behalf of the whole Steering Committee on administrative matters or as directed.

The **Working Groups** are interdisciplinary industry/government teams that work GAIN issues in a largely autonomous fashion, within the charters established for them by the Steering Committee. Working Groups are listed below in paragraph 16.1.2.

The **Program Office** administers GAIN and supports the Steering Committee, Working Groups, and the Government Support Team by communicating with GAIN participants, planning meetings and conferences, preparing meeting minutes, and other tasks.

A **Government Support Team (GST)** is planned, which will include representatives of government regulatory authorities from various countries plus related international groups. The GST will provide assistance to airlines and air traffic organizations in developing or improving safety reporting systems and sharing safety information.

FAA System Safety Handbook, Chapter 16: Operational Safety in Aviation  
December 30, 2000

### 16.1.1 The 1999 GAIN Action Plan

Acknowledging that the groundwork had been laid at the Long Beach conference, the GAIN Steering Committee unanimously agreed at their January 1999 meeting that the time had come to begin implementing the global sharing of safety information. After reviewing a compilation of comments and recommendations made by GAIN participants, the Steering Committee developed a 1999 GAIN Action Plan addressing the following areas:

- Increase global awareness of and support for GAIN
- Increase participation from the international aviation community to continue the expansion of GAIN
- Influence the reduction of organizational, regulatory, civil litigation, criminal sanction, and public disclosure impediments to voluntary, non-punitive collecting and sharing of safety information
- Promote the initiation of additional internal safety data collection and analysis programs, with the help of GAIN partners
- Support expansion of existing sharing among users
- Promote development and use of analytical methods and tools
- Plan next GAIN conference to continue development and assess progress.

### 16.1.2 GAIN Working Groups

The Steering Committee established four GAIN Working Groups (WGs) to assist the Steering Committee in implementing the 1999 GAIN Action Plan, and developed charters to define the responsibilities of each working group. Brief descriptions of the Working Groups are provided below.

**WG A: Aviation Operator Safety Practices** - This group will develop products to help operators obtain information on starting, improving, or expanding their internal aviation safety programs. The products should include commonly accepted standards and best operating practices, methods, procedures, tools and guidelines for use by safety managers. The group will identify currently available materials that support the development of these products. These materials could include sample safety reporting forms, computer programs for tracking safety reports, suggested procedures, manuals, and other information to help operators start or improve programs without "reinventing the wheel." The working group will then develop products that safety officers can use to implement programs to collect, analyze, and share aviation safety information.

**WG B: Analytical Methods and Tools** - The group will: (a) identify and increase awareness of existing analytical methods and tools; (b) solicit requirements for additional analytical methods and tools from the aviation community; and (c) promote the use of existing methods and tools as well as the development of new ones. The group will endeavor to address various types of safety data and information (including voluntary reports and digitally derived aircraft and ATC system safety performance data). They will also benchmark or validate to the extent possible the usefulness and usability of the tools and level of proficiency needed as a guide for potential users, identify data needs where required for use of tools, and transfer knowledge about methods and tools to users.

**WG C: Global Information Sharing Prototypes** - This group will develop prototypes to begin global sharing of aviation safety information. These prototypes could include (a) a sharing system capability for automated sharing of safety incident/event reports derived from existing and new safety reporting systems to enhance current sharing activities among airline safety managers; (b) a sharing library containing safety

FAA System Safety Handbook, Chapter 16: Operational Safety in Aviation  
December 30, 2000

information "published" by airlines and other aviation organizations; (c) an aviation safety Internet site to encourage use of existing "public" information/data sources.

**WG D: Reducing Impediments (Organizational, Regulatory, Civil Litigation, Criminal Sanction, and Risk of Public Disclosure)** - This working group will identify and evaluate barriers that prevent the collection and sharing of aviation safety information among various organizations and propose solutions that are reasonable and effective. They will pursue changes in ICAO Annexes to appropriately protect information from accident/incident prevention programs. They will propose means to obtain legislation to protect reporters and providers of safety information. They will promote "jeopardy-free" reporting procedures and create methods to obtain organizational commitment to sharing safety information.

## **16.2 Flight Operations Quality Assurance Program (FOQA)**

The FAA Administrator has announced that the FAA will soon issue a notice of proposed rulemaking on Flight Operations Quality Assurance Programs (FOQA).

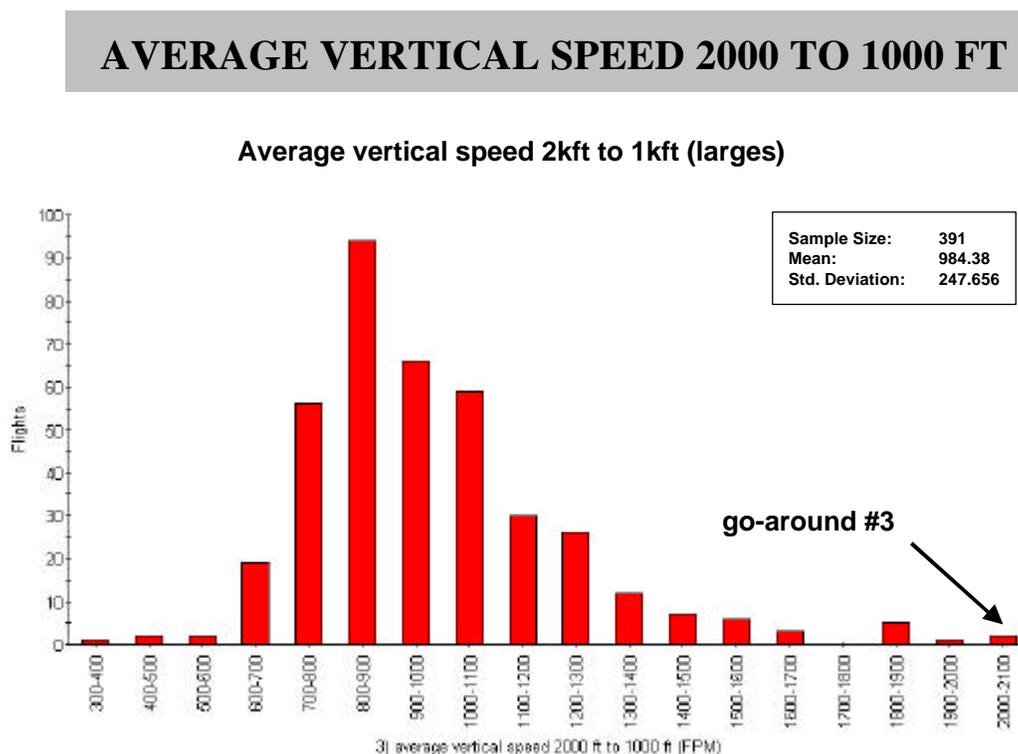
"This rule is intended to encourage the voluntary implementation of FOQA by providing assurance that information obtained from such programs cannot be used by the FAA for punitive enforcement purposes,"

FOQA is the voluntary collection, analysis, and sharing of routine flight operation data, obtained by analysis of flight data recorder information. The FOQA program is one of several where the FAA is working in partnership with industry and labor to enhance aviation safety.

The FAA also has a new program where the FAA is working in partnership with industry to use improved methods and technology to detect potential defects in aircraft engines

## 16.3 Special Safety Studies and Data Analysis

*Figure 16.1-1 Example Histogram for Illustrative Purposes Only*



### 16.3.1 Model Development

FAA, in cooperation with NASA and general industry, is developing models to evaluate aviation data from routine flights in order to identify precursor events that indicate a risk of incidents and accidents. Models are under development by the Office of System Safety, working in conjunction with the System Data and Modeling activity of the NASA Aviation Safety Program (AvSP). The modeling effort is closely related to the Aviation Performance Measurement System (APMS) program, Global Aviation Information Network (GAIN), and Flight Operations Quality Assurance (FOQA) programs. APMS is being developed by NASA to provide technical tools to ease the large-scale implementation of flight data analyses in support of airline FOQA. The GAIN program is designed to promote the sharing of safety information including aircraft flight data, to proactively improve safety.

One of the models under development is the Aircraft Performance Risk Assessment Model (ASPRAM). It has the objective of using empirical data and expert judgment to quantify the risk of incidents and accidents. The general approach is to develop an automated means of analyzing commercial aircraft flight

FAA System Safety Handbook, Chapter 16: Operational Safety in Aviation  
December 30, 2000

recorder data from non-accident precursors and their causes. Expert opinion is incorporated into the automated model through the use of knowledge-based rules, which are used to identify precursor events and assess the risk of incidents and accidents.

## 16.4 Operator's Flight Safety Handbook (OFSH)

The GAIN "Aviation Operator's Safety Practices" Working Group has developed the "Operator's Flight Safety Handbook" (OFSH). Specifically, the international aviation safety community, in coordination with industry and government, worked together to modify the Airbus "Flight Safety Manager's Handbook" to a generic, worldwide product. It is intended to serve as a guide for the creation and operation of a flight safety function within an operator's organization. The operator is encouraged to tailor the document as necessary to be compatible with the philosophy, practices, and procedures of the organization.<sup>1</sup>

**Section 1** of the OFSH<sup>2</sup> lists the important elements of an effective safety program:

- Senior management commitment to the company safety program
- Appointment of a Flight Safety Offices reporting directly to the CEO
- Encouragement of a positive safety culture
- Hazard identification and risk management
- Ongoing hazard reporting system
- Safety audits and assessment of quality or compliance
- Accident and incident reporting and investigation
- Documentation
- Immunity-based reporting systems
- Implementation of a Digital Flight Data Recorder information collection agreement with the pilots
- The exchange of valuable "Lessons Learned" with manufacturers and other airlines
- Safety training integration into the organization's training syllabi
- Human Factors training for all personnel
- Emergency response planning
- Regular evaluation and ongoing fine tuning of the program.

**Section 2** of the OFSH discusses Organization and Administration. "*A safety programme is essentially a coordinated set of procedures for effectively managing the safety of an operation.*"<sup>3</sup> Management should: specify the company's standards, ensure the everyone knows the standard and accepts them, make sure there is a system in place so that deviations from the standard are recognized, reported, and corrected.

The Company's Policy Manual should contain a signed statement the Chief Executive Officer which specifies the safety culture and commitment in order to give credence and validation.

**Section 3** outlines the elements of a Safety Program:

---

<sup>1</sup> GAIN Working Group A, "Aviation Operator's Safety Handbook", 3<sup>rd</sup> Draft Review, March 13-14, 2000.

<sup>2</sup> IBID, GAIN Working Group A.

<sup>3</sup> IBID, GAIN Working Group A

FAA System Safety Handbook, Chapter 16: Operational Safety in Aviation  
December 30, 2000

- Safety Objectives
- Flight Safety Committee
- Hazard Reporting
- Immunity-based Reporting
- Compliance and Verification
- Safety Trends Analysis
- FOQA Collection/Analysis
- Dissemination of Flight Safety Information
- Liaison with other Departments

**Section 4** is a review of Human Factors issues in aviation. The key points touched on in this section include:

- Human Error
- Ergonomics
- The SHEL Model
- Aim of Human Factors in Aviation
- Safety & Efficiency
- Personality vs. Attitude
- Crew Resource Management

**Section 5** discusses the concepts of Incident/Accident Investigation and Reports. Specific definitions of concepts associated with incident/accident investigation is presented. Accident investigation and reporting is also addressed.

**Section 6** discusses Emergency Response and Crisis Management. A detailed checklist is provided which provides requirements for a Crisis Management Center.

**Section 7** of the AOS handbook discusses Risk Management. The true cost of risk is highlighted as well as risk profiles, decision making and cost/benefit considerations.

**Section 8** provides information on external program interfaces, safety practices of contractors, sub-contractors, and other third parties.

**The appendices** provide additional detailed information, including sample report forms, references, organization and manufacturer information, reviews of analytical methods and tools, sample safety surveys and audits, an overview of the risk management process, and corporate accident response team guidelines.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
December 30, 2000

## **Chapter 17: Human Factors Engineering and Safety Principles & Practices**

<b>17.1 FAA HUMAN FACTORS PROCESS OVERVIEW.....</b>	<b>1</b>
<b>17.2 MANAGING THE HUMAN FACTORS PROGRAM .....</b>	<b>6</b>
<b>17.3 ESTABLISH HUMAN FACTORS REQUIREMENTS .....</b>	<b>7</b>
<b>17.4 CONDUCT HUMAN FACTORS INTEGRATION.....</b>	<b>9</b>
<b>17.6 HUMAN FACTORS IN SYSTEM-TO-SYSTEM INTERFACES .....</b>	<b>13</b>
<b>17.7 HUMAN FACTORS ENGINEERING AND SAFETY GUIDELINES .....</b>	<b>15</b>

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

## **17.0 Human Factors Engineering and System Safety: Principles and Practices**

This chapter will serve as an outline for the integration of human factors into activities where safety is a major consideration. The introductory section contains an overview of the FAA human factors process and principles. The remaining sections represent key human factors functions and guidelines that must be accomplished to produce a successful human factors program. The sections offer ways that have proven successful during previously conducted programs to accomplish the integration of human factors into acquisition programs.

The critical impact of human factors on safety is well documented in programs, studies, analyses, and accident and incident investigations. FAA Order 9550.8, Human Factors Policy directs that:

Human factors shall be systematically integrated into the planning and execution of the functions of all FAA elements and activities associated with system acquisitions and system operations. FAA endeavors shall emphasize human factors considerations to enhance system performance and capitalize upon the relative strengths of people and machines. These considerations shall be integrated at the earliest phases of FAA projects.

Objectives of the human factors approach should be to: a) Conduct the planning, reviewing, prioritization, coordination, generation, and updating of valid and timely human factors information to support agency needs; b) Develop and institutionalize formal procedures that systematically incorporate human factors considerations into agency activities; and, c) Establish and maintain the organizational infrastructure that provides the necessary human factors expertise to agency programs. This chapter will help in that endeavor. Additional information on human factors support and requirements can be obtained from the AUA and AND Human Factors Coordinators or the Office of the Chief Scientific and Technical Advisor for Human Factors, AAR-100, (202) 267-7125.

### **17.1 FAA Human Factors Process Overview**

#### **17.1.1 Definition of Human Factors**

Human factors is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to equipment, systems, software, facilities, procedures, jobs, environments, training, staffing, and personnel management to produce safe, comfortable, and effective human performance.

When human factors is applied early in the acquisition process, it enhances the probability of increased performance, safety, and productivity; decreased lifecycle staffing and training costs; and becomes well-integrated into the program's strategy, planning, cost and schedule baselines, and technical trade-offs. Changes in operational, maintenance or design concepts during the later phases of a project are expensive and entail high-risk program adjustments. Identifying lifecycle costs and human performance components of system operation and maintenance during requirements definition decreases program risks and long-term operations costs.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

### **17.1.2 The Total System Concept**

Experience has proven that when people think of a system or project, they tend to focus on the tangibles (e.g., hardware and the software) that are acquired. Individuals often fail to visualize that the “user” (the people who operate and maintain the system) will have different aptitudes, abilities, and training, and will perform under various operating conditions, organizational structures, procedures, equipment configurations, and work scenarios. The total composite of these elements and the human component will determine the safety, performance, and efficiency of the system in the National Airspace System (NAS).

### **17.1.3 Total System Performance**

The probability that the total system will perform correctly, when it is available, is the probability that the hardware/ software will perform correctly, times the probability that the operating environment will not degrade the system operation, times the probability that the user will perform correctly. By defining total system this way, human performance is identified as a component of the system. A system can operate perfectly from an engineering sense in a laboratory or at a demonstration site and then not perform well when it is operated and maintained by the users at a field location. By increasing the probability that the operator can perform the task effectively in the appropriate environment the Total System Performance will increase significantly.

Hardware and software design affects both the accuracy of operator task performance and the amount of time required for each task. Applying human factors principles to the “total system” design will increase performance accuracy, decrease performance time, and enhance safety. Research has shown that designing the system to improve human performance is the most cost-effective and safe solution... especially if it is done early in the acquisition process.

### **17.1.4 Early Application of Human Factors**

In the early phases of system design or development, functions are allocated to hardware, software, or people (or they can be shared). For system and software programs (especially NDI/COTS), a market survey is conducted to reveal what and how candidate systems and software have already made these functional allocations in ways that do or do not enhance total system performance. Identifying human-system performance sensitivities associated with competing vendors/designs lowers technical risks and lifecycle costs (research, engineering, and development; acquisition and development; and operations over the economic life of the system). Since operations risks and costs are often much greater than the costs for research, engineering, and development; early assessment of lifecycle costs and risks has significant benefit to the total program cost and safety. The early development and application of a human factors program is an important key to cost containment and risk reduction. Most lifecycle costs and safety risk components are determined by decisions made during the early phases of the program management process. Early objectives of the human factors program are to ensure that:

- Human-system capabilities and limitations are properly reflected in the system requirements

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

- Human-system performance characteristics and their associated cost, benefits, and risks assist in deciding among alternatives (especially since lifecycle operation and support costs are often largely dependent upon personnel-related costs)
- Human-system performance and safety risks are appropriately addressed in program baselines

Early in the acquisition program, the investment analysis must identify for each alternative the full range of human factors and interfaces (e.g., cognitive, organizational, physical, functional, environmental) necessary to achieve an acceptable level of performance for operating, maintaining, and supporting the system in concert with meeting the system's functional requirements. The analysis should provide information on what is known and unknown about the human-system performance risks in meeting minimum system performance requirements. Potential human factors/safety issues are listed at Table 17-1.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

**Table 17-1: Potential Human Factors/Safety Issues**

<p><b>Early in the program, the following issues may need to be assessed:</b></p> <ul style="list-style-type: none"> <li>• <b>Workload:</b> Operator and maintainer task performance and workload</li> <li>• <b>Training:</b> Minimized need for operator and maintainer training</li> <li>• <b>Functional Design:</b> Equipment design for simplicity, consistency with the desired human-system interface functions, and compatibility with the expected operation and maintenance concepts</li> <li>• <b>CHI:</b> Standardization of computer-human interface (to address common functions employ similar user dialogues, interfaces, and procedures)</li> <li>• <b>Staffing:</b> Accommodation of constraints and opportunities on staffing levels and organizational structures</li> <li>• <b>Safety and Health:</b> Prevention of operator and maintainer exposure to safety and health hazards</li> <li>• <b>Special Skills and Tools:</b> Considerations to minimize the need for special or unique operator or maintainer skills, abilities, tools, or characteristics</li> <li>• <b>Work Space:</b> Adequacy of work space for personnel and their tools and equipment, and sufficient space for the movements and actions they perform during operational and maintenance tasks under normal, adverse, and emergency conditions</li> <li>• <b>Displays and Controls:</b> Design and arrangement of displays and controls (to be consistent with the operator's and maintainer's natural sequence of operational actions)</li> <li>• <b>Information Requirements:</b> Availability of information needed by the operator and maintainer for a specific task when it is needed and in the appropriate sequence</li> <li>• <b>Display Presentation:</b> Ability of labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields to be consistent across the display sets, and enhance operator and maintainer performance</li> <li>• <b>Visual/Aural Alerts:</b> Design of visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response</li> <li>• <b>I/O Devices:</b> Capability of input and output devices and methods for performing the task quickly and accurately, especially critical tasks</li> <li>• <b>Communications:</b> System design considerations to enhance required user communications and teamwork</li> <li>• <b>Procedures:</b> Design of operation and maintenance procedures for simplicity and consistency with the desired human-system interface functions</li> <li>• <b>Anthropometrics:</b> System design accommodation of personnel (e.g., from the 5th through 95th percentile levels of the human physical characteristics) represented in the user population</li> <li>• <b>Documentation:</b> Preparation of user documentation and technical manuals (including any electronic HELP functions) in a suitable format of information presentation, at the appropriate reading level, and with the required degree of technical sophistication and clarity</li> <li>• <b>Environment:</b> Accommodation of environmental factors (including extremes) to which it will be subjected and their effects on human-system performance</li> </ul>
---

### 17.1.5 The Role of the Human Factors Coordinator

The Human Factors Coordinator (HFC) provides the support for the integration of human factors engineering in the program. The HFC helps to initiate, structure, direct, and monitor the human factors efforts. The HFC serves to identify, define, analyze, and report on human performance and human factors engineering considerations to ensure they are incorporated in investment decisions. Typical human-system performance and human factors engineering studies and analyses conducted, sponsored, or supported by the HFC include requirements analyses, baselines performance studies, trade-off

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

determinations, alternative analyses, lifecycle cost estimates, cost-benefit analyses, risk assessments, supportability assessments, and operational suitability assessments. The HFC helps identify system specific and aggregate technical human factors engineering problems and issues that might otherwise go undetected for their obscurity, complexity, or elaborate inter-relationships. The human performance considerations are developed for staffing levels, operator and maintainer skills, training strategies, human-computer interface, human engineering design features, safety and health issues, and workload and operational performance considerations in procedures and other human-system interfaces. The HFC facilitates the establishment of the necessary tools, techniques, methods, databases, metrics, measures, criteria, and lessons learned to conduct human factors analyses in investment analysis activities. The HFC provides technical quality control of human factors products, participates in special working groups, assists in team reviews, helps prepare documentation, and collaborates on technical exchanges among government and contractor personnel.

Human factors considerations relevant to meeting system performance and functional requirements (and having safety implications) include:

- Human performance (e.g., human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, and team versus individual performance)
- Training (e.g., length of training, training effectiveness, retraining, training devices and facilities, and embedded training)
- Staffing (e.g., staffing levels, team composition, and organizational structure)
- Personnel selection (e.g., minimum skill levels, special skills, and experience levels)
- Safety and health aspects (e.g., hazardous materials or conditions, system or equipment design, operational or procedural constraints, biomedical influences, protective equipment, and required warnings and alarms).

The HFC provides input to the acquisition program baseline by conducting the following activities:

- Determine the human factors cost, benefit, schedule, and performance baselines for each candidate solution
- Identify the human factors and human performance measures and thresholds to be achieved (e.g., for the equipment, software, environment, support concepts, and configurations expected for the solution)
- Determine the human factors activities to be undertaken during the program, the schedule for conducting them, their relative priority, and the expected costs to be incurred
- Calculate or estimate the relative or absolute benefits of the human factors component of each solution in terms of decision criteria (e.g., cost, schedule, human-system performance)

### **17.1.6 Major Management Actions**

Human factors professionals can assist in applying human factors information related to human resources management, training, safety, health hazards, and human engineering. The human factors process consists of four management actions:

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

- Manage the human factors program
- Establish human factors requirements
- Conduct human factors integration
- Conduct human factors test and evaluation

## 17.2 Managing the Human Factors Program

The Human Factors Program establishes the approach for applying human factors engineering to the system being acquired to increase total system performance and reduce developmental and lifecycle costs (especially in the areas of staffing, personnel, operations and training). The Human Factors Program focuses on the human performance produced when the system is operated and maintained in an operational environment by members of the intended target population.

Establishing a Human Factors Program for a given program or project requires focusing on the tasks the humans (operators, maintainers, and support personnel) will perform on the system, and the program activities that must be undertaken to allow early identification and resolution of human performance issues. Figure 17-1 illustrates the steps to be taken in developing the Human Factors Program.

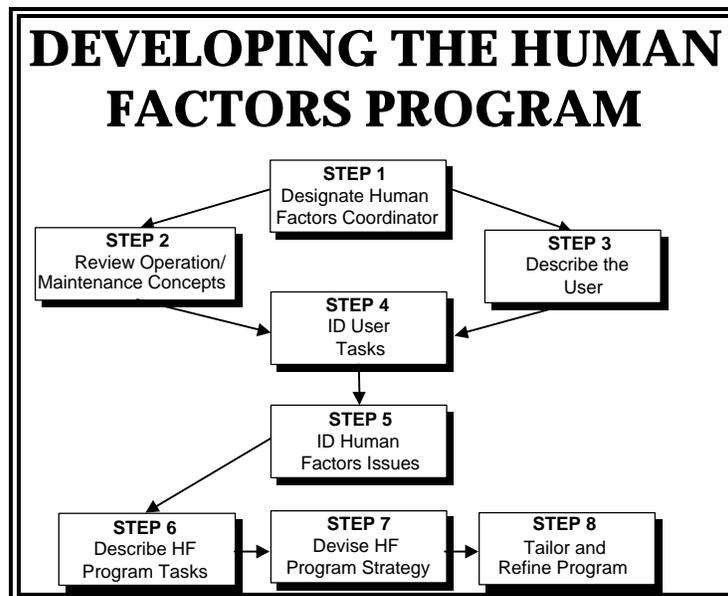


Figure 17-1: Steps in developing a Human Factors Program

Because each project or program is unique in its pace, cost, size, complexity, and human interfaces, the Human Factors Program should be tailored to meet program demands. As the system progresses through the lifecycle phases of the acquisition process, changes will occur. The Human Factors

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

Program must be structured and maintained to change iteratively with the project. To aid in the management of the Human Factors Program, a Human Factors Working Group may be established.

There is a strong link between the program documentation and the planning, management, and execution of the program. The documentation that supports a program defines the performance requirements and capabilities the program is to meet, the approach to be taken, and the specific tasks and activities that must be performed during design, development, and implementation of the program. Similarly, the human factors inputs to the program documentation accomplish the same result regarding the Human Factors Program. Human factors inputs define human performance requirements and criteria, identify human performance and resource trade-offs, specify human performance thresholds, establish an approach to ensure human performance supports project performance, and define the specific tasks and activities to be conducted.

Without such input, the capabilities and limitations of the designated operators and maintainers will not adequately influence the design, and may result in lower levels of operational suitability, effectiveness, and safety.

### **17.3 Establish Human Factors Requirements**

For human performance and safety considerations to effectively influence the design, project specifications must accommodate the following essential ingredients for all users:

- Staffing constraints
- System operator and maintainer (user) skills
- Training time available and cost limitations for formal, informal, and on-the-job skill development
- Acceptable levels of human and system performance when operated and maintained by members of the target population

Human-system performance considerations are embedded into the project by incorporating human factors requirements in project specifications. The formulation of draft human performance requirements is initiated during the early project phases and continues through implementation of the project.

By identifying and defining human resource and human performance considerations, inputs are provided to the development of project concepts for functional allocation, hardware and software, operations and training, and organizational structure. Through the process of assessing these concepts and the related human resource and human performance trade-offs of various alternatives, the project concepts (e.g., for requirements, design, and implementation) iteratively evolve. This process applies equally to various kinds of projects and program (including developmental, NDI, or COTS acquisitions). The purpose of this process is to place these essential ingredients into the project specifications so that human performance capabilities and limitations will be incorporated in the project in a binding manner.

#### **17.3.1 Project Specifications**

From a human performance perspective, the project specification will have the most significant impact on system design and safety. It states the technical and mission performance requirements for a system as an entity, allocates requirements to functional areas, documents design constraints, and defines the interfaces between or among the functional areas. To achieve the design objective in a manner that

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

results in a safe, efficient, usable system for the lowest possible expenditure of resources, the human performance constraints and requirements need to be placed into the system specification.

### **17.3.2 Generate Human Factors Requirements in a Statement of Work**

In simple terms, the Statement of Work (SOW) identifies the work the sponsor wants the contractor to perform, the CDRL specifies the data to be provided to the sponsor for a specific contract, and the DID specifies the format and content of the data to be submitted to the Sponsor. The objective of the human factors effort is to integrate all elements of the project involving human performance and safety, and to influence project design so as to optimize total system effectiveness. The objective of this human factors task is to translate these human performance design and integration activities to the contractor as clear, unambiguous requirements in a contractually binding way. Human factors contractual requirements, through the SOW, CDRLs, and DIDs, are the critical elements to achieve design and development conformance.

A good SOW starts with an understanding of what the sponsor wants the contractor to do. The starting point for determining human factors requirements for inclusion in the SOW is a review of human factors requirements in the early project documentation (such as requirements documents, program baselines, and program plans) to identify human factors issues that must be resolved, and tasks and analyses that must be conducted by the contractor to ensure that human performance goals are met.

Essential human factors elements that must be addressed by the requirements in the SOW include:

- Limits to the skill level and characteristics of operator, maintainer, and support personnel
- Maximum acceptable training burden
- Minimum acceptable performance of critical tasks
- Acceptable staffing limits
- System safety and health hazards

The contractor's response to these requirements will result in a comprehensive human factors program for the system that defines the management and technical aspects of the effort. The response should also address the scheduling of key events and their timing in relation to other system engineering activities. The contractor's program must demonstrate how it effectively integrates human factors with their design and development process.

The scope and level of effort to be applied to the various human factors tasks and activities must be tailored to suit the type of system being acquired and the phase of development. The SOW should describe the specific task or activity required and the associated data deliverable. Human factors reviews and demonstrations should be planned and conducted to coordinate and verify that requirements are being met. The contractor should convincingly indicate how human performance data would influence system lifecycle design and support.

### **17.3.3 Human Factors in Data Item Descriptions**

A Data Item Description (DID) describes the format and content of the data that is to be provided to the Sponsor as required by the SOW and CRDL. The DID should be tailored to require only those

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

items that are pertinent to the project being acquired, and what is necessary to allow the human factors engineer sufficient information to assess the quality and suitability of the contractor's human factors effort. The Human Factors Coordinator should prepare a list of human factors-related DIDs applicable to the project being acquired and provide them for inclusion in the SOW.

#### **17.3.4 Human Factors in Contract Data Requirements Lists**

The purpose of the CDRL is to describe all of the items that are required to be delivered under the terms of the contract. The Human Factors Coordinator should review the CDRL to ensure the proper timing of submission of the data and that the appropriate distribution is indicated. The Human Factors Coordinator should recommend approval or rejection of the delivered product.

#### **17.3.5 Human Factors in Source Selections**

Human factors criteria must be developed to support source selections conducted in any phase. Since it is difficult to enforce compliance after a contract is awarded if vendor capabilities are inadequate, offerors must demonstrate the ability to incorporate human factors design criteria and guidelines into their system design and engineering before contract award. The Sponsor incorporates human factors requirements in the Screening Information Request (SIR), which includes appropriate weighting in the proposal evaluation criteria. Offerors show they understand the requirements by making human factors commitments in their proposals. The offerors must demonstrate comprehension of and the ability to comply with the total system performance concept as well as their ability to integrate human considerations into system design and development. The human factors practitioner, having provided input to the source selection plan, helps determine how well offerors have met the human factors selection criteria. Representation of human factors expertise on source selection team or panel(s) will provide the capability to adequately assess the human factors aspects of proposals.

### **17.4 Conduct human factors integration**

The integration function (such as in system engineering activities) is the translation of operational requirements into design, development, and implementation of concepts and requirements. The Human Factors Coordinator assists the sponsor's and contractor's system engineering effort by integrating human factors within the project development and management process. Identifying the human performance and safety boundaries, risks, trade-offs, and opportunities of the system engineering options and alternatives does this. A human engineering effort (which may directly affect safety) is conducted to:

- Develop or improve human interfaces of the system,
- Achieve required effectiveness of human performance during system operation, maintenance, and support, and
- Make economical demands upon personnel resources, skills, training, and costs.

System engineering is an interdisciplinary approach to evolve and verify an integrated and lifecycle-balanced set of system product and process solutions that satisfy customer needs. The Human Factors Coordinator assists in the system engineering task by contributing information related to design enhancements, safety features, automation impacts, human-system performance trade-offs, ease of use, and workload. The Human Factors Coordinator also assists in identifying potential task overloading or skill creep for system operators and maintainers. Where user teams or operator juries and repre-

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

representatives participate in achieving an operational viewpoint to design, the human factors engineer complements the effort to ensure performance data represents more than individual preferences. Optimally, the Human Factors Coordinator participates fully in system engineering design decisions.

While the actual design and development work may be completed by either the sponsor or the contractor, the Human Factors Coordinator (in conjunction with the Human Factors Working Group) provides close, continuous direction throughout the process. To accomplish this, the Human Factors Coordinator reviews all documentation for human performance impacts that will affect total system performance and exercises his or her responsibility by participating in technical meetings and system engineering design reviews.

The human engineer actively participates in four major interrelated areas of system engineering:

- Planning
- Analysis
- Design and Development
- Test and Evaluation

#### **17.4.1 Human Engineering in Planning**

Human engineering planning is performed to ensure effective and efficient support of the system engineering effort for human performance and human resource considerations. Human engineering program planning includes the human factors tasks to be performed, human engineering milestones, level of effort, methods to be used, design concepts to be utilized, and the test and evaluation program, in terms of an integrated effort within the total project.

The human engineering planning effort specifies the documentation requirements and assists in the coordination with other program activities. Sponsor and contractor documentation provides traceability from initially identifying human engineering requirements during analysis and/or system engineering, through implementing such requirements during design and development, to verifying that these requirements have been met during test and evaluation. The efforts performed to fulfill the human engineering requirements must be coordinated with, but not duplicate, efforts performed by other system engineering functions.

#### **17.4.2 Human Engineering in System Analysis**

To support system analysis, the functions that must be performed by the system in achieving its objective(s) within specified mission environments are analyzed for their human factors implications and alternatives. Human engineering principles and criteria are applied to specify human-system performance requirements for system operation, maintenance and support functions and to allocate system functions to automated operation and maintenance, manual operation and maintenance, or some combination thereof. Essential activities related to system analysis include: functional analysis, functional allocation, design configuration, and task analysis.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

### **17.4.3 Human Engineering in Detail Design**

During detail design, the human engineering requirements are converted into detail engineering design features. Design of the equipment should satisfy human-system performance requirements and meet the applicable human engineering design criteria. The human factors engineer participates in design reviews and engineering change proposals for those items having a human interface. Essential products to be reviewed related to detail design include: hardware design and interfaces, tests and studies, drawings and representations, environmental conditions, procedures, software, technical documentation.

### **17.4.4 Human Engineering in Test and Evaluation**

The Sponsor and contractor establish and conduct a test and evaluation program that addresses human factors to:

- Ensure fulfillment of the applicable human performance and safety requirements;
- Demonstrate conformance of system, equipment, and facility design to human engineering design criteria;
- Confirm compliance with system performance and safety requirements where human performance is a system performance determinant;
- Secure quantitative measures of system and safety performance which are a function of the human interaction with equipment; and
- Determine whether undesirable design or procedural features have been introduced.

The fact that the above may occur at various stages in system development should not preclude a final human engineering verification of the complete system.

### **17.4.5 Human Engineering Coordination**

Coordinating the Human Factors and other activities (such as integrated logistics support activities) takes active and continuous communication. There are many opportunities to plan requirements, collect data, and share information, especially in the areas of maintenance staffing, training, training support, and personnel skills. Coordination will result in program cost savings or cost avoidance by eliminating redundancy and will strengthen the planning, analysis, design, and testing for both programs during all phases of the process.

### **17.5 Conduct Human Factors Test and Evaluation**

Testing is performed to assess the operational effectiveness, suitability, and safety of the products to meet system requirements. The purpose of human factors in project testing is to produce evidence of the degree to which the total system can be operated and maintained by members of the target population in an operational environment. If the total system exhibits performance deficiencies when operated or maintained by members of the target population, the testing should produce human factors causal information.

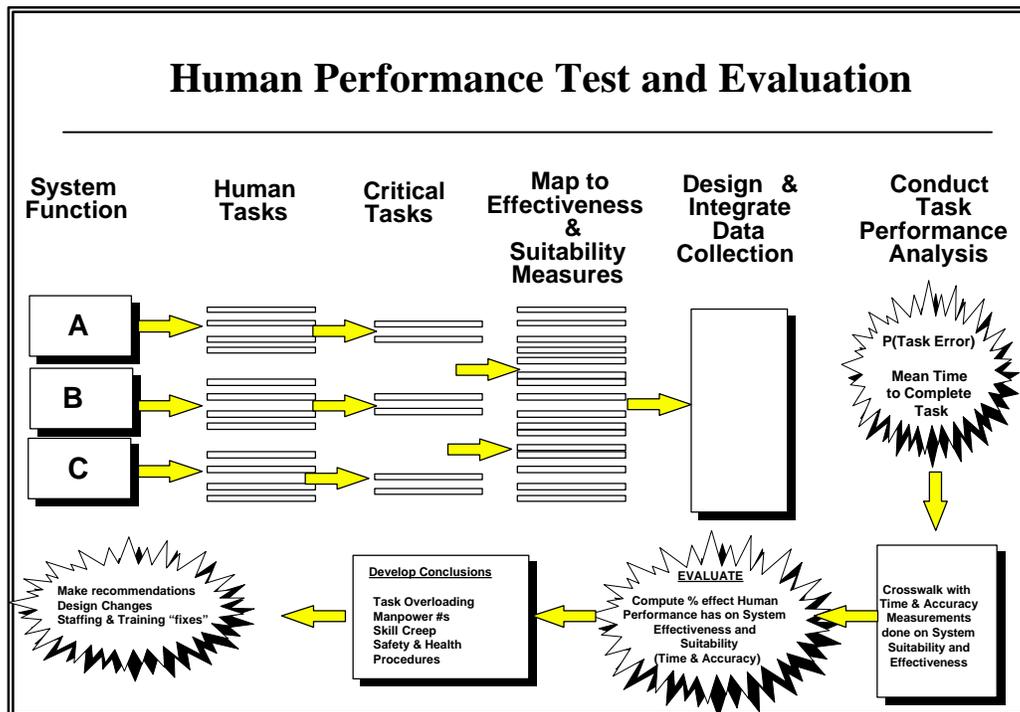
Human factors planning for test and evaluation (T&E) activities is initiated early in the project management process. Specific human factors-related T&E tasks and activities are subsequently

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

identified in the project/program planning documentation. The conduct of the human factors T&E is integrated with the system T&E program, which is largely performed during program implementation. Key principles for addressing human factors requirements in system testing are:

- Coordinate human factors test planning early in the program.
- Measure human performance of critical tasks during testing in terms of time, accuracy, and operational performance.
- Leverage human factors data collection by integrating efforts with system performance data collection.
- Make recommendations for human factors design and implementation changes and human performance improvements.

Providing human factors in system testing entails an early start and a continuous process. Figure 17-2 illustrates the flow of this process.



**Figure 17-2: Process for providing human factors in system testing**

Human engineering testing is incorporated into the project test and evaluation program and is integrated into engineering design and development tests, demonstrations, acceptance tests, fielding and other implementation assessments. Compliance with human engineering requirements should be tested as early as possible. Human engineering findings from design reviews, mockup inspections, demonstrations, and other early engineering tests should be used in planning and conducting later tests. Human engineering test planning is directed toward verifying that the system can be operated, maintained, and supported by user personnel in its intended operational environment.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

Human engineering test planning should also consider data needed or to be provided by operational test and evaluation. Test planning includes methods of testing (e.g., use of checklists, data sheets, test participant descriptors, questionnaires, operating procedures, and test procedures), schedules, quantitative measures, test criteria and reporting processes. Human engineering portions of tests include:

- Performance of task or mission;
- Critical tasks;
- Representative samples of non-critical, scheduled and unscheduled maintenance tasks;
- Personnel who are representative of the range of the intended user populations;
- Proposed job aids, new equipment training programs; training equipment, and special support equipment;
- Collection of task performance data in actual operational environments;
- Identification of discrepancies between required and obtained task performance; and
- Criteria for acceptable performance.

Unfavorable outcomes occurring during test and evaluation are subjected to a human engineering review to differentiate between failures of the equipment alone, failures resulting from human-system incompatibilities and failures due to human error. Human-system incompatibilities and human errors occurring in the performance of critical tasks are analyzed to determine the reason for their occurrence and to propose corrective action(s).

## **17.6 Human Factors in System-to-System Interfaces**

While the scope of human factors considerations for the development of acquisition product is obviously broad and complex, the application of human factors for the integration of systems within the National Airspace System is exponentially more complicated. Even beyond the increased scope of human factors demonstrated by Figure 17-3, maintaining the coordination, communication, situational awareness, and common understanding in the dynamic and interactive NAS demands sophisticated approaches to the research and engineering of the human component of system-to-system interfaces.

For example, *'Free Flight'* as described by the RTCA Task Force 3, provides a concept that suggests placing more responsibility on flight crews to maintain safe separation from other aircraft in the NAS. This idea could potentially shift aircraft separation responsibility from controllers to flight crews creating a *'shared separation'* authority environment. The guiding principle of the Free Flight concept is to provide benefits to users and providers. Some of the benefits include improved safety through enhanced conflict detection and resolution capabilities, more flexibility to manage flight operations, greater predictability of the NAS, and better decision-making tools for air traffic controllers and pilots. The major benefit anticipated for users is greater freedom to choose efficient routes and altitudes, resulting in savings on fuel and operating costs. To exercise these benefits, there may be a need to supply traffic information to flight crews, and develop operating methods and tools for both the air and ground to assure safety. While there have been studies done on new tools developed to display traffic

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

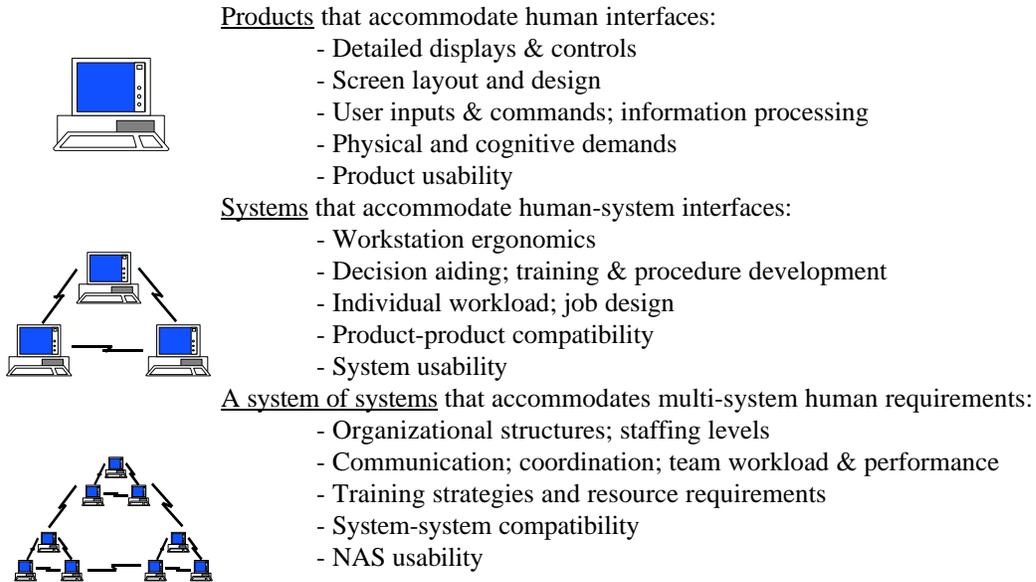
information in the cockpit (with its conflict alerting logic) and to support in controller decisions, investigating how the tools might (safely) work together in a shared separation environment requires considerable exploration and analysis.

An experiment intended to provide an examination of the effect of shared separation authority on flight operations when both air and ground have enhanced traffic and conflict alerting systems would necessarily emphasize identifying and evaluating the human factors impact. Such an evaluation would require detailed knowledge about how safety, human-system integration, and system-to-system performance are affected in the following broad areas:

- How automation should be used and how it should not be used
- How to balance the benefits of automation with the requirement for human authority and responsibility
- What information and feedback operators need to stay aware, in control, and able to intervene into the new or automated process
- Which are the best methods for selecting, training, and evaluating operators and teams in the context of the advanced systems and the changing environment
- What policies and procedures will ensure the appropriate use of the new automation and effective human performance and team coordination
- What formats and interfaces will best support the operator and team performance
- How to ensure the operators of the interacting systems maintain coordination with each other to maintain and enhance safety and efficiency during all operational activities
- What procedures are necessary to ensure that the appropriate information is applied during all stages of the development of the new automation applications and operations
- How physiological, psychological, and cultural factors such as fatigue, duty cycles, and concepts of authority affect operator performance, and what standards and measures need to be applied to ensure safety and efficiency
- What methods, materials, and configurations to apply to the new systems and operations that will reduce risks and ensure safety and efficiency during normal, abnormal, and emergency situations.

Many compromises in safety that lead to errors, accidents, or incidents can be attributed to unforeseen effects of how new technologies, new operational procedures, and changing organizations affect the human-system and system-to-system interface. Only through the rigorous exploration of these inter-relationships, can the safety of the NAS be ensured.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000



**Figure 17-3: The complexity of human factors increases in system-to-system interfaces**

## 17.7 Human Factors Engineering and Safety Guidelines

Human factors integration in the development and management of a project is a complex one because of the scope of the human factors considerations, the pervasiveness of human performance issues, and the difficulty in quantifying performance parameters especially early in the process. However, if given the proper resources and discipline, the process has proven to be successful in lowering lifecycle costs, improving overall system safety and performance, and reducing program technical risks. The human factors engineering process encompasses efforts related to the design, development, manufacturing, verification, deployment, operations, support, and disposal of system products and processes. Overarching principles include those that adhere to the summary guidelines and principles of Table 17-2. Some key human factors references that may be useful to the practitioner are listed in Table 17-3.

FAA System Safety Handbook, Chapter 17: Human Factors Principles & Practices  
August 2, 2000

**Table 17-2: Overarching Human Factors Guidelines/Principles**

<u>Overarching Human Factors Principles</u>
<b>1. Honor The User</b> (The user defines requirements – but only in a structured, data-driven way.)
<b>2. To Err Is Human</b> (People are not machines; machines are not perfect; design the interface to tolerate errors of both.)
<b>3. Human Factors Is Not Free</b> (Plan the resources for human factors program support.)
<b>4. Human Factors Requires Experts</b> (The application of human factors engineering is neither easy, nor common sense -- except in retrospect of an incident or accident or poor design; co-locate human factors resources near the project/program teams they serve.)
<b>5. People Are the Same; Individuals Are Different</b> (Design for people sameness & tolerance of measured differences, especially in their skill and performance.)
<b>6. Early Operator and Maintainer Decisions Drive Safety and Lifecycle Support Costs</b> (Identify early in the program development process a requirement to subject every product to an "Out-of-Box" human factors study.)
<b>7. Operator and Maintainer Skill Is a Function of Aptitude and Training</b> (Training is part of the system engineering and safety performance package.)
<b>8. Performance Is Measured in Terms of Time and Accuracy</b> (Performance is a matter of degree -- quantitatively and qualitatively determined; test for human performance early and often.)
<b>9. Task Safety &amp; Performance Are Determined by the Design</b> (Designs can improve or detract from task safety and performance.)
<b>10. Operator and Maintainer Performance Affect System Performance</b> (How people use the system IS the measure of the system's capabilities and risks.)

**Table 17-3: Key Human Factors References**

• FAA Order 9550.8, Human Factors Policy (October 1993)
• FAA Human Factors Design Guide (January 1996)
• MIL-STD-1472F, DOD Design Criteria Standard: Human Engineering (23 August 1999)
• MIL-HDBK-759, Human Engineering Design Guidelines (February 1997)
• MIL-HDBK-46855A, Human Engineering Guidelines for Military Systems, Equipment, and Facilities (17 May 1999)
• Cardosi, K. M., & Murphy, E. D. (Eds.). (1996). <u>Human Factors in the Design and Evaluation of ATC Systems: A Handbook for FAA User Teams</u> . Washington, DC: USDOT/FAA.
• Federal Aviation Administration. (1995). <u>The National Plan for Civil Aviation Human Factors</u> . Washington, DC: Federal Aviation Administration.
• National Research Council (1997). <u>Flight to the Future: Human Factors in Air Traffic Control</u> . Washington, DC: National Academy Press.
• National Research Council (1998). <u>The Future of Air Traffic Control: Human Operators and Automation</u> . Washington, DC: National Academy Press.

FAA System Safety Handbook, Appendix A: Glossary  
December 30, 2000

# **Appendix A**

## **Glossary**

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Acceptable Risk</b>	The residual (final) risk remaining after application of controls, i.e. Hazard Controls / Risk Controls, have been applied to the associated Contributory Hazards; that have been identified and communicated to management for acceptance.
<b>Accident</b>	<p>An unplanned fortuitous event that results in harm, i.e. loss, fatality, injury, system loss; also see Risk Severity. The specific type and level of harm must be defined; the worst case severity that can be expected as the result of the specific event under study. Various contributory hazards can result in a single accident; also see Contributory Hazard, Cause, Root Cause, and Initiating Events.</p> <p><u>Accident.</u> An unplanned event that results in a harmful outcome; e.g. death, injury, occupational illness, or major damage to or loss of property.</p> <p><u>Accident.</u> An unplanned event or series of events resulting in:</p> <p>Death. Injury. Occupational illness. Damage to or loss of equipment or property. Damage to the environment.</p>
<b>Accreditation</b>	A formal declaration by the Accreditation Authority that a system is approved to operate in a particular manner using a prescribed set of safeguards.
<b>Act</b>	A formal decision or law passed by a legislative body.
<b>Administrative Hazard Control</b>	Administrative controls to eliminate or reduce safety related risk, i.e. training, programs, procedures, warnings, instruction, tasks, plans; also see Risk Control.
<b>Anomalous Behavior</b>	Behavior which is not in accordance with the documented requirements
<b>Architecture</b>	The organizational structure of a system, identifying its components, their interfaces and a concept of execution between them.
<b>Assumed Risk</b>	The residual risk associated with a specific hazardous event or primary hazard, which has been accepted by management.
<b>Audit</b>	An independent examination of the life cycle processes and their products for compliance, accuracy, completeness and traceability.
<b>Audit Trail</b>	The creation of a chronological record of system activities (audit trail) that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or an event in a transaction from its inception to its final results.
<b>Authenticate</b>	<p>(1) To verify the identity of a user, device, (or other entity in a system, often as a prerequisite to allowing access to resources in the system.</p> <p>(2) To verify the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized modification.</p>
<b>Barrier</b>	A material object or set of objects that separates, Demarcates, or services as a barricade; or

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	something immaterial that impedes or separates. Both physical and non-physical barriers are utilized and applied in hazard control; i.e. anything used to control, prevent or impede unwanted adverse energy flow and / or anything used to control, prevent or impede unwanted event flow.
<b>Baseline</b>	The approved, documented configuration of a software or hardware configuration item, that thereafter serves the basis for further development and that can be changed only through change control procedures.
<b>Cause</b>	Something that brings about an event; a person or thing that is the occasion of an action or state; a reason for an action or condition.
<b>Certification</b>	<p>Legal recognition by the certification authority that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of checking the product, service, organization or person and the formal recognition of compliance with the applicable requirements by issue of certificate, license, approval or other document as required by national law or procedures. In particular, certification of a product involves:</p> <p>(a) the process of assuring the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety, (acceptable risk);</p> <p>(b) the process of assessing an individual product to ensure that it conforms to the certified type design;</p> <p>(c) the issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with item (a).</p>
<b>Certification Authority</b>	The organization or person responsible within the state (country) concerned with the certification of compliance with applicable requirements.
<b>Class(es)</b>	Parameters of risk are classified in order to conduct analysis, evaluations, reviews, presentations, etc.; i.e. generic contributory hazards, generic risks, generic events.
<b>Code</b>	A collection of laws, standards, or criteria relating to a particular subject.
<b>Component</b>	A combination of parts, devices, and structures, usually self-contained, which performs a distinctive function in the operation of the overall equipment.
<b>Configuration</b>	The requirements, design and implementation that define a particular version of a system or system component.
<b>Configuration Control</b>	The process of evaluating, approving or disapproving, and coordinating changes to configuration items after formal establishment of their configuration identification.
<b>Configuration Item</b>	A collection of hardware or software elements treated as a unit for the purpose of configuration management.
<b>Configuration Management</b>	The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items.
<b>Contributory</b>	The potential for harm. An unsafe act and / or unsafe condition which contributes to the

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Hazard</b>	accident, (see cause, root cause, contributory events, initiator; the potential for adverse energy flow to result in an accident.) A hazard is not an accident. A failure or a malfunction can result in an unsafe condition, and / or unsafe act. Human error can result in an unsafe act. Contributory Hazards define the contributory events that lead to the final outcome. For simplicity, Contributory Hazards can also include Initiating Events and Primary Hazards. Sequential logic defining the Hazardous Event should remain consistent throughout the hazard analysis process.
<b>Consequence</b>	See Risk Severity.
<b>Control</b>	See Risk Control
<b>Criticality</b>	Reliability term. The degree of impact that a malfunction has on the operation of a system.
<b>Critical Path</b>	Defines the sequence of events that control the amount of time needed to complete the effort described within the PERT (Program Evaluation Review Technique) network.
<b>Danger</b>	Danger expresses a relative exposure to a hazard. A hazard may be present, but there may be little danger because of the precautions taken.
<b>Damage</b>	Damage is the severity of injury, and / or the physical, and/ or functional, and /or monetary loss that could result if hazard control is less than adequate.
<b>Debug</b>	The process of locating and eliminating errors that have been shown, directly or by inference, to exist in software.
<b>Deductive Analysis</b>	A top down approach of analysis logic: "What can cause a specific event to occur?"
<b>Derived Requirements</b>	Essential, necessary or desired attributes not explicitly documented, but logically implied by the documented requirements.
<b>Development Configuration</b>	The requirements, design and implementation that define a particular version of a system or system component.
<b>Design Handbooks, Guides and Manuals</b>	Contain non-mandatory general rules, concepts, and examples of good and best practices to assist a designer or operator.
<b>Emulator</b>	A combination of computer program and hardware that mimic the instruction and execution of another computer or system.
<b>Engineering Controls</b>	Engineering design controls to eliminate or reduce safety related risks; also Hazard Control and Risk Control.
<b>Entity Item</b>	That which can be individually described and considered. May be an activity, process, product, organization, system, person or any combination thereof.
<b>Environment</b>	(a) The aggregate of operational and ambient conditions to include the external procedures, conditions, and objects that affect the development, operation, and maintenance of a system. Operational conditions include traffic density, communication density, workload, etc. Ambient conditions include weather, emi, vibration, acoustics, etc.  (b) Everything external to a system which can affect or be affected by the system.
	An act that through ignorance, deficiency, or accident departs from or fails to achieve what

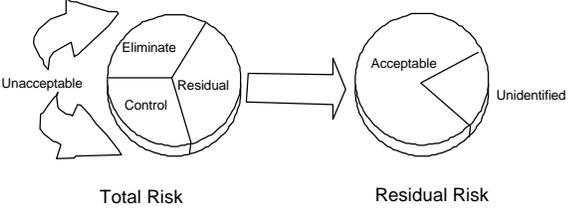
<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Error</b>	should be done. Errors can be predictable and random. Errors can also be categorized as primary or contributory. Primary errors are those committed by personnel immediately and directly involved with the accident. Contributory errors result from actions on the part of personnel whose duties preceded and affected the situation during which the results of the error became apparent. The difference between a computed, observed, or measured value or condition and true, specified, or theoretically correct value or condition. A mistake in engineering, requirement specification, or design, implementation, or operation which could result in a failure, and /or contributory hazard. There are four types of Human Errors: 1) Omission 2) Commission 3) Sequence 4) Timing
<b>Explosion Proof</b>	The item is designed to withstand an internal explosion; designed to vent explosive bases below ignition temperature.
<b>Fail-Operational</b>	A characteristic design which permit continued operation in spite of the occurrence of a discrete malfunction.
<b>Fail-safe</b>	A characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters.
<b>Fail-Soft</b>	Pertaining to a system that continues to provide partial operational capability in the event of a certain malfunction.
<b>Failure</b>	Reliability term. The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration. A failure may result in an unsafe condition and / or act, i.e. a hazard; the termination of the ability of a system element to perform a required function; the lack of correct performance. Failures and hazards are not interchangeable.
<b>Firmware</b>	The combination of a hardware device and computer instructions and data that reside as read-only software on that device.
<b>Formal Verification</b>	The process of evaluating the products of a given phase using formal mathematical proofs to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
<b>Formal Qualification Review</b>	Formal evaluation by top management of the status and adequacy of the quality system in relation to quality policy and objectives.
<b>Formal Qualification</b>	The process that allows the determination of whether a configuration item complies with the requirements allocated to it.
<b>Hazard</b>	<p>The potential for harm; also see Contributory Hazard, Primary Hazard. A hazard is not an accident. Per FAA Order 8040.4 a " Condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event."</p> <p><u>Hazard or hazardous condition.</u> Anything, real or potential, that could make possible, or contribute to making possible, an accident.</p> <p><u>Hazard.</u> A condition that is prerequisite to an accident.</p>
<b>Hazardous</b>	An accident; also see Accident. It should be noted that a Hazardous Event is not being defined

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Event</b>	<p>an occurrence that creates a hazard. This logic indicates that a Hazardous Event is an occurrence that creates the potential for harm; Initiating Event, or Root Cause, are more appropriate terms.</p> <p>The Hazardous Event (now) defines the total sequence of events from the Initiating Event to the final outcome, the harm, the Initiating Event, Contributory Hazards, Primary Hazard, and Risk Severity.</p> <p>The Hazardous Event under study is considered open or closed depending Report Status on the status of Hazard Control.</p> <p>The Hazardous Event under study is considered open; the corrective action Report Status evaluation and verification is in process. The status will remain open until (Open) management has reviewed the actions taken and accepted the associated risk. All related Contributory Hazards are to be evaluated.</p> <p>The hazardous Event under study is considered closed; the corrective Report Status action evaluation and verification is completed, and management has (Closed) reviewed the actions taken and has accepted the associated risk.</p>
<b>Hazard Probability</b>	<p>Hazard Probability defines in quantitative or qualitative terms, the estimated probability of the specific Contributory Hazards which are defined within the Hazardous Event under study; possible elements within a fault tree.</p> <p>Note that hazard probability is not defined as the aggregate probability of occurrence of the individual hazardous events that create a specific hazard; see Hazardous Event and Accident. Also note that Hazard Probability is not the same as likelihood; see likelihood.</p> <p><u>Hazard Probability</u>. The aggregate probability of occurrence of the individual events (conditions).</p> <p><u>Hazard Severity</u>. An assessment of the consequences of the worst credible accident that could be caused by a specific hazard.</p>
<b>Hazard Tracking and Resolution.</b>	A tracking log is maintained for closeout. Risk Tracking and Risk Resolution should be conducted throughout the system life cycle. Risk/Hazard Controls are to be formally verified.
<b>Inadvertent Operation</b>	Unintentional operation.
<b>Independent Verification &amp; Validation (IV&amp;V)</b>	Confirmation by independent examination and provision of objective evidence that specified requirements have been fulfilled, and that the particular requirements for a specific intended use are fulfilled.
<b>Inductive</b>	A bottom-up analysis approach of analysis logic: "What happens if a specific failure occurs?"

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Analysis</b>	
<b>Incident</b>	<p>A near miss accident with minor consequences that could have resulted in greater loss.</p> <p>An unplanned event that could have resulted in an accident, or did result in minor damage, and which indicates the existence of, though may not define, a hazard or hazardous condition. Sometimes called a mishap.</p>
<b>Initiating Events</b>	Initiating Events; initiator; the contributory hazard; unsafe act and / or unsafe condition that initiated the adverse event flow, which resulted in the hazardous event under evaluation; also see Root Cause.
<b>Intrinsically Safe Design</b>	Designers determine which hazards could be present, the level of associated risk that could constitute danger, and the controls to assure acceptable risk. Nothing is perfectly safe; see safe.
<b>Inspection</b>	A static technique that relies on visual examination of development products to detect deviations, violations or other problems.
<b>Latent</b>	Present and capable of becoming though not now visible or active.
<b>Likelihood</b>	<p>Likelihood defines in quantitative or qualitative terms, the estimated probability of the specific Hazardous event under study. Likelihood is one element of associated risk. Fault Trees and other models can be constructed and individual Hazard Probabilities are estimated, and likelihood can be calculated via Boolean Logic. It should be noted that estimated likelihood defined in conventional hazard analysis may be appropriate due to the variability, conference, resources, and other factors.</p> <p>See chapter 3 for specific definitions of likelihood.</p>
<b>Malfunction</b>	Fail to operate in the normal or usual manner. Any anomaly which results in system deviation.
<b>Maintainability</b>	The ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures, resources and equipment at each prescribed level of maintenance and repair.
<b>Managing Activity</b>	FAA organization assigned acquisition management responsibility for the system, facility, or prime or associated contractors or subcontractors who wish to impose system safety tasks on their suppliers.
<b>Methodology</b>	A particular procedure or set of procedures.
<b>Mishap</b>	<p>A source of irritation, annoyance, grievance, nuisance, vexation, mortification. Note that mishap is not a synonym for accident. It is more appropriate to consider a mishap a minor accident.</p> <p>A hazard. Note that the use of mishap is different within the FAA community than as used in MIL-STD-882C. The latter equates mishap to an accident.</p>
<b>N-Version Software</b>	Software developed and tested to fulfill a set of requirements where multiple versions of software are intentionally made independent and different. Differences can be in some or all of: specifications, design, use of language, algorithms, data structures, etc.
<b>Non-Developmental</b>	<p>Deliverable part not developed as a part of the developmental process being addressed.</p> <p>The developer, or some other party but provides software - deliverable software that is not</p>

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Item (NDI)</b>	developed under the contract. Non-developmental software may also be referred to as reusable software, government furnished software, commercially available software, or Commercial Off-The-Shelf (COTS) software.
<b>Non-Programmable (N-P) System</b>	A system based upon non-programmable hardware devices (i.e., a system not based on programmable electronics. NOTE: Examples would include hardwired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems, etc.
<b>Objective Evidence</b>	Information, which can be proved true, based on facts obtained through observation, measurement, test or other means.
<b>Optimum Safety</b>	The associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.
<b>Phase</b>	Defined segment of work. Note: a phase does not imply the use of any specific life-cycle model, nor does it imply a period of time in the development of a product.
<b>Practice</b>	Recommended methods, rules, and designs for voluntary compliance.
<b>Process</b>	Set of inter-related resources and activities, which transform inputs into outputs.
<b>Product Service History</b>	Historical data generated by activities at the interface between the supplier and the customer and by supplier internal activities to meet the customer needs regarding the quality, reliability and safety trends of the product or service.
<b>Product Liability</b>	Generic term used to describe the onus on a producer or others to make restitution for loss related to personal injury, property damage or other harm caused by a product.
<b>Proximate Cause</b>	The relationship between the plaintiff's injuries and the plaintiff's failure to exercise a legal duty, such as reasonable care.
<b>Primary Hazard</b>	A primary hazard is one that can directly and immediately results in: loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury, etc. The primary hazard is also referred to as: catastrophe, catastrophic event, critical event, marginal event, and negligible event.
<b>Quality Assurance</b>	A planned and systematic pattern of actions necessary to provide adequate confidence that an item or product conforms to established requirements.
<b>Quality Audit</b>	Systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives.
<b>Quality Evaluation</b>	Systematic examination of the extent to which an entity is capable of fulfilling specified requirements.
<b>Qualification Process</b>	Process of demonstrating whether an entity is capable of fulfilling specified requirements.
<b>Quantitative Assessment.</b>	In any discussion of mishap risk management and risk assessment, the question of quantified acceptability parameters arises. Care should be exercised, under such conditions not to forget the limitations of a mathematical approach. In any high-risk system, there is a strong temptation to rely totally on statistical probability because, on the surface, it looks like a convenient way to measure safety "who can argue with numbers"? To do so, however, requires that the limitations and principles of this approach are well understood and that past engineering experience is not ignored. Quantitative acceptability parameters must be well

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p>defined, predictable, demonstrable, and above all, useful. They must be useful in the sense that they can be easily related to the design and the associate decision criteria. More detail may be found in chapter 7 on the limitations of the use of probabilities.</p> <p>Many factors fundamental to system safety are not quantifiable. Design deficiencies are not easily examined from a statistical standpoint. Additionally, the danger exists that system safety analysts and managers will become so enamored with the statistics that simpler and more meaningful engineering processes are ignored. Quantification of certain specific failure modes, which depend on one of two system components, can be effective to bolster the decision to accept or correct it.</p> <p>General risk management principles are:</p> <ol style="list-style-type: none"> <li>a. All human activity involving a technical device or process entails some element of risk.</li> <li>b. Most hazards (safety risks) can be neutralized or controlled.</li> <li>c. Hazards should be kept in proper perspective. Weighing the risk does this by knowledge gained through analysis and experience against program need.</li> <li>d. System operations represent a gamble to some degree; good analysis assists the MA in controlling the risk.</li> <li>e. System safety analysis and risk assessment does not eliminate the need for good engineering judgment.</li> <li>f. It is more important to establish clear objectives and parameters for risk assessment than to find a cookbook approach and procedure.</li> <li>g. There is no "best solution" to a safety problem. There are a variety of directions to go. Each of these directions may produce some degree of risk reduction.</li> </ol>
<b>Redundancy</b>	The existence in a system of more than one means of accomplishing a given function.
<b>Reliability</b>	The ability of a system to perform its required functions under stated conditions for a specified period of time. A reliable system is no total assurance of acceptable risk.
<b>Requirements</b>	Statements describing essential, necessary or desired attributes.
<b>Requirements Specification</b>	Specification that sets forth the requirements for a system or system component.
<b>Risk</b>	Risk is an expression of possible loss over a specific period of time or number of operational cycles. It may be indicated by the probability of an accident times the damage in dollars, lives,

CONCEPT or TERM	DESCRIPTION
	<p>and / or operating units.</p> <p>Hazard Probability and Severity are measurable and, when combined, give us risk.</p> <p><u>Total risk</u> is the sum of identified and unidentified risks.</p> <p><u>Identified risk</u> is that risk which has been determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks. This step precedes determine the significance of the risk (severity) and the likelihood of its occurrence (hazard probability). The time and costs of analysis efforts, the quality of the safety program, and the state of technology impact the number of risks identified.</p> <p><u>Unidentified risk</u> is the risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.</p> <p><u>Unacceptable risk</u> is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.</p> <p><u>Acceptable risk</u> is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.</p> <p><u>Residual risk</u> is the risk left over after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk. Residual risk is the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.</p>  <p>The diagram shows two circles. The left circle, labeled 'Total Risk', is divided into three segments: 'Unacceptable' (top-left), 'Residual' (top-right), and 'Control' (bottom). An arrow points from the 'Unacceptable' segment to the 'Residual' segment. The right circle, labeled 'Residual Risk', is divided into two segments: 'Acceptable' (top) and 'Unidentified' (bottom). An arrow points from the 'Residual' segment of the 'Total Risk' circle to the 'Residual Risk' circle.</p>
<b>Risk Analysis</b>	The development of qualitative and / or quantitative estimate of risk based on evaluation and mathematical techniques.
<b>Risk Acceptance.</b>	<p>Accepting risk is a function of both risk assessment and risk management. Risk acceptance is not a simple matter and the concept is difficult for some to accept. Several points must be kept in mind.</p> <p>(1) Risk is a fundamental reality.</p>

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p>(2) Risk management is a process of tradeoffs.</p> <p>(3) Quantifying risk doesn't ensure safety.</p> <p>(4) Risk is a matter of perspective.</p> <p>On the surface, taking risks seems foolish and to be avoided. Everything we do, however, involves risk. Defining acceptable risk is subjective and perceived risks are often as important as actual risks. Risks imposed on us by others are generally considered to be less unacceptable than those inherent in nature. There are dangers in every type of travel, but there are dangers in staying home--40 percent of all fatal accidents occur there. There are dangers in eating most food caused by pesticides, preservatives, natural fats, or just eating more than necessary. There are breathing related dangers in industrial and urban areas. The results of air pollution leads to the death of at least 10,000 Americans each year; inhaling natural radioactivity is believed to kill a similar number; and many diseases are contracted by inhaling germs. 12,000 Americans are killed each year in job related accidents, and probably 10 times that number die from job related illness. There are dangers in exercising and dangers in not getting enough exercise. Risk is an unavoidable part of our everyday lives.</p> <p>We all accept risk, knowingly or unknowingly. In a FAA program, it is the ultimately the responsibility of the MA to determine how much and what kind is to be accepted and what is not. In the real world, making this decision is a trade-off process involving many inputs. As tradeoffs are being considered and the design progresses, it may become evident that some of the safety parameters are forcing higher program risk. From the program manager's perspective, a relaxation of one or more of the established parameters may appear to be advantageous when considering the broader perspective of cost and performance optimization. The program manager has the authority and responsibility, in some circumstances, to make a decision against the recommendation of his system safety manager. The system safety manager must recognize such management prerogatives.</p> <p>A prudent program manager must make a decision whether to fix the identified problem or formally document acceptance of the added risk. In some cases, this requires contract or system specification modification. When the program manager decides to accept the risk, the decision must be coordinated with all affected organizations and then documented so that in future years everyone will know and understand the elements of the decision and why it was made. It also provides necessary data if the decision must be revisited.</p>
<b>Risk Assessment</b>	The process by which the results of risk analysis are used to make decisions.
<b>Risk Control</b>	The Risk associated with the hazardous event under study is adequately controlled, by the reduction of severity and / or likelihood, via the application of engineering and/ or administrative hazard controls. Anything that mitigates or ameliorates the risk. See system

CONCEPT or TERM	DESCRIPTION
	safety design order of precedence in Chapter 3.
<b>Risk Hazard Index.</b>	<p>By combining the probability of occurrence with hazard severity, a matrix is created where intersecting rows and columns are defined by a Risk Hazard Index (RHI). The risk hazard index forms the basis for judging both the acceptability of a risk and the management level at which the decision of acceptability will be made. The index may also be used to prioritize resources to resolve risks due to hazards or to standardize hazard notification or response actions.</p> <p>Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative hazard risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition.</p>
<b>Risk Management</b>	The application of management methods for the identification, evaluation, elimination and control of all forms of risk. This effort is not confined only to safety-related risks. Risk Management comprised of two parts, Risk Control and Risk Finance. Risk Control considers all aspects in System Safety, Safety Management, and Safety Engineering. Risk Finance considers insurance, risk pooling, and self-insurance.
<b>Risk Perspectives.</b>	<p>There are three different perspectives in safety risk assessment:</p> <ol style="list-style-type: none"> <li>1. Standpoint of an <b>INDIVIDUAL</b> exposed to a hazard. An individual exposed to a hazard is primarily concerned with the questions: How large is the probability that I will be killed or injured in an accident? How much does my individual risk due to this hazard increase my normal fatality rate? <b>INDIVIDUAL RISK</b> is defined as the (usually annual) probability that an identified person will be killed or injured as a consequence of an accident.</li> <li>2. Standpoint of the <b>SOCIETY</b>. Besides being interested in guaranteeing minimum individual risk for each of its members, society is concerned about the total risk to the general public: How large are the total losses (e.g., per year) from a hazardous activity? The risk to society is called <b>COLLECTIVE RISK</b>. If expressed in terms of annual risks, it corresponds to the respective value shown in annual accident statistics.</li> <li>3. Standpoint of the <b>INSTITUTION RESPONSIBLE FOR THE ACTIVITY</b>. The institution responsible for an activity can be a private company or a government agency. From their point of view, it is not only essential to keep individual risks of employees or other persons and the collective risk at a minimum but also to avoid catastrophic and spectacular accidents. As experience clearly demonstrates (Bhopal, Seveso, Challenger, etc.), such catastrophic accidents damage the reputation, the image, and even the prosperity of the, institution responsible for the activity. Such risks are defined as <b>INSTITUTIONAL RISKS</b>.</li> </ol> <p>3.7 Residual <u>Risk</u>. To make important program decisions, the PM must know what residual risk exists in the system being acquired. When such risks are marginally acceptable or potentially unacceptable, the PM is required to raise the presence of residual risk to higher levels of authority such as the Service Director or Associate/Assistant Administrator for action</p>

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p>or acceptance. To present a cohesive description of the hazard to this higher level of decision making, all analyses performed and either the contractor or the FAA must document actions taken to control the hazard. In some contractual situations, the PM may apply additional resources or other remedies to help the contractor satisfactorily resolve the issue. If not, the PM can add his position to the contractor information and forward the matter to a higher decision level. A decision matrix very similar to a Risk Hazard Index called in this example a Risk Hazard Level index can be used to establish which decisions fall under the PM and which should be forwarded to a higher organizational level.</p>
<b>Risk Severity</b>	<p>The harm expected should the hazardous event occur, (i.e., loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury) considering the risk associated with the hazardous event under evaluation.</p> <p>See chapter three for specific definitions of severity. Severity ranges should be sized so that events within each category are of comparable severity. Equating the severity of event and conditions, which can cause one fatality with those, which can cause 100 or 1,000 does not make sense. The potential problems associated with sizing of the severity ranges grow as the size of the system grows. Program managers need to be provided with risk information that has the fidelity to distinguish the hazardous events that meet general criteria.</p> <p>Severity range thresholds for each severity category should be comparable when considering personal, system, or facility losses. For example, events or conditions that could cause the loss of an entire aircraft or facility would be categorized by MIL-STD-882 as catastrophic. Loss of a single crewman, mechanic, or passenger would also fall in the catastrophic category. Severe injuries, such as total loss of sight of a mechanic, and system damage of several million dollars are not normally considered to have equal value, even though both are in the critical category.</p> <p>If the RHI ranking criteria use risk as a function of severity and probability, quantitative scales or qualitative scales based on quantitative logic should be used. If the concept that the expected losses (or risk) associated with a hazardous event or condition may be estimated by multiplying the expected severity of the accident by the probability of the accident, then some sort of quantitative basis is necessary. Failure to provide a quantitative basis for the scales can cause significant confusion and dissipation of safety resources when an arbitrary risk ranking scale is used.</p> <p>Develop the severity values using order of magnitude ranges. There are several advantages to separating severity categories by orders of magnitude ranges: They include:</p> <ul style="list-style-type: none"> <li>Limiting the likelihood of misuse of the analysis.</li> <li>Avoiding meaningless hair-splitting arguments.</li> <li>Simplifying severity assessment during PHAs without impacting usefulness.</li> </ul>

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p>Quantify the threshold values for the probability ranges. Quantification reduces confusion associated with strictly qualitative definitions. Although it is impossible to quantify the ranges in 882(C) due to its extremely broad application, developing quantified probability ranges for specific systems is a relatively easy task to accomplish.</p> <p>The probability of occurrence should refer to the probability of an accident/consequence as opposed to the probability of an individual hazard/basic event occurring. The typical accident sequence is much more complicated than a single line of erect dominos where tipping the first domino (hazard) triggers a clearly predictable reaction.</p> <p>Develop the probability values using order of magnitude ranges.</p>
<b>Reaction Time</b>	Human response movement time plus response initiation time.
<b>Root Cause</b>	The contributory events, initiating events, which started the adverse event flow are considered root causes. Should these causes be eliminated the hazardous event would not have occurred. It should be noted that accidents are the result of many contributors, both unsafe acts and /or unsafe conditions; also see Contributory Hazards, Hazard.
<b>Safe</b>	<p>Freedom from all forms of harm. Nothing is safe. General term denoting an acceptable level of risk of, relative freedom from, and low probability of harm. The associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.</p> <p><u>Safety or Safe.</u> Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.</p> <p>Note that absolute safety is not possible because complete freedom from all hazardous conditions is not possible. Therefore, safety is a relative term that implies a level of risk that is both perceived and accepted. Thus the emphasis in SSPs as reflected in the definitions above is in managing risk. Chapter 3(FAA SS HB) describes the risk management process. "System" is also a relative term. A subsystem can be viewed as a system with more narrow predetermined boundaries than the system. System safety is not an absolute quantity either. System safety is an optimized level of risk that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated and the level of risk accepted or rejected by an authority. Finally, system safety is a discipline employed from the initial design steps through system disposal (also known as "cradle to grave or "womb to tomb").</p>
<b>Safety Analysis</b>	All associated analysis methods, process, and / or techniques to systematically evaluate safety related risks.
<b>Safety Risk Management Committee (SRMC)</b>	The principal reason to employ risk management and/or risk analysis is to improve decision-making. Risk analysis and risk management is at the heart of many FAA regulatory decisions. For example, risk analysis was performed to determine the hazards to flight from airborne wind shear. Risk management was also evident in the decision to require that all airliners be equipped with airborne wind shear detection. Risk management requires first analyzing risk in turn requiring access to sufficient credible data, and then developing policies and procedures to

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p>eliminate, mitigate, and/or manage them. In keeping with this process, an intra-agency team (the SRMC) was formed to examine the FAA's approach to risk management. The committee was and remains open to representatives of all FAA organizations interested in risk management.</p> <p>If the RHI ranking criteria use risk as a function of severity and probability, quantitative scales or qualitative scales based on quantitative logic should be used. If the concept that the expected losses (or risk) associated with a hazardous event or condition may be estimated by multiplying the expected severity of the accident by the probability of the accident, then some sort of quantitative basis is necessary. Failure to provide a quantitative basis for the scales can cause significant confusion and dissipation of safety resources when an arbitrary risk ranking scale is used.</p> <p>This committee inventoried existing FAA risk management processes, capabilities, and practices. Processes included types of decisions appropriate for risk management and current technical approaches. Capabilities included personnel skill levels, tools, and access to needed data. Practices include details of implementation and documentation.</p> <p>The SRMC has become a standing committee to serve as a resource for the FAA. It currently: exchanges risk management information between offices and other government agencies to avoid duplication of effort. It provides support across program lines including risk management/analysis training assistance capability. It identifies and recommends needed enhancements to FAA risk management/analysis capabilities and/or efficiencies.</p>
<b>Safety Critical</b>	All interactions, elements, components, subsystems, functions, processes, interfaces, within the system that can affect a predetermined level of risk.
<b>Safety Engineering Report</b>	Documents the results of safety analyses, including Operational Safety Assessments (OSA), Comparative Risk Assessments (CRA), Preliminary Hazard Analyses (PHA), System Hazard Analyses (SHA), Subsystem Hazard Analyses (SSHA), and Operational and Support Hazard Analysis (O&SHA).
<b>Security Risk</b>	<p>Some safety risks that the FAA must manage are the result of security issues. By its nature, the details of methodologies used to analyze and assess security hazards/risks cannot be published in this document. The section does, however, summarize a top-level approach to security risk management, especially as it relates to the methodologies used for safety risk management. Since the development of safety and risk management has not always been parallel, their terminology is sometimes different. Several security unique terms are introduced.</p> <p>Safety and Security hazards are both caused by experiencing a series of events that lead to a questionable condition. In security analyses, the term vulnerability is used to summarize the event path (approach used to achieve negative effect) that leads to the hazard.</p>
<b>Single Point Failure</b>	A single item of hardware, the failure of which would lead directly to loss of life, and / or system. Actually, a single malfunction, and / or failure, and /or error, of which would lead to loss of life, and / or system.

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Software</b>	Computer programs, procedures, rules, and associated documentation and data pertaining to the operation of a computer system.
<b>Software Code</b>	A software program or routine or set of routines, which were specified, developed and tested for a system configuration.
<b>Structured Programming</b>	Any software development technique that includes structured design and results in the development of structured programs.
<b>Subprogram</b>	A separately compilable, executable component of a computer programs.
<b>Subroutine</b>	A routine that returns control to the program of subprogram that called it.
<b>Subsystem</b>	An element of a system that, in itself, may constitute a system.
<b>Syntax</b>	The structural or grammatical rules that define how the symbols in a language are to be combined to form words, phrases, expressions, and other allowable constructs.
<b>System</b>	<p>A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, requirement; a set of arrangement of components so related or connected as to form a unity or organic whole.</p> <p>A composite of people, procedures, materials, tools, equipment, facilities, and software operating in a specific environment to perform a specific task or achieve a specific purpose, support, or mission requirement.</p>
<b>Systems Approach</b>	A step - by - step procedure for solving problems; a decision making process which moves from the general to the specific; an iterative process.
<b>System Safety</b>	<p>The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.</p> <p>A standardized management and engineering discipline that integrates the consideration of man, machine, and environment in planning, designing, testing, operating, and maintaining FAA operations, procedures, and acquisition projects. System safety is applied throughout a system's entire life cycle to achieve an acceptable level of risk within the constraints of operational effectiveness, time, and cost.</p>
<b>System Safety Analysis</b>	The analysis of a complex system by means of methods, techniques, and / or processes, to comprehensively evaluate safety related risks that are associated with the system under study.
<b>System Safety Engineer</b>	<p>An engineer qualified by appropriate credentials: training, education, registration, certification, and / or experience to perform system safety engineering.</p> <p>One should have an appropriate background and credentials directly related to system safety in order to practice in the field, i.e., CSP, PE, training, education, and actual experience.</p>
<b>System Safety Engineering</b>	An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate, or reduce safety related risks.
<b>System Safety</b>	A formally charted group of persons representing organizations associated with the system

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
<b>Working Group</b>	under study, organized to assist management in achieving the system safety objectives.
<b>System Safety Manager</b>	A person responsible for managing the system safety program.
<b>System Safety Objectives</b>	<p>System safety is achieved through the implementation and careful execution of an SSP. As stated previously, the ultimate objective of system safety is eliminated or minimize accidents and their results. The objectives of an SSP are to ensure that:</p> <ul style="list-style-type: none"> <li>• Safety, consistent with system purpose and program constraints, is designed into the system in a timely, cost-effective manner.</li> <li>• Hazards are identified, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the managing activity (MA) throughout the entire life cycle of a system.</li> <li>• Historical safety data, including lessons learned from other systems, are considered and used.</li> <li>• Minimum risk is sought in accepting and using new designs, materials, and production and test techniques.</li> <li>• Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.</li> <li>• Retrofit actions are minimized.</li> <li>• Changes in design, configuration, or operational requirements are accomplished in a manner that maintains a risk level acceptable to the MA.</li> <li>• Consideration is given to safety, ease of disposal, and storage of any hazardous materials associated with the system.</li> <li>• Significant safety data are documented as "lessons learned" and are submitted to data banks, design handbooks, or specifications.</li> <li>• Hazards identified after production are minimized consistent with program restraints.</li> </ul>
<b>System Safety Order of Precedence.</b>	The overall goal of a system safety program is to design systems that do not contain unacceptable hazards. However, the nature of most complex systems makes it impossible or impractical to design them completely hazard-free. As hazard analyses are performed, hazards will be identified that require resolution. System safety precedence defines the order to be followed for satisfying system safety requirements and reducing the presence and impact of risks. The alternatives for eliminating the specific hazard or controlling its associated risk must be evaluated so that an acceptable method for risk reduction can be pursued.

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<p><b>Design for Minimum Risk.</b> The most effective safety program is one that eliminates hazards through design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection. Defining minimum risk is not a simple matter. It is not a cookbook process that can be numerically developed without considerable thought. Minimum risk varies from program to program. See paragraph 3.6 for more information.</p> <p><b>Incorporate Safety Devices.</b> If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk should be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions should be made for periodic functional checks of safety devices when applicable.</p> <p><b>Provide Warning Devices.</b> When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices should be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application must be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.</p> <p><b>Develop Procedures and Training.</b> Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training should be used. However, without a specific waiver from the MA, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards. Procedures may include the use of personal protective equipment.</p>
<b>System Safety Program</b>	The tasks and activities of system safety that enhance effectiveness by ensuring that requirements are met, in a timely, cost-effective manner throughout all phases of the system life cycle.
<b>System Safety Program Plan</b>	A description of the planned methods to be used to implement the system safety requirements.
<b>System Safety Requirements by Acquisition Phase</b>	<p>Concept Exploration</p> <ul style="list-style-type: none"> <li>• Evaluate system safety design features</li> <li>• Identify possible interface problems</li> <li>• Highlight special safety considerations</li> <li>• Describe safety tests/data needed for next phase</li> <li>• Update requirements based on analysis results</li> <li>• Review designs of similar systems</li> <li>• Use past experience with similar system requirements</li> <li>• Identify waiver requirements</li> <li>• Prepare a report for milestone reviews</li> <li>• Tailor subsequent phase SSPs.</li> </ul>

CONCEPT or TERM	DESCRIPTION
	<p>Demonstration/Validation</p> <ul style="list-style-type: none"> <li>• SSPP describing contractor's proposed safety program effort</li> <li>• Establish criteria for validating contractor performance</li> <li>• Update specifications, requirements, safety characteristics</li> <li>• PHA for hazards and inherent risks</li> <li>• Safety Interface study for subsystems, e.g., Subsystem Hazard Analysis (SSHA)</li> <li>• Trade-off studies</li> <li>• Identify risks from design, operating environment, and technology</li> <li>• Identify qualification/quantitative system safety requirements</li> <li>• Perform system and equipment interface analyses e.g., System Hazard Analysis (SHA) and Operating and Support Hazard Analysis (O&amp;SHA)</li> <li>• Update test plans</li> <li>• Prepare summary reports for major program milestones</li> <li>• Review test plans</li> <li>• Review training plans</li> <li>• Evaluate hazards and failures for corrective actions</li> <li>• Perform SHA on test model</li> <li>• Identify need for special production and maintenance tools (e.g. barriers)</li> <li>• Review all related maintenance and production instructions</li> <li>• Review applicable safety requirements from FAA, DOT, EPA, and Occupational Safety and Health Administration (OSHA).</li> </ul> <p>Full Scale Development</p> <ul style="list-style-type: none"> <li>• Timely implementation of SSPP</li> <li>• Update system safety requirements</li> <li>• Perform hazard analyses. (SHA/O&amp;SHA)</li> <li>• Evaluate system design for hazards and safety improvements</li> <li>• Establish test requirements and ensure verification of design</li> <li>• Participate in design reviews</li> <li>• Provide inputs to training manuals, emergency procedures</li> <li>• Evaluate mishaps/failures and make recommendations</li> <li>• Review/input to trade-off studies</li> <li>• Review drawings/specifications for safety</li> <li>• Identify safety/protective equipment</li> <li>• Provide safety input to training</li> <li>• Ensure designs incorporate safety</li> <li>• Correct hazards identified demonstration/validation phase</li> </ul>

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	<ul style="list-style-type: none"> <li>• Evaluate storage, packing, and handling requirements/plans</li> <li>• Review production plans, drawings, procedures</li> <li>• Review plans for disposal of hazardous materials</li> <li>• Prepare documentation for major milestones</li> <li>• Tailor requirements for production</li> <li>• Review National Airspace Integrated Logistics Support (NAIS) considerations.</li> </ul> <p>Production and Deployment</p> <ul style="list-style-type: none"> <li>• Monitor system for adequacy of design safety</li> <li>• Evaluate design changes to prevent degraded inherent safety</li> <li>• Review operations and maintenance publications for safety information</li> <li>• Evaluate accidents; recommended design changes</li> <li>• Review deficiency reports for operators</li> <li>• Review disposal of hazardous materials</li> <li>• Update SSPP</li> <li>• Monitor production line for safety and safety control of system</li> <li>• Review production, maintenance, and operation manuals for necessary cautions, warnings etc. for previously identified hazards</li> <li>• Review system for necessary cautions, warning labels, etc. previously identified (e.g., high voltage)</li> <li>• Verify safety precautions in test and evaluation (T&amp;E) plans and procedures</li> <li>• Identify safety related aging problems and associated controls.</li> <li>• Update O&amp;SHA</li> <li>• Identify critical parts, procedures, facilities, and inspections</li> <li>• Continue to monitor design and procedures to uncover residual hazards; follow-up on corrective action.</li> </ul> <p>Facilities-Related Requirements</p> <ul style="list-style-type: none"> <li>• Ensure building, fire, and other related requirements are met</li> <li>• Review facility and installed systems interfaces</li> <li>• Review equipment plans</li> <li>• Update hazard tracking system</li> <li>• Evaluate accidents for deficiencies/oversights/corrective actions</li> <li>• Review design modifications for hazards; monitor corrective actions.</li> </ul>
<b>Test Case</b>	A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to test a particular program path or to verify compliance with a specific requirement.
<b>Testing</b>	The process of operating a system under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system.
<b>Test Procedure</b>	(a) Specified way to perform a test.

<b>CONCEPT or TERM</b>	<b>DESCRIPTION</b>
	(b) Detailed instructions for the set-up and execution of a given set of test cases, and instructions for the evaluation of results of executing the test cases.
<b>Traceability</b>	Ability to trace the history, application or location of an entity by means of recorded identifications.
<b>Transient Error</b>	An error that occurs once, or at unpredictable intervals.
<b>Validation</b>	The process of evaluating a system (and subset), during or at the end of the development process to determine whether it satisfies specified requirements. Conformance to requirements is no total assurance of acceptable risk.
<b>Verification</b>	The process of evaluating a system (and subset) to determine whether the products of a given development phase satisfy the conditions imposed at the start of the phase.
<b>Volatile Memory</b>	Memory that requires a continuous supply of power to its internal circuitry to prevent the loss of stored information.
<b>Voting</b>	A scheme in which the outputs of three or more channels of a system implementation are compared with each other in order to determine agreement between two or more channels, and to permit continued operation in the presence of a malfunction in one of the channels. A degree of fault / malfunction tolerance is obtained.
<b>Watchdog Timer</b>	A device that monitors a prescribed operation of computer hardware and / or software and provides an indication when such operation has ceased.
<b>Zero Energy State</b>	<p>All energy within the system has been reduced to the lowest possible energy level, at “zero energy level” if possible. All stored or residual energy, such as within capacitors, springs, elevated devices, rotating flywheels, hydraulic systems, pneumatic systems, have been dissipated.</p> <p>It should be noted that it is not possible to dissipate / de-energize all energy within the system additional controls should be implemented, i.e. lockout, repositioning, isolating, restraining, guarding, shielding, relief, bleed off devices.</p>

FAA System Safety Handbook, Appendix B: Comparative Risk Assessment (CRA) Form  
December 30, 2000

## **Appendix B**

# **Comparative Risk Assessment Form**

FAA System Safety Handbook, Appendix B: Comparative Risk Assessment (CRA) Form  
December 30, 2000

<b>SEC TRACKING No:</b> This is the number assigned to the CRA by the FAA System Engineering Council (SEC)		<b>CRA Title:</b> Title as assigned by the FAA SEC					
<b>SYSTEM:</b> This is the system being affected by the change, e.g. National Airspace System <b>Initial Date:</b> Date initiated <b>SEC date:</b> Date first reviewed by the SEC							
<b>REFERENCES:</b> A short list or references. If a long list is used can be continued on a separate page.							
<b>SSE INFORMATION</b>							
<b>SSE Name/Title:</b> Name and title of person who performed or led team		<b>Location:</b> Address and office symbol of SSE		<b>Telephone No.:</b>			
<b>SUMMARY OF HAZARD CLASSIFICATION:</b> (worst credible case; see List of Hazards below for individual risk assessments)							
<b>Option A (Baseline):</b> Place the highest risk assessment code for the baseline here			<b>Proposed Change</b> <b>Option(s) B-X:</b> Place the highest risk assessment code for the alternatives here.				
<b>DESCRIPTION OF (Option A) BASELINE AND PROPOSED CHANGE(s)</b> <b>Option A:</b> Describe the system under study here in terms of the 5 M Model discussed in chapter 2. Describe the baseline (or no change) system and each alternative. This section can be continued in an appendix if it does not fit into this area. Avoid too much detail, but include enough so that the decision-maker has enough information to understand the risk associated with each alternative.							
<b>SEVERITY:</b> 1 CATASTROPHIC – Death, system or aircraft loss, permanent total disability 2 HAZARDOUS - Severe injury or major aircraft or system damage 3 MAJOR - Minor injury or minor aircraft or system damage 4 MINOR – Less than minor injury or aircraft or system damage 5 NO SAFETY EFFECT  <b>PROBABILITY:</b> A PROBABLE - Likely to occur in lifetime of each system (> 1E-5) B REMOTE – Possible for each item, several for system (< 1E-5) C EXTREMELY REMOTE – Unlikely for item, may occur few in system (< 1E-7) D EXTREMELY IMPROBABLE – so unlikely, not expected in system (<1E-9)			<b>PROBABILITY</b>				
			<b>SEVERITY</b>	A	B	C	D
			1				
			2				
			3				
			4				
5	No risk						

FAA System Safety Handbook, Appendix B: Comparative Risk Assessment (CRA) Form  
December 30, 2000

<b>HAZARD LIST</b>						
<b>No.</b>	<b>Hazard Condition</b>	<b>RISK ASSESSMENT CODE (RAC)</b>				
		Baseline Option A	Option B	Option C	Option D	Option E
	List the hazard conditions here. Enter the risk assessment codes for each hazard – alternative to the right.					
1	Loss of communication between air traffic controllers and aircraft (flight essential)	1D	1D	1C	1C	1B
2	Loss of communication between air traffic controllers in different domains (ARTCC to ARTCC, ARTCC to TRACON, etc.)	1D				
3	Loss of communication between air traffic controllers and flight service (flight plans, etc.)					
4	Loss of communication between air traffic & ground controllers and vehicles in the airport movement area					
5	Loss of the means for operator and flight service to communicate information relative to planned flight					
6	Loss of the capability to detect, classify, locate, and communicate adverse weather such as: thunderstorms, rain and snow showers, lightning, windshear, tornadoes, icing, low visibility or ceilings, turbulence, hail, fog, etc.					
7	Loss of navigation functions providing aircrew with independently determined 3D present position of the aircraft, defined routes, destination(s), and navigation solution (course, distance) to destination.					
8	Loss of Air traffic control determination of 3D location, velocity vector, and identity of each aircraft operating in a domain.					
9	Loss of Air traffic control determination of location, identity, and velocity vector of each participating vehicle operating in the airport movement area domain.					

FAA System Safety Handbook, Appendix B: Comparative Risk Assessment (CRA) Form  
December 30, 2000

10	Loss of approach guidance to runway. Precision – horizontal and vertical guidance; Non-precision – horizontal guidance, vertical procedures.					
11	Loss of ground vehicle or aircraft operator independent determination of present position, destination(s), and navigation solution on the airport movement area.					
12	Hazardous runway surface precludes safe takeoff or touchdown and rollout.					

**SAFETY ASSESSMENT SUMMARY**

(Conclusions/Recommendations)

Summarize your conclusions. Which option is best (and 2<sup>nd</sup>, 3<sup>rd</sup>, etc) and why. Include enough detail to appropriately communicate with the audience.

Recommendations: Provide additional controls to further mitigate or eliminate the risks. Follow the safety order of precedence, i.e., (1) eliminate/mitigate by design, (2) incorporate safety features, (3) provide warnings, and (4) procedures/training. See Chapter 4 for further elaboration of the Safety Order of Precedence). Define SSE requirements for reducing the risk of the design/option(s).



<b>Probability</b>	<p><b>Rationale for Probability:</b>          Use this section to explain how you derived the probability. This may be quantitative or qualitative. In general, the higher risk items will require more quantitative analysis than low or medium risk hazards. The example below is qualitative.</p> <p>Many controls exist to preclude this hazard from occurring-          Multiple radios both in the aircraft and in the ATC facility provide redundant communication channels from aircraft to ATC.          In the event of failure multiple facilities can be used including FSS, other ARTCC, TRACON, or ATCC, even airborne telephones.</p> <ol style="list-style-type: none"> <li>1. Planning systems assist in keeping aircraft at different altitudes or routes. Emergency procedures exist to ensure an aircraft in “lost communication” will not converge on another aircraft’s flight path.</li> </ol>
--------------------	---

<sup>1</sup> Federal Aviation Administration. (1995). Airman’s Information Manual. Para. 4-2-1.

---

**Severity Definitions**

<b>Catastrophic</b>	Results in multiple fatalities and/or loss of the system
<b>Hazardous</b>	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: Large reduction in safety margin or functional capability Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely (1) Serious or fatal injury to small number of occupants of aircraft (except operators) Fatal injury to ground personnel and/or general public
<b>Major</b>	Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be – Significant reduction in safety margin or functional capability Significant increase in operator workload Conditions impairing operator efficiency or creating significant discomfort Physical distress to occupants of aircraft (except operator) including injuries Major occupant illness and/or major environmental damage, and/or major property damage
<b>Minor</b>	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include Slight reduction in safety margin or functional capabilities Slight increase in workload such as routine flight plan changes Some physical discomfort to occupants or aircraft (except operators)
<b>No Safety Effect</b>	Has no effect on safety

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

## **Appendix C**

### **REFERENCES**

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

## GOVERNMENT REFERENCES

FAA Order 1810, Acquisition Policy

FAA Order 8040.4 FAA Safety Risk Management

FAA Advisory Circular 25.1309 (Draft), System Design and Analysis, January 28, 1998

RTCA-DO 178B, Software Considerations In Airborne Systems And Equipment Certification, December 1, 1992 COMDTINST M411502D, System Acquisition Manual, December 27, 1994DODD 5000.1, Defense Acquisition, March 15, 1996

DOD 5000.2R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems, March 15, 1996

DOD-STD 2167A, Military Standard Defense System Software Development, February 29, 1988

MIL-STD 882D, System Safety Program Requirements, February 10, 2000

MIL-STD 498, Software Development and Documentation, December 5, 1994

MIL-HDBK-217A, "Reliability Prediction of Electronic Equipment," 1982.

MIL-STD-1629A "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," November 1980.

MIL-STD-1472D, "Human Engineering Design Criteria for Military Systems, Equipment and Facilities," 14 March 1989.

NSS 1740.13, Interim Software Safety Standard, June 1994

29 CFR 1910.119 Process Safety Management, U.S. Government Printing Office, July 1992.

Department of the Air Force, Software Technology Support Center, Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems, Version-2, June 1996, Volumes 1 and 2 AFISC SSH 1-1, Software System Safety Handbook, September 5, 1985

Department of Defense, AF Inspections and Safety Center (now the AF Safety Agency), AFIC SSH 1-1 "Software System Safety," September 1985.

Department of Labor, 29 CFR 1910, "OSHA Regulations for General Industry," July 1992.

Department of Labor, 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals," Federal Register, 24 February 1992.

Department of Labor, 29 CFR 1926, "OSHA Regulations for Construction Industry," July 1992.

Department of Labor, OSHA 3133, "Process Safety Management Guidelines for Compliance," 1992.

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

Department of Labor, OSHA Instructions CPL 2-2.45A, Compliance Guidelines and Enforcement Procedures, September 1992.

Department of Transportation, DOT P 5800.5, "Emergency Response Guidebook," 1990.

Environmental Protection Agency, 1989d, Exposure Factors Handbook, EPA/600/8-89/043, Office of Health and Environmental Assessment, Washington, DC 1989.

Environmental Protection Agency, 1990a, Guidance for Data Usability in Risk Assessment, EPA/540/G-90/008, Office of Emergency and Remedial Response, Washington, DC 1990.

## **COMMERCIAL REFERENCES**

ACGIH, "Guide for Control of Laser Hazards," American Conference of Government Industrial Hygienists, 1990.

American Society for Testing and Materials (ASTM), 1916 Race Street, Philadelphia, PA. 19103

ASTM STP762, "Fire Risk Assessment" American Society for Testing Materials, 1980.

EIA-6B, G-48, Electronic Industries Association, System Safety Engineering In Software Development 1990 IEC 61508: International Electrotechnical Commission. Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems, December 1997

EIC 1508 -(Draft), International Electrotechnical Commission, Functional Safety; Safety-Related System, June 1995

IEEE STD 1228, Institute of Electrical and Electronics Engineers, Inc., Standard For Software Safety Plans, 1994

IEEE STD 829, Institute of Electrical and Electronics Engineers, Inc., Standard for Software Test Documentation, 1983

IEEE STD 830, Institute of Electrical and Electronics Engineers, Inc., Guide to Software Requirements Specification, 1984

IEEE STD 1012, Institute of Electrical and Electronics Engineers, Inc., Standard for Software Verification and Validation Plans, 1987

ISO 12207-1, International Standards Organization, Information Technology-Software, 1994

Joint Software System Safety Committee, "Software System Safety Handbook", December 1999

NASA NSTS 22254, "Methodology for Conduct of NSTS Hazard Analyses," May 1987.

National Fire Protection Association, "Flammable and Combustible Liquids Code."

National Fire Protection Association, "Hazardous Chemical Handbook"

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

National Fire Protection Association, "Properties of Flammable Liquids, Gases and Solids".

National Fire Protection Association, "Fire Protection Handbook."

Nuclear Regulatory Commission NRC, "Safety/Risk Analysis Methodology", April 12, 1993.

Joint Services Computer Resources Management Group, "Software System Safety Handbook: A Technical and Managerial Team Approach", Published on Compact Disc, December 1999.

Society of Automotive Engineers, Aerospace Recommended Practice 4754: "Certification Considerations for Highly Integrated or Complex Aircraft Systems", November 1996.

Society of Automotive Engineers, Aerospace Recommended Practice 4761: "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", December 1996.

System Safety Society: System Safety Analysis Handbook, July 1997.

## **INDIVIDUAL REFERENCES**

Ang, A.H.S., and Tang, W.H., "Probability Concept in Engineering Planning and Design", Vol. II John Wiley and Sons, 1984.

Anderson, D. R., Dennis J. Sweeney, Thomas A. Williams, "An Introduction to Management Science Quantitative Approaches to Decision Making." West Publishing Co., 1976.

Bahr, N. J., "System Safety Engineering and Risk Assessment: A Practical Approach", Taylor and Francis 1997.

Benner, L. "Guide 7: A Guide for Using energy Trace and Barrier Analysis with the STEP Investigation System", Events Analysis, Inc., Oakton, Va., 1985.

Briscoe, G.J., "Risk Management Guide", EG&G Idaho, Inc. SSDC-11, June 1997.

Brown, M., L., "Software Systems Safety and Human Error", Proceedings: COMPASS 1988

Brown, M., L., "What is Software Safety and Who's Fault Is It Anyway?" Proceedings: COMPASS 1987

Brown, M., L., "Applications of Commercially Developed Software in Safety Critical Systems", Proceedings of Parari '99, November 1999

Bozarth, J. D., Software Safety Requirement Derivation and Verification, Hazard Prevention, Q1, 1998

Card, D.N. and Schultz, D.J., "Implementing a Software Safety Program", Proceedings: COMPASS 1987

Clark, R., Benner, L. and White, L. M., "Risk Assessment Techniques Manual," Transportation Safety Institute, March 1987, Oklahoma City, OK.

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

Clemens, P.L. "A Compendium of Hazard Identification and Evaluation Techniques for System Safety Application," Hazard Prevention, March/April, 1982.

Cooper, J.A., "Fuzzy-Algebra Uncertainty Analysis," Journal of Intelligent and Fuzzy Systems, Vol. 2 No. 4 1994.

Connolly, B., "Software Safety Goal Verification Using Fault Tree Techniques: A Critically Ill Patient Monitor Example", Proceedings: COMPASS 1989

De Santo, B., "A Methodology for Analyzing Avionics Software Safety", Proceedings: COMPASS 1988

Dunn, R., Ullman, R., "Quality Assurance For Computer Software", McGraw Hill, 1982

Forrest, M., and McGoldrick, Brendan, "Realistic Attributes of Various Software Safety Methodologies", Proceedings: 9 Th International System Safety Society, 1989

Hammer, W., R., "Identifying Hazards in Weapon Systems – The Checklist Approach", Proceedings: Parari '97, Canberra, Australia

Hammer, Willie, "Occupational Safety Management and Engineering", 2 Ed., Prentice-Hall, Inc, Englewood Cliffs, NJ, 1981.

Heinrich, H.W., Petersen, D., Roos, N., "Industrial Accident Prevention: A Safety Management Approach", McGraw-Hill, 5 Th Ed., 1980.

Johnson, W.G., "MORT –The Management Oversight and Risk Tree," SAN 821-2, U.S. Atomic Energy Commission, 12 February 1973.

Kije, L.T., "Residual Risk," Rusee Press, 1963.

Kjos, K., "Development of an Expert System for System Safety Analysis", Proceedings: 8 Th International System Safety Conference, Volume II.

Klir, G.J., Yuan, B., "Fuzzy Sets and Fuzzy logic: Theory and Applications", Prentice Hall P T R, 1995.

Kroemer, K.H.E., Kroemer, H.J., Kroemer-Elbert, K.E., "Engineering Physiology: Bases of Human Factors/Ergonomics", 2 Nd. Ed., Van Nostrand Reinhold, 1990.

Lawrence, J.D., "Design Factors for Safety-Critical Software", NUREG/CR-6294, Lawrence Livermore National Laboratory, November 1994

Lawrence, J.D., "Survey of Industry Methods for Producing Highly Reliable Software", NUREG/CR-6278, Lawrence Livermore National Laboratory, November 1994.

Leveson, N., G, "SAFWARE; System Safety and Computers, A Guide to Preventing Accidents and Losses Caused By Technology", Addison Wesley, 1995

FAA System Safety Handbook, Appendix C: Related Readings in Aviation System Safety  
December 30, 2000

Leveson, N., G., "Software Safety: Why, What, and How, Computing Surveys", Vol. 18, No. 2,  
June 1986.

Littlewood, B. and Strigini, L., "The Risks of Software", Scientific American, November 1992.

Mattern, S.F. Capt., "Defining Software Requirements for Safety-Critical Functions",  
Proceedings: 12 Th International System Safety Conference, 1994.

Mills, H., D., "Engineering Discipline for Software Procurement", Proceedings: COMPASS  
1987.

Moriarty, Brian and Roland, Harold, E., "System Safety Engineering and Management", Second  
Edition, John Wiley & Sons, 1990.

Ozkaya, N., Nordin, M. " Fundamentals of Biomechanics: Equilibrium, Motion, and  
Deformation", Van Nostrand Reinhold, 1991.

Raheja, Dev, G., "Assurance Technologies: Principles and Practices", McGraw-Hill, Inc., 1991.

Rodger, W.P. "Introduction to System Safety Engineering", John Wiley and Sons.

Russo, Leonard, "Identification, Integration, and Tracking of Software System Safety  
Requirements", Proceedings: 12 Th International System Safety Conference, 1994.

Saaty, T.L., "The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation", 2  
Nd., RWS Publications, 1996.

Stephenson, Joe, "System Safety 2000 A Practical Guide for Planning, Managing, and  
Conducting System Safety Programs", Van Nostrand Reinhold, 1991.

Tarrants, William, E. "The Measurement of Safety Performance", Garland STPM Press, 1980.

## **OTHER REFERENCES**

DEF(AUST) 5679, Army Standardization (ASA), "The Procurement Of Computer-Based Safety  
Critical Systems", May 1999

UK Ministry of Defense. Interim DEF STAN 00-54: "Requirements for Safety Related Electronic  
Hardware in Defense Equipment", April 1999.

UK Ministry of Defense. Defense Standard 00-55: "Requirements for Safety Related Software in  
Defense Equipment", Issue 2, 1997

UK Ministry of Defense. Defense Standard 00-56: "Safety Management Requirements for  
Defense Systems", Issue 2, 1996

International Electrotechnical Commission, IEC 61508, "Functional Safety of  
Electrical/Electronic/Programmable Electronic Safety-Related Systems", draft 61508-2 Ed 1.0,  
1998

FAA System Safety Handbook, Appendix D  
December 30, 2000

# **Appendix D**

## **Structured Analysis and Formal Methods**

## D.1 Structured Analysis and Formal Methods

Structured Analysis became popular in the 1980's and is still used by many. The analysis consists of interpreting the system concept (or real world) into data and control terminology, that is into data flow diagrams. The flow of data and control from bubble to data store to bubble can be very hard to track and the number of bubbles can get to be extremely large. One approach is to first define events from the outside world that require the system to react, then assign a bubble to that event, bubbles that need to interact are then connected until the system is defined. This can be rather overwhelming and so the bubbles are usually grouped into higher level bubbles. Data Dictionaries are needed to describe the data and command flows and a process specification is needed to capture the transaction/transformation information. The problems have been: 1) choosing bubbles appropriately, 2) partitioning those bubbles in a meaningful and mutually agreed upon manner, 3) the size of the documentation needed to understand the Data Flows, 4) still strongly functional in nature and thus subject to frequent change, 5) though "data" flow is emphasized, "data" modeling is not, so there is little understanding of just what the subject matter of the system is about, and 6) not only is it hard for the customer to follow how the concept is mapped into these data flows and bubbles, it has also been very hard for the designers who must shift the DFD organization into an implementable format.

Information Modeling, using entity-relationship diagrams, is really a forerunner for OOA. The analysis first finds objects in the problem space, describes them with attributes, adds relationships, refines them into super and sub-types and then defines associative objects. Some normalization then generally occurs. Information modeling is thought to fall short of true OOA in that, according to Peter Coad & Edward Yourdon:

- 1) Services, or processing requirements, for each object are not addressed,
- 2) Inheritance is not specifically identified,
- 3) Poor interface structures (messaging) exists between objects, and
- 4) Classification and assembly of the structures are not used as the predominate method for determining the system's objects.

This handbook presents in detail the two new most promising methods of structured analysis and design: Object-Oriented and Formal Methods (FM). OOA/OOD and FM can incorporate the best from each of the above methods and can be used effectively in conjunction with each other. Lutz and Ampo described their successful experience of using OOD combined with Formal Methods as follows: "For the target applications, object-oriented modeling offered several advantages as an initial step in developing formal specifications. This reduced the effort in producing an initial formal specification. We also found that the object-oriented models did not always represent the "why," of the requirements, i.e., the underlying intent or strategy of the software. In contrast, the formal specification often clearly revealed the intent of the requirements."

## D.2 Object Oriented Analysis and Design

Object Oriented Design (OOD) is gaining increasing acceptance worldwide. These fall short of full Formal Methods because they generally do not include logic engines or theorem provers. But they are more widely used than Formal Methods, and a large infrastructure of tools and expertise is readily available to support practical OOD usage.

FAA System Safety Handbook, Appendix D  
December 30, 2000

OOA/OOD is the new paradigm and is viewed by many as the best solution to most problems. Some of the advantages of modeling the real world into objects is that 1) it is thought to follow a more natural human thinking process and 2) objects, if properly chosen, are the most stable perspective of the real world problem space and can be more resilient to change as the functions/services and data & commands/messages are isolated and hidden from the overall system. For example, while over the course of the development life-cycle the number, as well as types, of functions (e.g. turn camera 1 on, download sensor data, ignite starter, fire engine 3, etc.) may change, the basic objects (e.g. cameras, sensors, starter, engines, operator, etc.) needed to create a system usually are constant. That is, while there may now be three cameras instead of two, the new Camera-3 is just an instance of the basic object 'camera'. Or while an infrared camera may now be the type needed, there is still a 'camera' and the differences in power, warm-up time, and data storage may change, all that is kept isolated (hidden) from affecting the rest of the system.

OOA incorporates the principles of abstraction, information hiding, inheritance, and a method of organizing the problem space by using the three most "human" means of classification. These combined principles, if properly applied, establish a more modular, bounded, stable and understandable software system. These aspects of OOA should make a system created under this method more robust and less susceptible to changes, properties which help create a safer software system design.

Abstraction refers to concentrating on only certain aspects of a complex problem, system, idea or situation in order to better comprehend that portion. The perspective of the analyst focuses on similar characteristics of the system objects that are most important to them. Then, at a later time, the analyst can address other objects and their desired attributes or examine the details of an object and deal with each in more depth. Data abstraction is used by OOA to create the primary organization for thinking and specification in that the objects are first selected from a certain perspective and then each object is defined in detail. An object is defined by the attributes it has and the functions it performs on those attributes. An abstraction can be viewed, as per Shaw, as "a simplified description, or specification, of a system that emphasizes some of the system's details or properties while suppressing others. A good abstraction is one that emphasizes details that are significant to the reader or user and suppresses details that are, at least for the moment, immaterial or diversionary".

Information hiding also helps manage complexity in that it allows encapsulation of requirements, which might be subject to change. In addition, it helps to isolate the rest of the system from some object specific design decisions. Thus, the rest of the s/w system sees only what is absolutely necessary of the inner workings of any object.

Inheritance " defines a relationship among classes [objects], wherein one class shares the structure or behavior defined in one or more classes... Inheritance thus represents a hierarchy of abstractions, in which a subclass [object] inherits from one or more superclasses [ancestor objects]. Typically, a subclass augments or redefines the existing structure and behavior of its superclasses".

Classification theory states that humans normally organize their thinking by: looking at an object and comparing its attributes to those experienced before (e.g. looking at a cat, humans tend to think of its size, color, temperament, etc. in relation to past experience with cats) distinguishing between an entire object and its component parts (e.g., a rose bush versus its roots, flowers, leaves, thorns, stems, etc.) classification of objects as distinct and separate groups (e.g. trees, grass, cows, cats, politicians).

In OOA, the first organization is to take the problem space and render it into objects and their attributes (abstraction). The second step of organization is into Assembly Structures, where an object and its parts are considered. The third form of organization of the problem space is into Classification Structures during which the problem space is examined for generalized and specialized instances of objects

FAA System Safety Handbook, Appendix D  
December 30, 2000

(inheritance). That is, if looking at a railway system the objects could be engines (provide power to pull cars), cars (provide storage for cargo), tracks (provide pathway for trains to follow/ride on), switches (provide direction changing), stations (places to exchange cargo), etc. Then you would look at the Assembly Structure of cars and determine what was important about their pieces parts, their wheels, floor construction, coupling mechanism, siding, etc. Finally, Classification Structure of cars could be into cattle, passenger, grain, refrigerated, and volatile liquid cars.

The purpose of all this classification is to provide modularity which partitions the system into well defined boundaries that can be individually/independently understood, designed, and revised. However, despite “classification theory”, choosing what objects represent a system is not always that straight forward. In addition, each analyst or designer will have their own abstraction, or view of the system which must be resolved. OO does provide a structured approach to software system design and can be very useful in helping to bring about a safer, more reliable system.

### **D.3 Formal Methods - Specification Development**

“Formal Methods (FM) consists of a set of techniques and tools based on mathematical modeling and formal logic that are used to specify and verify requirements and designs for computer systems and software.”

While Formal Methods (FM) are not widely used in US industry, FM has gained some acceptance in Europe. A considerable learning curve must be surmounted for newcomers, which can be expensive. Once this hurdle is surmounted successfully, some users find that it can reduce overall development life-cycle cost by eliminating many costly defects prior to coding.

#### **WHY ARE FORMAL METHODS NECESSARY?**

A digital system may fail as a result of either physical component failure, or design errors. The validation of an ultra-reliable system must deal with both of these potential sources of error.

Well known techniques exist for handling physical component failure; these techniques use redundancy and voting. The reliability assessment problem in the presence of physical faults is based upon Markov modeling techniques and is well understood.

The design error problem is a much greater threat. Unfortunately, no scientifically justifiable defense against this threat is currently used in practice. There are 3 basic strategies that are advocated for dealing with the design error:

1. Testing (Lots of it)
2. Design Diversity (i.e. software fault-tolerance: N-version programming, recovery blocks, etc.)
3. Fault/Failure Avoidance (i.e. formal specification/verification, automatic program synthesis, reusable modules)

The problem with life testing is that in order to measure ultrareliability one must test for exorbitant amounts of time. For example, to measure a  $10^{-9}$  probability of failure for a 1-hour mission one must test for more than 114,000 years.

Many advocate design diversity as a means to overcome the limitations of testing. The basic idea is to use separate design/implementation teams to produce multiple versions from the same specification. Then,

non-exact threshold voters are used to mask the effect of a design error in one of the versions. The hope is that the design flaws will manifest errors independently or nearly so.

By assuming independence one can obtain ultra-reliable-level estimates of reliability even though the individual versions have failure rates on the order of  $10^{-4}$ . Unfortunately, the independence assumption has been rejected at the 99% confidence level in several experiments for low reliability software. Furthermore, the independence assumption cannot ever be validated for high reliability software because of the exorbitant test times required. If one cannot assume independence then one must measure correlations. This is infeasible as well--it requires as much testing time as life-testing the system because the correlations must be in the ultra-reliable region in order for the system to be ultra-reliable. Therefore, it is not possible, within feasible amounts of testing time, to establish that design diversity achieves ultra-reliability.

Consequently, design diversity can create an illusion of ultra-reliability without actually providing it.

It is felt that formal methods currently offer the only intellectually defensible method for handling the design fault problem. Because the often quoted  $1 - 10^{-9}$  reliability is well beyond the range of quantification, there is no choice but to develop life-critical systems in the most rigorous manner available to us, which is the use of formal methods.

#### WHAT ARE FORMAL METHODS?

Traditional engineering disciplines rely heavily on mathematical models and calculation to make judgments about designs. For example, aeronautical engineers make extensive use of computational fluid dynamics (CFD) to calculate and predict how particular airframe designs will behave in flight. We use the term formal methods to refer to the variety of mathematical modeling techniques that are applicable to computer system (software and hardware) design. That is, formal methods is the applied mathematics engineering and, when properly applied, can serve a role in computer system design.

Formal methods may be used to specify and model the behavior of a system and to mathematically verify that the system design and implementation satisfy system functional and safety properties. These specifications, models, and verifications may be done using a variety of techniques and with various degrees of rigor. The following is an imperfect, but useful, taxonomy of the degrees of rigor in formal methods:

- Level-1: Formal specification of all or part of the system.
- Level-2: Formal specification at two or more levels of abstraction and paper and pencil proofs that the detailed specification implies the more abstract specification.
- Level-3: Formal proofs checked by a mechanical theorem prover.

Level 1 represents the use of mathematical logic or a specification language that has a formal semantics to specify the system. This can be done at several levels of abstraction. For example, one level might enumerate the required abstract properties of the system, while another level describes an implementation that is algorithmic in style.

Level 2 formal methods goes beyond Level 1 by developing pencil-and-paper proofs that the more concrete levels logically imply the more abstract-property oriented levels. This is usually done in the manner illustrated below.

Level 3 is the most rigorous application of formal methods. Here one uses a semi-automatic theorem prover to make sure that all of the proofs are valid. The Level 3 process of convincing a mechanical

FAA System Safety Handbook, Appendix D  
December 30, 2000

prover is really a process of developing an argument for an ultimate skeptic who must be shown every detail.

Formal methods is not an all-or-nothing approach. The application of formal methods to only the most critical portions of a system is a pragmatic and useful strategy. Although a complete formal verification of a large complex system is impractical at this time, a great increase in confidence in the system can be obtained by the use of formal methods at key locations in the system.

### **D.3.1 Formal Inspections of Specifications**

Formal inspections and formal analysis are different. Formal Inspections should be performed within every major step of the software development process.

Formal Inspections, while valuable within each design phase or cycle, have the most impact when applied early in the life of a project, especially the requirements specification and definition stages of a project. Studies have shown that the majority of all faults/failures, including those that impinge on safety, come from missing or misunderstood requirements. Formal Inspection greatly improves the communication within a project and enhances understanding of the system while scrubbing out many of the major errors/defects.

For the Formal Inspections of software requirements, the inspection team should include representatives from Systems Engineering, Operations, Software Design and Code, Software Product Assurance, Safety, and any other system function that software will control or monitor. It is very important that software safety be involved in the Formal Inspections.

It is also very helpful to have inspection checklists for each phase of development that reflect both generic and project specific criteria. The requirements discussed in this section and in Robyn R. Lutz's paper "Targeting Safety-Related Errors During Software Requirements Analysis" will greatly aid in establishing this checklist. Also, the checklists provided in the NASA Software Formal Inspections Guidebook are helpful.

### **D.3.2 Timing, Throughput And Sizing Analysis**

Timing and sizing analysis for safety critical functions evaluates software requirements that relate to execution time and memory allocation. Timing and sizing analysis focuses on program constraints. Typical constraint requirements are maximum execution time and maximum memory usage. The safety organization should evaluate the adequacy and feasibility of safety critical timing and sizing requirements. These analyses also evaluate whether adequate resources have been allocated in each case, under worst case scenarios. For example, will I/O channels be overloaded by many error messages, preventing safety critical features from operating.

Quantifying timing/sizing resource requirements can be very difficult. Estimates can be based on the actual parameters of similar existing systems.

Items to consider include:

- memory usage versus availability;
- I/O channel usage (load) versus capacity and availability;
- execution times versus CPU load and availability;
- sampling rates versus rates of change of physical parameters.

FAA System Safety Handbook, Appendix D  
December 30, 2000

In many cases it is difficult to predict the amount of computing resources required. Hence, making use of past experience is important.

### **D.3.3 Memory usage versus availability**

Assessing memory usage can be based on previous experience of software development if there is sufficient confidence. More detailed estimates should evaluate the size of the code to be stored in the memory, and the additional space required for storing data and scratchpad space for storing interim and final results of computations. Memory estimates in early program phases can be inaccurate, and the estimates should be updated and based on prototype codes and simulations before they become realistic. Dynamic Memory Allocation can be viewed as either a practical memory run time solution or as a nightmare for assuring proper timing and usage of critical data. Any suggestion of Dynamic Memory Allocation, common in OOD, CH environments, should be examined very carefully; even in “non-critical” functional modules.

#### **D.3.3.1 I/O channel usage (Load) versus capacity and availability**

Address I/O for science data collection, housekeeping and control. Evaluate resource conflicts between science data collection and safety critical data availability. During failure events, I/O channels can be overloaded by error messages and these important messages can be lost or overwritten. (e.g. the British “Piper Alpha” offshore oil platform disaster). Possible solutions includes, additional modules designed to capture, correlate and manage lower level error messages or errors can be passed up through the calling routines until at a level which can handle the problem; thus, only passing on critical faults or combinations of faults, that may lead to a failure.

Execution times versus CPU load and availability. Investigate time variations of CPU load, determine circumstances of peak load and whether it is acceptable. Consider multi-tasking effects. Note that excessive multi-tasking can result in system instability leading to “crashes”.

#### **D.3.3.2 Sampling rates versus rates of change of physical parameters**

Analysis should address the validity of the system performance models used, together with simulation and test data, if available.

FAA System Safety Handbook, Appendix E: System Safety Principles  
December 30, 2000

## **Appendix E**

### **System Safety Principles**

<p><b>System Safety Principles</b></p>	<ul style="list-style-type: none"> <li>• System safety is a basic requirement of the total system.</li> <li>• System safety must be planned       <ul style="list-style-type: none"> <li>- Integrated and comprehensive safety engineering effort</li> <li>- Interrelated, sequential, and continuing effort</li> <li>- Plan must influence facilities, equipment, procedures, and personnel</li> <li>- Applicable to <u>all</u> program phases</li> <li>- Covers transportation and logistics support</li> <li>- Covers storage, packaging, and handling</li> <li>- Covers Non-Development Items (NDI).</li> </ul> </li> <li>• MA provides management of system safety effort Managerial and technical procedures to be used must be for MA approval.       <ul style="list-style-type: none"> <li>- Resolves conflicts between safety and other design requirements</li> <li>- Resolves conflicts between associate contractors.</li> </ul> </li> <li>• Design safety precedence:       <ul style="list-style-type: none"> <li>- Design to minimum hazard</li> <li>- Use safety devices</li> <li>- Use warning devices</li> <li>- Use special procedures.</li> </ul> </li> <li>• System Safety requirements must be consistent with other program requirements. Performance, cost, etc., requirements may have priority over safety Requirements.</li> <li>• System analyses are basic tools for systematically developing design specifications. Ultimate measure of safety is not the scope of analysis but in satisfied Requirements.       <ul style="list-style-type: none"> <li>- Analyses are performed to:           <ul style="list-style-type: none"> <li>▪ Identify hazards and corrective actions</li> <li>▪ Review safety considerations in tradeoffs</li> <li>▪ Determine/evaluate safety design requirements</li> <li>▪ Determine/evaluate operational, test, logistics requirements</li> <li>▪ Validate qualitative/quantitative requirements have been met.</li> </ul> </li> <li>- Analyses are <u>hazard</u> not <u>safety</u> analyses</li> </ul> </li> </ul>
--	--

	<ul style="list-style-type: none"><li>• Level of risk assumption and criteria are an inherent part of risk management.</li><li>• Safety Management<ul style="list-style-type: none"><li>- Defines functions, authority, and interrelationships</li><li>- Exercises appropriate controls.</li></ul></li><li>• Degree of safety effort and achievements are directly dependent upon management emphasis by the FAA and contractors.</li><li>• Results of safety effort depend upon MA clearly stating safety objectives/requirements.</li><li>• MA responsibilities:<ul style="list-style-type: none"><li>- Plan, organize, and implement SSP</li><li>- Establish safety requirements for system design</li><li>- State safety requirements in contract</li><li>- Requirements for activities in Statement of Work (SOW)</li><li>- Review and insure adequate and complete system safety program plan (SSPP)</li><li>- Supply historical data</li><li>- Review contractor system safety effort/data</li><li>- Ensure specifications are updated with test analyses results</li><li>- Establish and operate system safety groups.</li></ul></li><li>• Software hazard analyses are a flow down requirements process followed by an upward flow verification process</li><li>• Four elements of an effective SSP:<ul style="list-style-type: none"><li>- Planned approach to accomplish tasks</li><li>- Qualified people</li><li>- Authority to implement tasks through all levels of management</li><li>- Appropriate manning/funding.</li></ul></li></ul>
--	---

FAA System Safety Handbook, Appendix F  
December 30, 2000

## **Appendix F**

### **ORM Details and Examples**

## 1.0 HAZARD IDENTIFICATION TOOLS, DETAILS AND EXAMPLES

Chapter 15 summarizes the Operational Risk Management methodology. This Appendix provides examples of those tools, as they are applied to the ORM process:

- Hazard Identification
- Risk Assessment
- Risk Control Option Analysis
- Risk Control Decisions
- Risk Control Implementation
- Supervision and Review

### 1.1 PRIMARY HAZARD IDENTIFICATION TOOLS

The seven described in this appendix are considered the basic set of hazard identification tools to be applied on a day-to-day basis in organizations at all levels. These tools have been chosen for the following reasons:

They are simple to use, though they require some training.

They have been proven effective.

Widespread application has demonstrated they can and will be used by operators and will consistently be perceived as positive.

As a group, they complement each other, blending the intuitive and experiential with the more structured and rigorous.

They are well supported with worksheets and job aids.

In an organization with a mature ORM culture, the use of these tools by all personnel will be regarded as the natural course of events. The norm will be “Why would I even consider exposing myself and others to the risks of this activity before I have identified the hazards involved using the best procedures or designs available?” The following pages describe each tool using a standard format with models and examples.

#### 1.1.1 THE OPERATIONS ANALYSIS AND FLOW DIAGRAM

**FORMAL NAME:** The Operations Analysis

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

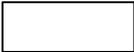
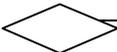
**PURPOSE:** The Operations Analysis (OA) provides an itemized sequence of events or a flow diagram depicting the major events of an operation. This assures that all elements of the operation are evaluated as potential sources of risk. This analysis overcomes a major weaknesses of traditional risk management, which tends to focus effort on one or two aspects of an operation that are intuitively identified as risky, often to the exclusion of other aspects that may actually be riskier. The Operations Analysis also guides the allocation of risk management resources over time as an operation unfolds event by event in a systematic manner.

FAA System Safety Handbook, Appendix F  
December 30, 2000

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

**METHOD:** Whenever possible, the Operations Analysis is taken directly from the planning of the operation. It is difficult to imagine planning an operation without identifying the key events in a time sequence. If for some reason such a list is not available, the analyst creates it using the best available understanding of the operation. The best practice is to break down the operation into time-sequenced segments strongly related by tasks and activities. Normally, this is well above the detail of individual tasks. It may be appropriate to break down aspects of an operation that carry obviously higher risk into more detail than less risky areas. The product of an OA is a compilation of the major events of an operation in sequence, with or without time checks. An alternative to the Operations Analysis is the flow diagram. Commonly used symbols are provided at Figure 1.1.1A. Putting the steps of the process on index cards or sticky-back note paper allows the diagram to be rearranged without erasing and redrawing, thus encouraging contributions.

**Figure 1.1.1A Example Flow Chart Symbols**

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

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

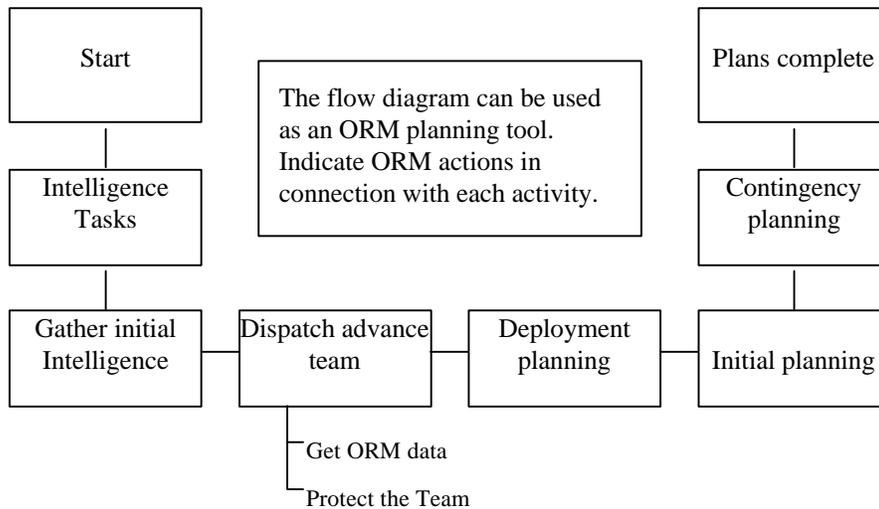
**COMMENTS:** Look back on your own experience. How many times have you been surprised or seen others surprised because they overlooked possible sources of problems? The OA is the key to minimizing this source of accidents.

### THE PLANNING PHASE

- Initial Intelligence Received (Maps, Facility Lists, Environment, Etc.)
- Advance Party Dispatched
- Advance Party Data Received
- Deployment Planning Underway
- Deployment Preparations Initiated
- Initial Operation Planning Underway
- Contingency Planning Underway

If more detail and more structured examination of the operational flow are desired, the flow diagram can be used. This diagram will add information through the use of graphic symbols. A flow diagram of the planning phase above might be developed as illustrated in Figure 1.1.1B below.

**Figure 1.1.1B Example Flow Diagram**



### 1.1.2 THE PRELIMINARY HAZARD ANALYSIS

**FORMAL NAME:** Preliminary Hazard Analysis

**ALTERNATIVE NAMES:** The PHA, the PHL

**PURPOSE:** The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep. The key idea of the PHA is to consider the risk inherent to every aspect of an operation. The PHA helps overcome the tendency to focus immediately on risk in one aspect of an operation, sometimes at the expense of overlooking more serious issues elsewhere in the operation. The PHA will often serve as the hazard identification process when risk is low or routine. In higher risk operations, it serves to focus and prioritize follow-on hazard analyses by displaying the full range of risk issues.

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

**METHOD:** The PHA is usually based on the Operations Analysis or flow diagram, taking each event in turn from it. Analysts apply their experience and intuition, use reference publications and standards of various kinds, and consult with personnel who may have useful input. The extent of the effort is dictated by resource and time limitations, and by the estimate of the degree of overall risk inherent in the operation. Hazards that are detected are often listed directly on a copy of the Operations Analysis as shown at Figure 1.1.2A. Alternatively, a more formal PHA format such as the worksheet shown at Figure 1.1.2B can be used. Operations Analysis. The completed PHA is used to identify hazards requiring more in-depth hazard identification or it may lead directly to the remaining five steps of the ORM process, if

FAA System Safety Handbook, Appendix F  
December 30, 2000

hazard levels are judged to be low. Key to the effectiveness of the PHA is assuring that all events of the operation are covered.

**Figure 1.1.2A Building the PHA directly From the Operations Analysis Flow Diagram**

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

**RESOURCES:** The two key resources for the PHA are the expertise of personnel actually experienced in the operation and the body of regulations, standards, and instructions that may be available. The PHA can be accomplished in small groups to broaden the List the operational phases vertically down the page. Be sure to leave plenty of space on the worksheet between each phase to allow several hazards to be noted for each phase. List the hazards noted for each operational phase. Strive for detail within the limits imposed by time. A copy of a PHA accomplished for an earlier similar operation would aid in the process.

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

**EXAMPLES:** The following (Figure 1.1.2B) is an example of a PHA.

**Figure 1.1.2B Example PHA**

<b>MOVING A HEAVY PIECE OF EQUIPMENT</b>	
<p>The example below uses an operation analysis for moving a heavy piece of equipment as the start point and illustrates the process of building the PHA direct from the Operations Analysis.            Operation: Move a 3-ton machine from one building to another.            Start Point: The machine is in its original position in building A            End Point: The machine is in its new position in building B</p>	
<b>ACTIVITY / EVENT</b>	<b>HAZARD</b>
Raise the machine to permit positioning of the forklift	Machine overturns due to imbalance Machine overturns due to failure of lifting device Machine drops on person or equipment due to failure of lifting device or improper placement (person lifting device) Machine strikes overhead obstacle Machine is damaged by the lifting process
Position the forklift	Forklift strikes the machine Forklift strikes other items in the area
Lift the machine	Machine strikes overhead obstacle Lift fails due to mechanical failure (damage to machine, objects, or people) Machine overturns due to imbalance
Move machine to the truck	Instability due to rough surface or weather condition Operator error causes load instability The load shifts
Place machine on the truck	Improper tiedown produces instability Truck overloaded or improper load distribution
Drive truck to building B	Vehicle accident during the move Poor driving technique produces instability Instability due to road condition
Remove machine from the truck	Same factors as "Move it to the truck"
Place machine in proper position in building B	Same factors as "Raise the machine" except focused on lowering the machine

### 1.1.3 THE "WHAT IF" TOOL

**FORMAL NAME:** The "What If" tool

**ALTERNATIVE NAMES:** None.

FAA System Safety Handbook, Appendix F  
December 30, 2000

**PURPOSE:** The "What If" tool is one of the most powerful hazard identification tools. As in the case of the Scenario Process tool, it is designed to add structure to the intuitive and experiential expertise of operational personnel. The "What If" tool is especially effective in capturing hazard data about failure modes that may create hazards. It is somewhat more structured than the PHA. Because of its ease of use, it is probably the single most practical and effective tool for use by operational personnel.

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

**METHOD:** Ensure that participants have a thorough knowledge of the anticipated flow of the operation. Visualize the expected flow of events in time sequence from the beginning to the end of the operation. Select a segment of the operation on which to focus. Visualize the selected segment with "Murphy" injected. Make a conscious effort to visualize hazards. Ask, "what if various failures occurred or problems arose"? Add hazards and their causes to your hazard list and assess them based on probability and severity.

The "What-If" analysis can be expanded to further explore the hazards in an operation by developing short scenarios that reflect the worst credible outcome from the compound effects of multiple hazards in the operation.

Follow these guidelines in writing scenarios:

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

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

**COMMENTS:** The "What If" tool is so effective that the Occupational Safety and Health Administration (OSHA) has designated as it one of six tools from among which activities facing catastrophic risk situations must choose under the mandatory hazard analysis provisions of the process safety standard.

**EXAMPLES:** Following (Figure 1.1.3A) is an extract from the typical output from the "What If" tool.

Figure 1.1.3A Example What If Analysis

<p>Situation: Picture a group of 3 operational employees informally applying the round robin procedure for the "What If" tool to a task to move a multi-ton machine from one location to another. A part of the discussion might go as follows:</p>
<p><u>Joe</u>: What if the machine tips over and falls breaking the electrical wires that run within the walls behind it?  <u>Bill</u>: What if it strikes the welding manifolds located on the wall on the West Side? (<i>This illustrates "piggybacking" as Bill produces a variation of the hazard initially presented by Joe.</i>)  <u>Mary</u>: What if the floor fails due to the concentration of weight on the base of the lifting device?  <u>Joe</u>: What if the point on the machine used to lift it is damaged by the lift?  <u>Bill</u>: What if there are electrical, air pressure hoses, or other attachments to the machine that are not properly neutralized?  <u>Mary</u>: What if the lock out/tag out is not properly applied to energy sources servicing the machine? <i>And so on....</i></p>
<p>Note: The list above for example might be broken down as follows:</p> <p>Group 1: Machine falling hazards  Group 2: Weight induced failures  Group 3: Machine disconnect and preparation hazards</p> <p>These related groups of hazards are then subjected to the remaining five steps of the ORM process.</p>

#### 1.1.4 THE SCENARIO PROCESS TOOL

**FORMAL NAME:** The Scenario Process tool

**ALTERNATIVE NAMES:** The mental movie tool.

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

**APPLICATION:** The Scenario Process tool should be used in most hazard identification applications, including some time-critical applications. In the time-critical mode, it is indeed one of the few practical

FAA System Safety Handbook, Appendix F  
December 30, 2000

tools, in that the user can quickly form a “mental movie” of the flow of events immediately ahead and the associated hazards.

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

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

**RESOURCES:** The key resource for the Scenario Process tool is the Operations Analysis. It provides the script for the flow of events that will be visualized. Using the tool does not require a specialist. Operational personnel leading or actually performing the task being assessed are key resources for the OA. Using this tool is often entertaining, dynamic and often motivates even the most junior personnel in the organization.

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

**EXAMPLES.** Following is an example (Figure 1.1.4A) of how the Scenario Process tool might be used in an operational situation.

Figure 1.1.4A Example Machine Movement Scenario

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

### 1.1.5 THE LOGIC DIAGRAM

**FORMAL NAME:** The Logic Diagram

**ALTERNATIVE NAMES:** The Logic Tree

**PURPOSE:** The Logic Diagram is intended to provide considerable structure and detail as a primary hazard identification procedure. Its graphic structure is an excellent means of capturing and correlating

FAA System Safety Handbook, Appendix F  
December 30, 2000

the hazard data produced by the other primary tools. Because of its graphic display, it can also be an effective hazard-briefing tool. The more structured and logical nature of the Logic Diagram adds substantial depth to the hazard identification process to complement the other more intuitive and experiential tools. Finally, an important purpose of the Logic Diagram is to establish the connectivity and linkages that often exist between hazards. It does this very effectively through its tree-like structure.

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

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

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

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

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

All of the various Logic Diagram options can be applied either to an actual operating system or one being planned. Of course, the best time for application is in the planning stages of the operational lifecycle. All of the Logic Diagram options begin with a top block. In the case of the positive diagram, this is a desired outcome; in the case of the event diagram, this is an operations event or contingency possibility; in the case of the negative diagram, it is a loss event. When working with positive diagram or negative diagram, the user then, reasons out the factors that could produce the top event. These are entered on the next line of blocks. With the event diagram, the user lists the possible results of the event being analyzed. The conditions that could produce the factors on the second line are then considered and they are entered on the third line. The goal is to be as logical as possible when constructing Logic Diagrams, but it is more important to keep the hazard identification goal in mind than to construct a masterpiece of logical thinking. Therefore, a Logic Diagram should be a worksheet with lots of changes and variations marked on it. With the addition of a chalkboard or flip chart, it becomes an excellent group tool.

Figure 1.1.5A below is a generic diagram, and it is followed by a simplified example of each of the types of Logic Diagrams (Figures 1.1.5B, 1.1.5C, 1.1.5D).

Figure 1.1.5A Generic Logic Diagram

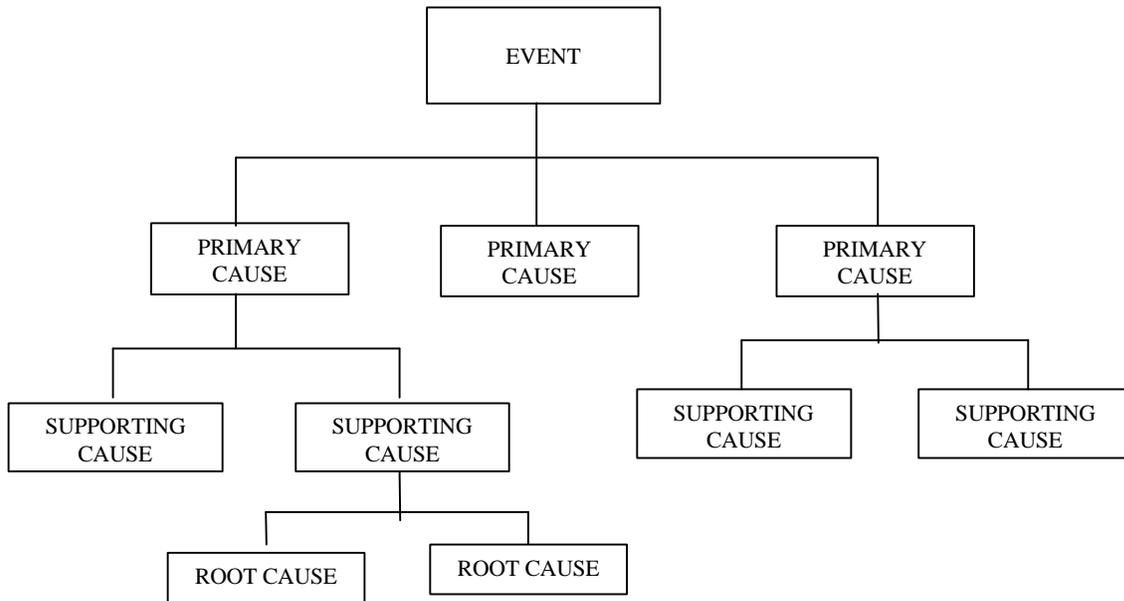
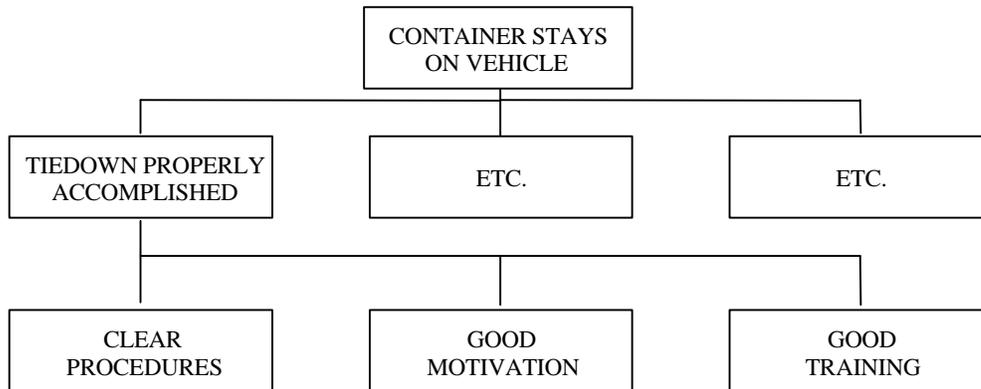
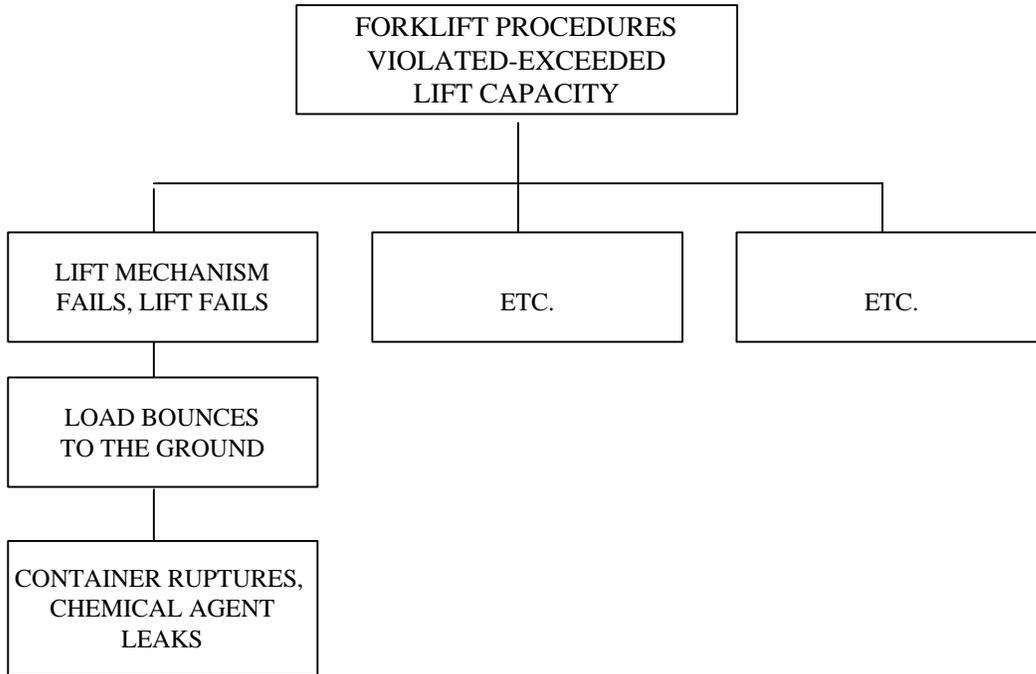


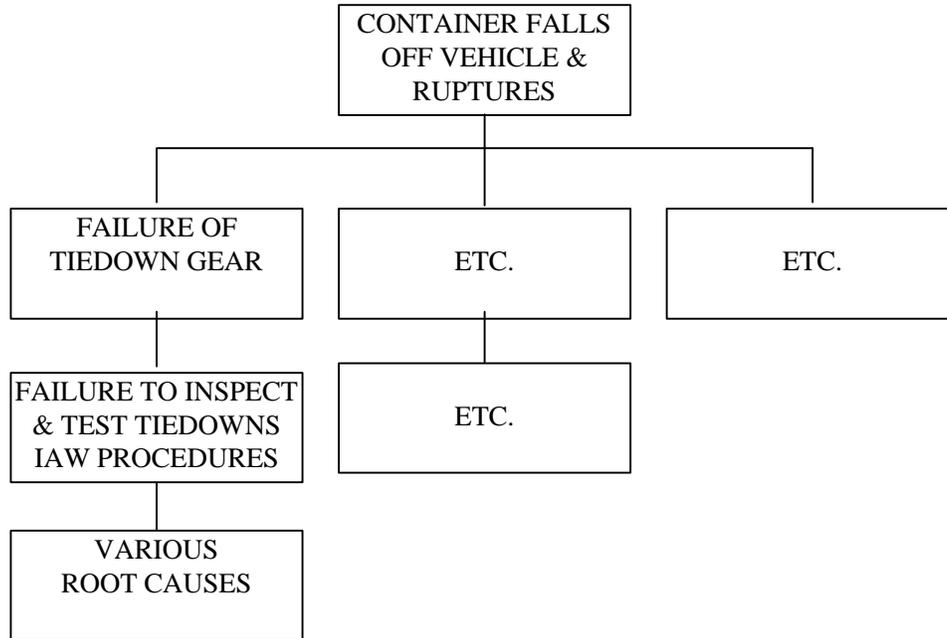
Figure 1.1.5B Positive Event Logic Diagram



**Figure 1.1.5C Risk Event Diagram**



**Figure 1.1.5D Negative Event Logic Diagram**

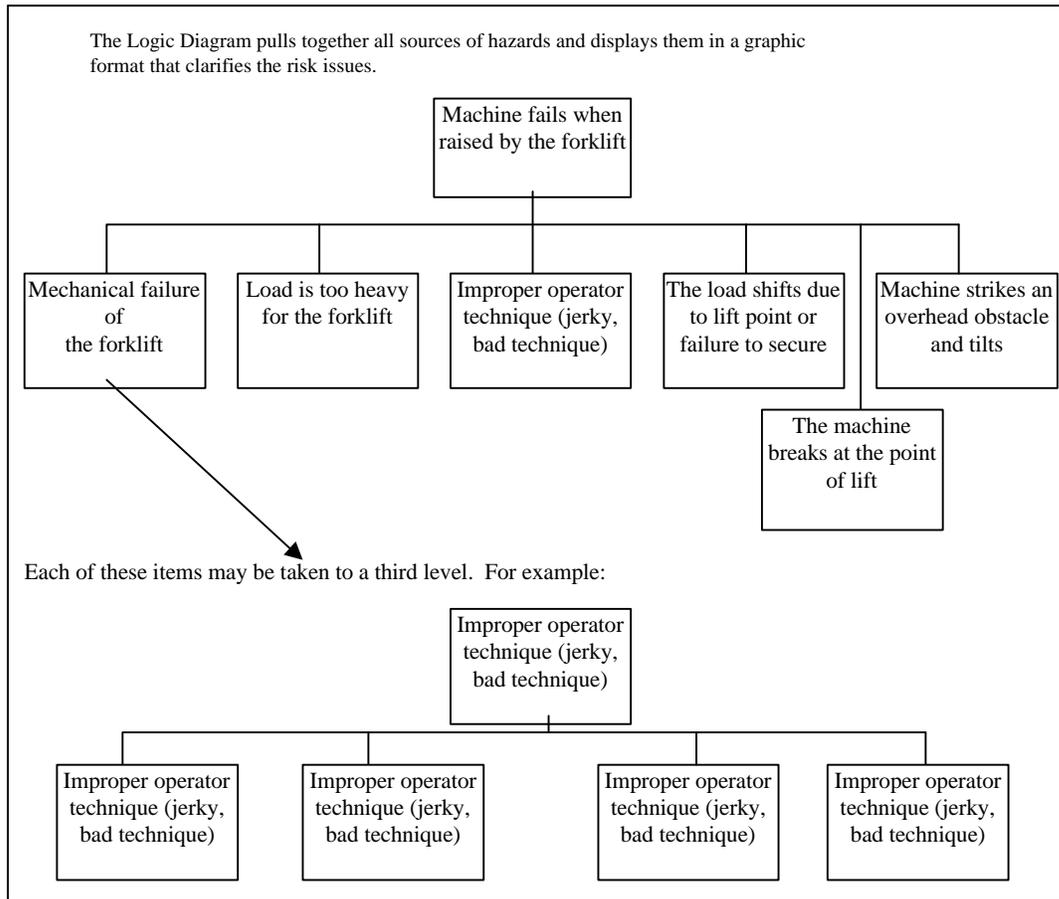


**RESOURCES:** All of the other primary tools are key resources for the Logic Diagram, as it can correlate hazards that they generate. If available, a safety professional may be an effective facilitator for the Logic Diagram process.

**COMMENTS:** The Logic Diagram is the most comprehensive tool available among the primary procedures. Compared to other approaches to hazard identification, it will substantially increase the quantity and quality of hazards identified.

**EXAMPLE:** Figure 1.1.5E illustrates how a negative diagram could be constructed for moving a heavy piece of equipment.

Figure 1.1.5E Example Negative Diagram



### 1.1.6 THE CHANGE ANALYSIS

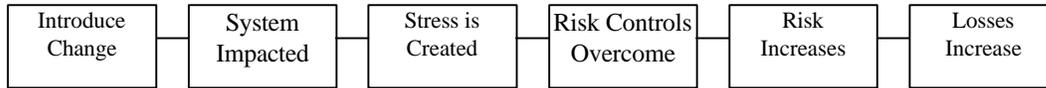
**FORMAL NAME:** The Change Analysis

**ALTERNATIVE NAMES:** None

**PURPOSE:** Change is an important source of risk in operational processes.

Figure 1.1.6A illustrates this causal relationship.

**Figure 1.1.6A Change Causation**



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

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

Whenever significant changes are planned in operations in which there is significant operational risk of any kind. An example is the decision to conduct a certain type of operation at night that has heretofore only been done in daylight.

Periodically in any important operation, to detect the occurrence of unplanned changes.

As an accident investigation tool.

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

**METHOD:** The Change Analysis is best accomplished using a format such as the sample worksheet shown at Figure 1.1.6B. The factors in the column on the left side of this tool are intended as a comprehensive change checklist.

**Figure 1.1.6B Sample Change Analysis Worksheet**

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

FAA System Safety Handbook, Appendix F  
December 30, 2000

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

**COMMENTS:** In organizations with mature ORM processes, most, if not all, higher risk activities will have been subjected to thorough ORM applications and the resulting risk controls will have been incorporated into operational guidance. In these situations, the majority of day-to-day ORM activity will be the application of Change Analysis to determine if the operation has any unique aspects that have not been previously analyzed.

### 1.1.7 THE CAUSE AND EFFECT TOOL

**FORMAL NAME:** The Cause and Effect Tool

**ALTERNATIVE NAMES:** The cause and effect diagram. The fishbone tool, the Ishikawa Diagram

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

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

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

**RESOURCES:** There are many publications describing in great detail how to use cause and effect diagrams.<sup>1</sup>

**COMMENTS:**

**EXAMPLES:** An example of Cause and Effect Tool in action is illustrated at Figure 1.1.7A.

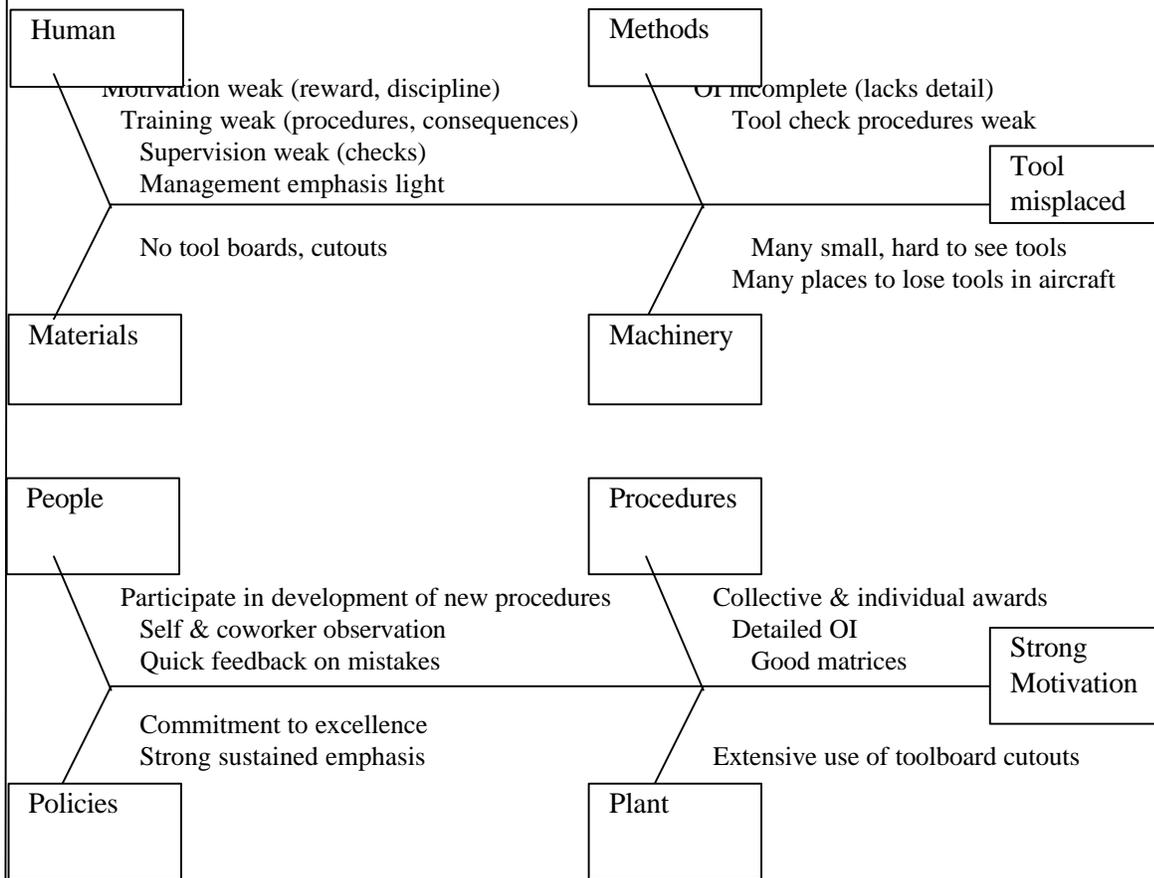
---

<sup>1</sup> K. Ishikawa, Guide to Quality Control, Quality Resources, White Plains, New York, 12<sup>th</sup> Printing 1994.

**Figure 1.1.7 Example of Cause and Effect**

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

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



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

## 1.2 THE SPECIALTY HAZARD IDENTIFICATION TOOLS

The tools that follow are designed to augment the primary tools described in part 1.1. These tools have several advantages:

FAA System Safety Handbook, Appendix F  
December 30, 2000

They can be used by nearly everyone in the organization, though some may require either training or professional facilitation.

Each tool provides a capability not fully realized in any of the primary tools.

They use the tools of the less formal safety program to support the ORM process.

They are well supported with forms, job aids, and models.

Their effectiveness has been proven. In an organization with a mature ORM process, all personnel will be aware of the existence of these specialty tools and capable of recognizing the need for their application. While not everyone will be comfortable using every procedure, a number of people within the organization will have experience applying one or another of them.

### 1.2.1 THE HAZARD AND OPERABILITY TOOL

**FORMAL NAME:** The Hazard and Operability Tool

**ALTERNATIVE NAMES:** The HAZOP analysis

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

**APPLICATION:** The HAZOP should be considered when a completely new process or procedure is going to be undertaken. The issue should be one where there is significant risk because the HAZOP does demand significant expenditure of effort and may not be cost effective if used against low risk issues. The HAZOP is also useful when an operator or leader senses that "something is wrong" but they can't identify it. The HAZOP will dig very deeply into the operation and to identify what that "something" is.

**METHOD:** The HAZOP is the most highly structured of the hazard identification procedures. It uses a standard set of guide terms (Figure 1.1) which are then linked in every possible way with a tailored set of process terms (for example "flow"). The process terms are developed directly from the actual process or from the Operations Analysis. The two words together, for example "no" (a guideword) and "flow" (a process term) will describe a deviation. These are then evaluated to see if a meaningful hazard is indicated. If so, the hazard is entered in the hazard inventory for further evaluation. Because of its rigid process, the HAZOP is especially suitable for one-person hazard identification efforts.

**Figure 1.2.1A Standard HAZOP Guidewords**

NO	Note: This basic set of guidewords should be all that are needed for all applications. Nevertheless, when useful, specialized terms can be added to the list. In less complex applications only some of the terms may be needed.
MORE	
LESS	
REVERSE	
LATE	
EARLY	

FAA System Safety Handbook, Appendix F  
December 30, 2000

**RESOURCES:** There are few resources available to assist with HAZOP; none are really needed.

**COMMENTS:** The HAZOP is highly structured, and often time-consuming. Nevertheless, in its special role, this tool works very effectively. OSHA selected it for inclusion in the set of six mandated procedures of the OSHA process safety standard.

### 1.2.2 THE MAPPING TOOL

**FORMAL NAME:** The Mapping Tool

**ALTERNATIVE NAMES:** Map analysis

**PURPOSE:** The map analysis is designed to use terrain maps and other system models and schematics to identify both things at risk and the sources of hazards. Properly applied the tool will reveal the following:

Task elements at risk

The sources of risk

The extent of the risk (proximity)

Potential barriers between hazard sources and operational assets

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

**METHOD:** The Mapping Tool requires some creativity to realize its full potential. The starting point is a map, facility layout, or equipment schematic. The locations of hazard sources are noted. The easiest way to detect these sources is to locate energy sources, since all hazards involve the unwanted release of energy. Figure 1.2.2A lists the kinds of energy to look for. Mark the locations of these sources on the map or diagram. Then, keeping the operation in mind, locate the personnel, equipment, and facilities that the various potentially hazardous energy sources could impact. Note these potentially hazardous links and enter them in the hazard inventory for risk management.

**Figure 1.2.2A Major Types of Energy**

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

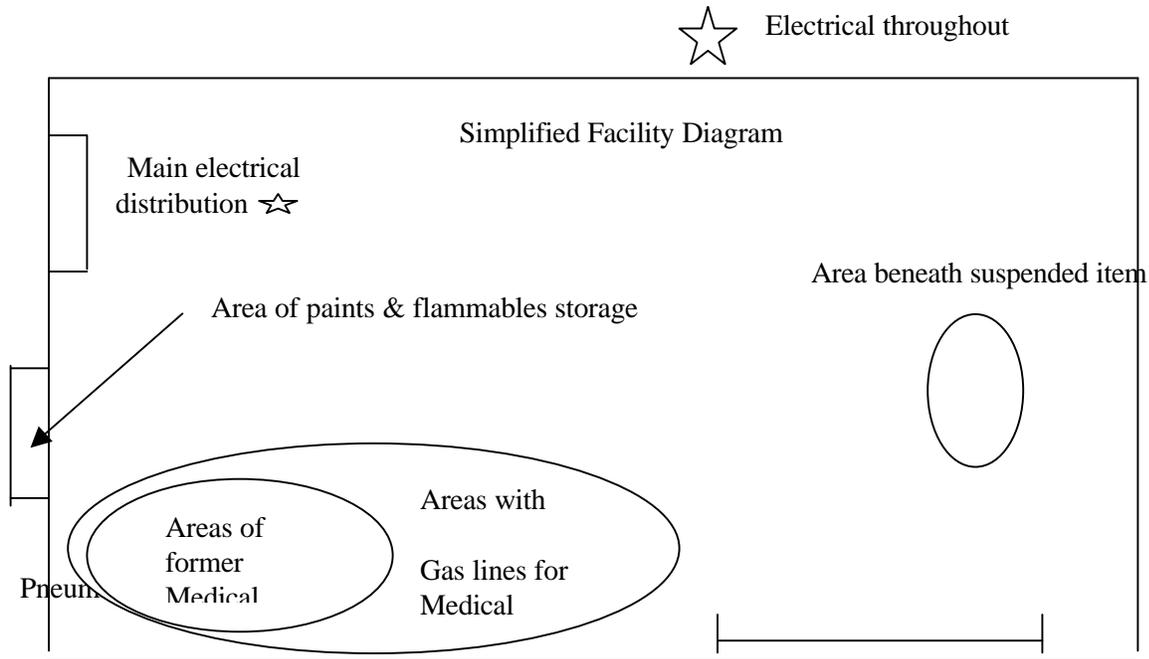
**RESOURCES:** Maps can convey a great deal of information, but cannot replace the value of an on-site assessment. Similarly, when working with an equipment schematic or a facility layout, there is no substitute for an on-site inspection of the equipment or survey of the facility.

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

**EXAMPLE:** The following example (Figure 1.2.2B) illustrates the use of a facility schematic that focuses on the energy sources there as might be accomplished in support of an Energy Trace and Barrier Analysis.

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

Figure 1.2.2B Example Map Analysis  
**FACILITY ENERGY SOURCES**



### 1.2.3 THE INTERFACE ANALYSIS

**FORMAL NAME:** The Interface Analysis

**ALTERNATIVE NAMES:** Interface Hazard Analysis

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

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

**METHOD:** The Interface Analysis is normally based on an outline such as the one illustrated at Figure 3.1. The outline provides a list of potential energy types and guides the consideration of the potential interactions. A determination is made whether a particular type of energy is present and then whether

FAA System Safety Handbook, Appendix F  
December 30, 2000

there is potential for that form of energy to adversely affect other activities. As in all aspects of hazard identification, the creation of a good Operations Analysis is vital.

**Figure 1.2.3A The Interface Analysis Worksheet**

<p>Energy Element Kinetic (objects in motion) Electromagnetic (microwave, radio, laser) Radiation (radioactive, x-ray) Chemical Other <b>Personnel Element:</b> Personnel moving from one area to another <b>Equipment Element:</b> Machines and material moving from one area to another Supply/materiel Element: Intentional movement from one area to another Unintentional movement from one area to another <b>Product Element:</b> Movement of product from one area to another <b>Information Element:</b> Flow of information from one area to another or interference (i.e. jamming) Bio-material Element Infectious materials (virus, bacteria, etc.) Wildlife Odors</p>
--

**RESOURCES:** Interface Analyses are best accomplished when personnel from all of the involved activities participate, so that hazards and interfaces in *both* directions can be effectively and knowledgeably addressed. A safety office representative can also be useful in advising on the types and characteristics of energy transfers that are possible.

**COMMENTS:** The lessons of the past indicate that we should give serious attention to use of the Interface Analysis. Nearly anyone who has been involved in operations for any length of time can relate stories of overlooked interfaces that have had serious adverse consequences.

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

FAA System Safety Handbook, Appendix F  
December 30, 2000

Figure 1.2.3B Example Interface Analysis

**SITUATION:** Construction of a heavy equipment maintenance facility is planned for the periphery of the complex at a major facility. This is a major complex costing over \$2,000,000 and requiring about eight months to complete. The objective is to detect interface issues in both directions. Notice that the analysis reveals a variety of interface issues that need to be thought through carefully.

**Energy Interface**

Movement of heavy construction equipment

Movement of heavy building supplies

Movement of heavy equipment for repair

Possible hazmat storage/use at the facility

**Personnel Interface**

Movement of construction personnel (vehicle or pedestrian) through base area

Movement of repair facility personnel through base area

Possible movement of base personnel (vehicular or pedestrian) near or through the facility

**Equipment Interface:** Movement of equipment as indicated above

**Supply Interface**

Possible movement of hazmat through base area

Possible movement of fuels and gases

Supply flow for maintenance area through base area

**Product Interface**

Movement of equipment for repair by tow truck or heavy equipment transport through the base area

**Information Interface**

Damage to buried or overhead wires during construction or movement of equipment

Possible Electro-magnetic interference due to maintenance testing, arcing, etc.

**Biomaterial Interface:** None

## 1.2.4 THE ACCIDENT/INCIDENT ANALYSIS

**FORMAL NAME:** The Accident/Incident Analysis

**ALTERNATIVE NAMES:** The accident analysis

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

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

FAA System Safety Handbook, Appendix F  
December 30, 2000

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

Typical factors to examine include the following:

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

**RESOURCES:** The analysis relies upon a relatively complete and accurate database. The FAA's system safety office (ASY) may have the needed data. That office can also provide assistance in the analysis process. System Safety personnel may have already completed analyses of similar activities or may be able to suggest the most productive areas for initial analysis.

**COMMENTS:** The data in databases has been acquired the hard way - through the painful and costly mistakes of hundreds of individuals. By taking full advantage of this information the analysis process can be more realistic, efficient, and thorough and thereby preventing the same accidents (incidents?) from occurring over and over again.

### 1.2.5 THE INTERVIEW TOOL

**FORMAL NAME:** The Interview Tool

**ALTERNATIVE NAMES:** None

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

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

**METHOD:** The Interview Tool's great strength is versatility. Figure 1.2.5A illustrates the many options available to collect interview data. Key to all of these is to create a situation in which interviewees feel free to honestly report what they know, without fear of any adverse consequences. This means absolute confidentiality must be assured, by not using names in connection with data.

**Figure 1.2.5A Interview Tool Alternatives**

<ul style="list-style-type: none"> <li>Direct interviews with operational personnel</li> <li>Supervisors interview their subordinates and report results</li> <li>Questionnaire interviews are completed and returns</li> <li>Group interview sessions (several personnel at one time)</li> <li>Hazards reported formally</li> <li>Coworkers interview each other</li> </ul>
--

FAA System Safety Handbook, Appendix F  
December 30, 2000

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

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

**EXAMPLES:** Figure 1.2.5B illustrates several variations of the Interview Tool.

Figure 1.2.5B Example Exit Interview Format

Name (optional) _____	Organization _____
<p>1. Describe below incidents, near misses or close calls that you have experienced or seen since you have been in this organization. State the location and nature (i.e. what happened and why) of the incident. If you can't think of an incident, then describe two hazards you have observed.</p> <p><b>INCIDENT 1: Location:</b> _____ What happened and why? _____</p> <p>_____</p> <p><b>INCIDENT 2: Location:</b> _____ What happened and why? _____</p> <p>_____</p> <p>2. What do you think other personnel can do to eliminate these problems?</p> <p><b>Personnel:</b> _____</p> <p>Incident 1 _____</p> <p>Incident 2 _____</p> <p><b>Supervisors:</b> _____</p> <p>Incident 1 _____</p> <p>Incident 2 _____</p> <p><b>Top Leadership:</b> _____</p> <p>Incident 1 _____</p> <p>Incident 2 _____</p>	

FAA System Safety Handbook, Appendix F  
December 30, 2000

### 1.2.6 THE INSPECTION TOOL

**FORMAL NAME:** The Inspection Tool

**ALTERNATIVE NAMES:** The survey tool

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

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

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

**RESOURCES:** There are many inspection criteria, checklists and related job aids available commercially. Many have been tailored for specific types of organizations and activities. The System Safety Office can be a valuable resource in the development of criteria and can provide technical support in the form of interpretations, procedural guidance, and correlation of data.

**COMMENTS:** Inspections and surveys have long track records of success in detecting hazards and reducing risk. However, they have been criticized as being inconsistent with modern management practice because they are a form of “downstream” quality control. By the time a hazard is detected by an inspection, it may already have caused loss. The ORM approach to inspections emphasizes focus on the

FAA System Safety Handbook, Appendix F  
December 30, 2000

higher risks within the organization and emphasizes the use of management and safety program surveys that detect the underlying causes of hazards, rather than the hazards themselves.

**EXAMPLES:** Conventional inspections normally involve seeking and recording unsafe acts or conditions. The number of these may reflect either the number of unsafe acts or conditions occurring in the organization or the extent of the effort extended to find hazards. Thus, conventional inspections are not a reliable indicator of the extent of risk. To change the nature of the process, it is often only necessary to record the total number of observations made of key behaviors, then determine the number of unsafe behaviors. This yields a rate of “unsafeness” that is independent of the number of observations made.

### 1.2.7 THE JOB HAZARD ANALYSIS

**FORMAL NAME:** The Job Hazard Analysis

**ALTERNATIVE NAMES:** The task analysis, job safety analysis, JHA, JSA

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

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

The JHA is best accomplished using an outline similar to the one illustrated at Figure 1.2.7A. As shown in the illustration, the job is broken down into its individual steps. Jobs that involve many quite different tasks should be handled by analyzing each major task separately. The illustration considers risks both to the workers involved, and to the system, as well as. Risk controls for both. Tools such as the Scenario and "What If" tools can contribute to the identification of potential hazards. There are two alternative ways to accomplish the JHA process. A safety professional can complete the process by asking questions of the workers and supervisors involved. Alternatively, supervisors could be trained in the JHA process and directed to analyze the jobs they supervise.

FAA System Safety Handbook, Appendix F  
December 30, 2000

**Figure 1.2.7A Sample Job Hazard Analysis Format**

Job Safety Analysis	Job Title or Operation		Page of ISA Number
	Job Series/AFSC		Supervisor
Organization Symbol	Location/Building Number	Shop Title	Reviewed By
Required and/or Recommended Personal Protective Equipment			Approved By
SEQUENCE OF BASIC JOB STPES	POTENTIAL HAZARDS USAFE ACTS OR CONDITIONS	RECOMMENDED ACTION OR PROCEDURE	

**RESOURCES:** The System Safety Office has personnel trained in detail in the JHA process who can serve as consultants, and may have videos that walk a person through the process.

**COMMENTS:** The JHA is risk management. The concept of completing in-depth hazard assessments of all jobs involving significant risk with the active participation of the personnel doing the work is an ideal model of ORM in action.

FAA System Safety Handbook, Appendix F  
December 30, 2000

## 1.2.8 THE OPPORTUNITY ASSESSMENT

**FORMAL NAME:** The Opportunity Assessment

**ALTERNATIVE NAMES:** The opportunity-risk tool

**PURPOSE:** The Opportunity Assessment is intended to identify opportunities to expand the capabilities of the organization and/or to significantly reduce the operational cost of risk control procedures. Either of these possibilities means expanded capabilities.

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

**METHOD:** The Opportunity Assessment involves five key steps as outlined at Figure 1.2.10A. In Step 1, operational areas that would benefit substantially from expanded capabilities are identified and prioritized. Additionally, areas where risk controls are consuming extensive resources or are otherwise constraining operation capabilities are listed and prioritized. Step 2 involves the analysis of the specific risk-related barriers that are limiting the desired expanded performance or causing the significant expense. This is a critical step. Only by identifying the risk issues precisely can focused effort be brought to bear to overcome them. Step 3 attacks the barriers by using the risk management process. This normally involves reassessment of the hazards, application of improved risk controls, improved implementation of existing controls, or a combination of these options. Step 4 is used when available risk management procedures don't appear to offer any breakthrough possibilities. In these cases the organization must seek out new

ORM tools using benchmarking procedures or, if necessary, innovate new procedures. Step 5 involves the exploitation of any breakthroughs achieved by pushing the operational limits or cost saving until a new barrier is reached. The cycle then repeats and a process of continuous improvement begins.

### Figure 1.2.9A Opportunity Analysis Steps

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

**RESOURCES:** The Opportunity Assessment depends upon a detailed understanding of operational processes so that barriers can be identified. An effective Opportunity Assessment will necessarily involve operations experts.

### 1.3 THE ADVANCED HAZARD IDENTIFICATION TOOLS

The five tools that follow are advanced hazard identification tools designed to support strategic hazard analysis of higher risk and critical operations. These advanced tools are often essential when in-depth hazard identification is needed. They provide the mechanism needed to push the limits of current hazard identification technology. For example, the Management Oversight and Risk Tree (MORT) represents the full-time efforts of dozens of experts over decades to fully develop an understanding of all of the sources of hazards.

As might be expected, these tools are complex and require significant training to use. Full proficiency also requires experience in using them. They are best reserved for use by, loss control professionals. Those with an engineering, scientific, or other technical background are certainly capable of using these tools with a little read-in. Even though professionals use the tools, much of the data that must be fed into the procedures must come from operators.

In an organization with a mature ORM culture, all personnel in the organization will be aware that higher risk justifies more extensive hazard identification. They will feel comfortable calling for help from loss control professionals, knowing that these individuals have the advanced tools needed to cope with the most serious situations. These advanced tools will play a key role in the mature ORM culture in helping the organization reach its hazard identification goal: No significant hazard undetected.

#### 1.3.1 THE ENERGY TRACE AND BARRIER ANALYSIS

**FORMAL NAME:** The Energy Trace and Barrier Analysis

**ALTERNATIVE NAMES:** Abnormal energy exchange

**PURPOSE:** The Energy Trace and Barrier Analysis (ETBA) is a procedure intended to detect hazards by focusing in detail on the presence of energy in a system and the barriers for controlling that energy. It is conceptually similar to the Interface Analysis in its focus on energy forms, but is considerably more thorough and systematic.

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

**METHOD:** The ETBA involves 5 basic steps as shown at Figure 1.3.1A.

Step 1 is the identification of the types of energy found in the system. It often requires considerable expertise to detect the presence of the types of energy listed at Figure 1.3.1B.

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

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

In Step 4 the risk of barrier failure and the unwanted release of the energy are assessed. Finally, in Step 5, risk control options are considered and selected.

**Figure 1.3.1A ETBA Steps**

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

**Figure 1.3.1B Types of Energy**

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

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

**COMMENTS:** Most accidents involve the unwanted release of one kind of energy or another. This fact makes the ETBA a powerful hazard identification tool. When the risk stakes are high and the system is complex, the ETBA is a must have.

**EXAMPLES:** A simplified example of the ETBA procedure is provided at Figure 1.3.

**Figure 1.3.1C Example ETBA**

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

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

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

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

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

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

FAA System Safety Handbook, Appendix F  
December 30, 2000

### **1.3.2 THE FAULT TREE ANALYSIS**

**FORMAL NAME:** The Fault Tree Analysis

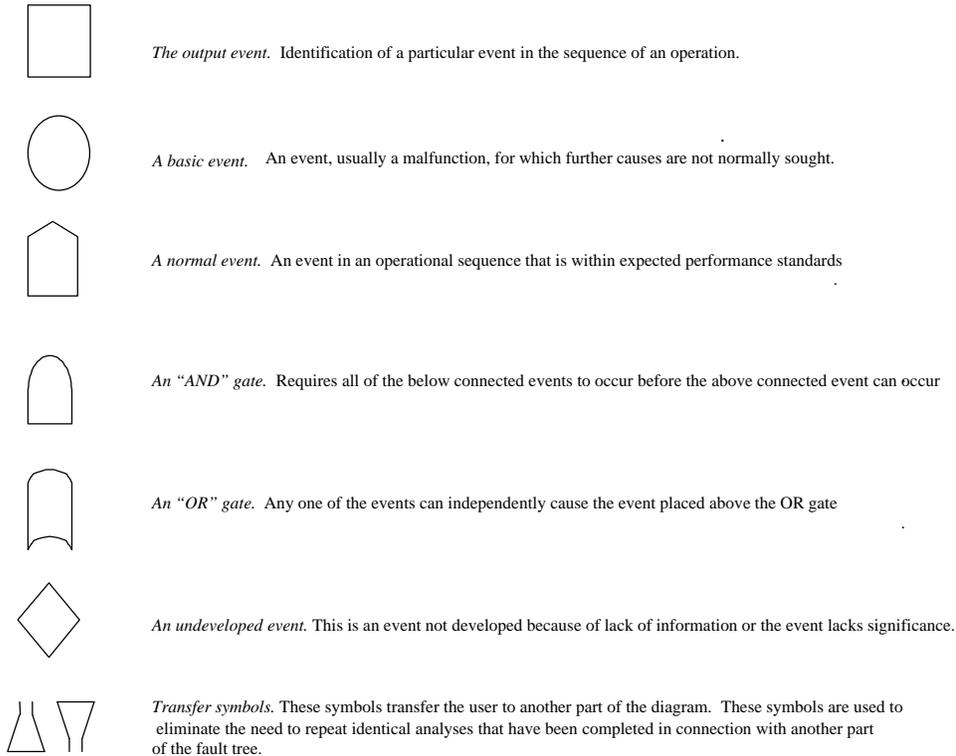
**ALTERNATIVE NAMES:** The logic tree

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

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

**METHOD:** The FTA is constructed exactly like a negative Logic Diagram except that the symbols depicted in Figure 1.3.2A are used.

**Figure 1.3.2A Key Fault Tree Analysis Symbols**

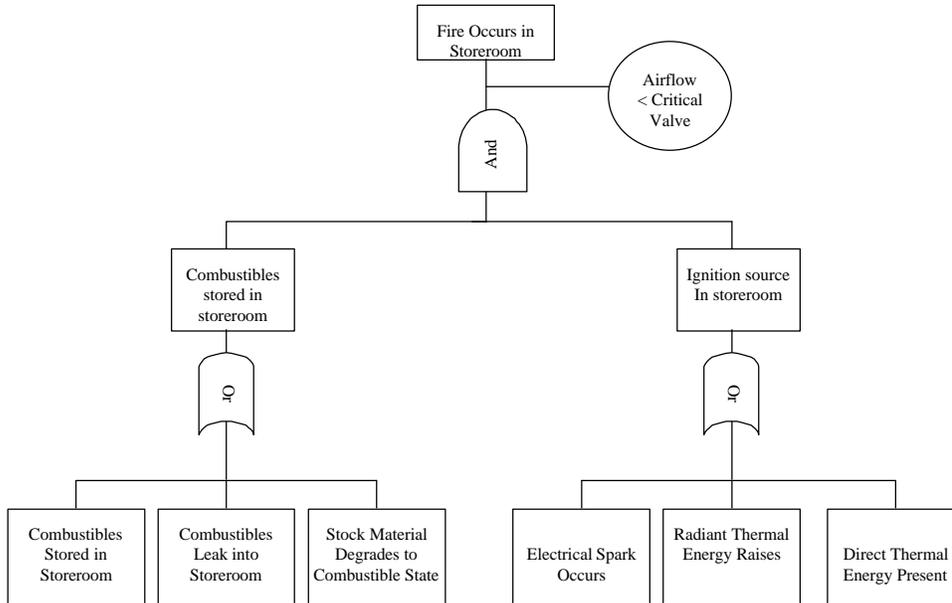


**RESOURCES:** The System Safety Office is the best source of information regarding Fault Tree Analysis. Like the other advanced tools, the FTA will involve the consultation of a safety professional or engineer trained in the use of the tool. If the probabilistic aspects are added, it will also require a database capable of supplying the detailed data needed.

**COMMENTS:** The FTA is one of the few hazard identification procedures that will support quantification when the necessary data resources are available.

**EXAMPLE:** A brief example of the FTA is provided at Figure 1.3.2B. It illustrates how an event may be traced to specific causes that can be very precisely identified at the lowest levels.

**Figure 1.3.2B Example of Fault Tree Analysis**



### 1.3.3 THE FAILURE MODES AND EFFECTS ANALYSIS

**FORMAL NAME:** The Failure Modes and Effects Analysis

**ALTERNATIVE NAMES:** The FMEA

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

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

FAA System Safety Handbook, Appendix F  
December 30, 2000

**METHOD:** The FMEA uses a worksheet similar to the one illustrated at Figure 1.3.3A. As noted on the sample worksheet, a specific component of the system to be analyzed is identified. Several components can be analyzed. For example, a rotating part might freeze up, explode, breakup, slow down, or even reverse direction. Each of these failure modes may have differing impacts on connected components and the overall system. The worksheet calls for an assessment of the probability of each identified failure mode.

**Figure 1.3.3A Sample Failure Mode and Effects Analysis Worksheet**

FAILURE MODES AND EFFECTS ANALYSIS						
Page ___ of ___ Pages						
System _____				Date _____		
Subsystem _____				Analyst _____		
Component Description	Failure Mode	Effects on Other Components	Effects On System	RAC or Hazard Category	Failure Frequency Effects Probability	Remarks

**RESOURCES:** The best source of more detailed information on the FMEA is the System Safety Office.

**EXAMPLES:** An example of the FMEA is provided at Figure 1.3.3B.

**Figure 1.3.3B Example FMEA**

Situation: The manager of a major facility is concerned about the possible impact of the failure of the landline communications system that provides the sole communications capability at the site. The decision is made to do a Failure Modes and Effects Analysis. An extract from the resulting FMEA is shown below.						
Component	Function	Failure Mode & Cause	Failure Effect on Higher Item	System	Probability	Corrective Action
Landline Wire	Comm	Cut-natural cause, falling tree, etc.	Comm system down	Cease Fire	Probable	Clear natural obstacle from around wires

FAA System Safety Handbook, Appendix F  
December 30, 2000

Wire		Cut-unrelated operational activities	Comm system down	Cease Fire	Probable	Warn all operations placement of wire
Wire		Line failure	Comm system down	Cease Fire	Probable	Placement of wires Proper grounding
Wire		Cut – vandals & thieves	Comm system down	Cease Fire	Unlikely	Placement of wires Area security

### 1.3.4 THE MULTI-LINEAR EVENTS SEQUENCING TOOL

**FORMAL NAME:** The Multi-linear Events Sequencing Tool

**ALTERNATIVE NAMES:** The timeline tool, the sequential time event plot (STEP)<sup>2</sup>

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

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

**METHOD:** The MES uses a worksheet similar to the one illustrated at Figure 4.1. The sample worksheet displays the timeline of the operation across the top and the “actors” (people or things) down the left side. The flow of events is displayed on the worksheet, showing the relationship between the actors on a time basis. Once the operation is displayed on the worksheet, the sources of risk will be evident as the flow is examined.

<sup>2</sup> K. Hendrisk, and L. Benner, Investigating Accidents with Step, Marcel Dekker, New York, 1988.

Figure 1.3.4A Multi-linear Events Sequencing Form

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

**RESOURCES:** The best sources for more detailed information on the MES is the System Safety staff. As with the other advanced tools, using the MES will normally involve consultation with a safety professional familiar with its application.

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

### 1.3.5 THE MANAGEMENT OVERSIGHT AND RISK TREE

**FORMAL NAME:** The Management Oversight and Risk Tree

**ALTERNATIVE NAMES:** The MORT

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

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

**METHOD:** MORT is accomplished using the MORT diagrams, of which there are several levels available. The most comprehensive, with about 10,000 blocks, fills a book. There is an intermediate diagram with about 1500 blocks, and a basic diagram with about 300. It is possible to tailor a MORT diagram by choosing various branches of the tree and using only those segments. The MORT is essentially a negative tree, so the process begins by placing an undesired loss event at the top of the

FAA System Safety Handbook, Appendix F  
December 30, 2000

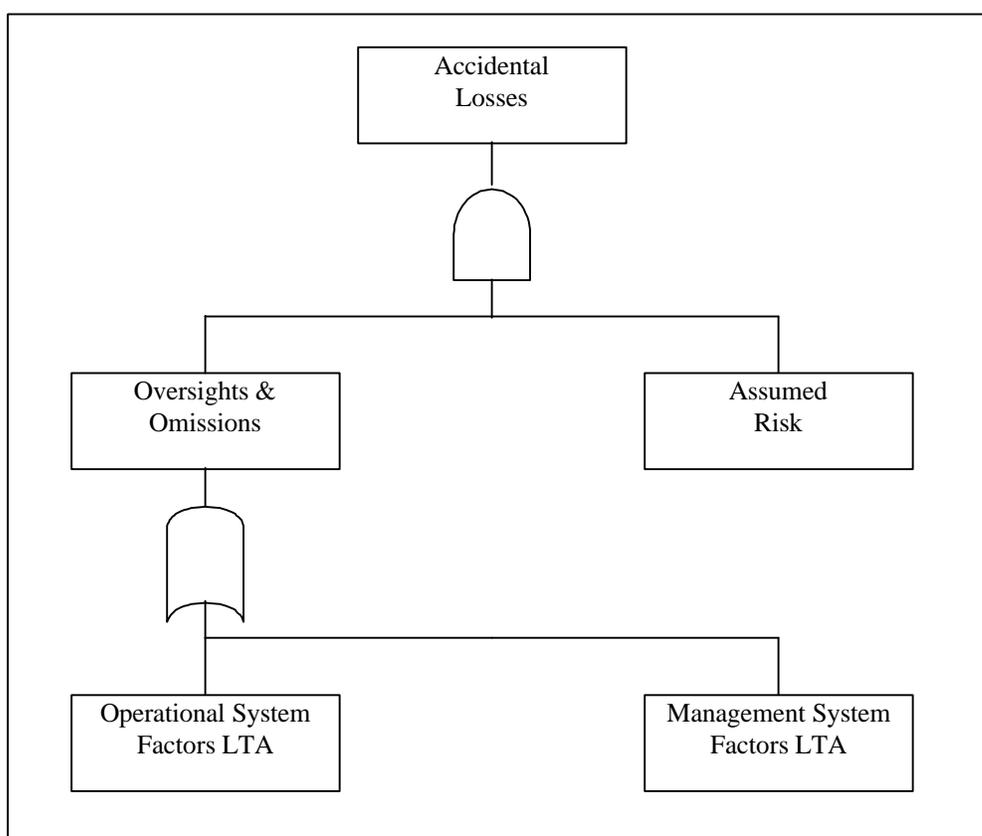
diagram used. The user then systematically responds to the issues posed by the diagram. All aspects of the diagram are considered and the “less than adequate” blocks are highlighted for risk control action.

**RESOURCES:** The best source of information on MORT is the System Safety Office.

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

**EXAMPLES:** The top blocks of the MORT diagram are displayed at Figure 1.3.5A.

Figure 1.3.5A Example MORT Section



## 2.0 RISK ASSESSMENT TOOLS, DETAILS, AND EXAMPLES

Introduction. This section contains an example of assessing risk, using a risk assessment matrix (Figure 2). The easiest way to understand the application of the matrix is to apply it. The reasoning used in constructing the matrix in the example below is provided.

FAA System Safety Handbook, Appendix F  
December 30, 2000

Example. The example below demonstrates the application of the matrix to the risk associated with moving a heavy piece of machinery.

Risk to be assessed: The risk of the machine falling over and injuring personnel.

Probability assessment: The following paragraphs illustrate the thinking process that might be followed in developing the probability segment of the risk assessment:

Use previous experience and the database, if available. “We moved a similar machine once before and although it did not fall over, there were some close calls. This machine is not as easy to secure as that machine and has a higher center of gravity and poses an even greater chance of falling. The base safety office indicates that there was an accident about 18 months ago that involved a similar operation. An individual received a broken leg in that case.”

Use the output of the hazard analysis process. “Our hazard analysis shows that there are several steps in the machine movement process where the machine is vulnerable to falling. Furthermore, there are several different types of contributory hazards that could cause the machine to fall. Both these factors increase the probability of falling.”

Consider expert opinion. “My experienced manager feels that there is a real danger of the machine falling”

Consider your own intuition and judgment. “My gut feeling is that there is a real possibility we could lose control of this machine and topple it. The fact that we rarely move machines quite like this one increases the probability of trouble.”

Refer to the matrix terms. “Hmmm, the decision seems to be between *likely* and *occasional*. I understand *likely* to mean that the machine is likely to fall, meaning a pretty high probability. Certainly there is a real chance it may fall, but if we are careful, there should be no problem. I am going to select *Occasional* as the best option from the matrix.”

Severity assessment. The following illustrates the thinking process that might occur in selecting the severity portion of the risk assessment matrix for the machine falling risk:

Identify likely outcomes. “If the machine falls, it will crush whatever it lands on. Such an injury will almost certainly be severe. Because of the height of the machine, it can easily fall on a person’s head and body with almost certain fatal results. There are also a variety of different crushing injuries, especially of the feet, even if the machine falls only a short distance.

Identify the most likely outcomes. “Because of the weight of the machine, a severe injury is almost certain. Because people are fairly agile and the fact that the falling machine gives a little warning that it is falling, death is not likely.”

Consider factors other than injuries. “We identified several equipment and facility items at risk. Most of these we have guarded, but some are still vulnerable. If the machine falls nobody can do any thing to protect these items. It would take a couple of days at least to get us back in full production.”

FAA System Safety Handbook, Appendix F  
December 30, 2000

Refer to the matrix (see Figure 2.1A). “Let’s see, any injury is likely to be severe, but a fatality is not very probable, property damage could be expensive and could cost us a lot of production time. Considering both factors, I think that *critical* is the best choice.”

Combine probability and severity in the matrix. The thinking process should be as follows:

The probability category *occasional* is in the middle of the matrix (refer to the matrix below). I go down until it meets the *critical* category coming from the left side. The result is a *high* rating. I notice that it is among the lower *high* ratings but it is still *high*.”

**Figure 2.1A Risk Assessment Matrix**

		Probability				
		Frequent	Likely	Occasional	Seldom	Unlikely
		A	B	C	D	E
S E V E R E I T Y	Catastrophic I	Extremely				
	Critical II	High	High			
	Moderate III		Medium			
	Negligible IV					Low
		Risk Levels				

Limitations and concerns with the use of the matrix. As you followed the scenario above, you may have noted that there are some problems involved in using the matrix. These include the following:

**Subjectivity.** There are at least two dimensions of subjectivity involved in the use of the matrix. The first is in the interpretation of the matrix categories. Your interpretation of the term “critical” may be quite different from mine. The second is in the interpretation of the risk. If a few weeks ago I saw a machine much like the one to be moved fall over and crush a person to death, I might have a greater tendency to rate both the probability and severity higher than someone who did not have such an experience. If time and resources permit, averaging the rating of several can reduce this variation personnel.

**Inconsistency.** The subjectivity described above naturally leads to some inconsistency. A risk rated very high in one organization may only have a high rating in another. This becomes a real problem if the two risks are competing for a limited pot of risk control resources (as they always are). There will be real motivation to inflate risk assessments to enhance competitiveness for limited resources.

### 3.0 RISK CONTROL OPTION ANALYSIS TOOLS, DETAILS, AND EXAMPLES

#### 3.1 BASIC RISK CONTROL OPTIONS

Major risk control options and examples of each are as follows:

**Reject** a risk. We can and should refuse to take a risk if the overall costs of the risk exceed its benefits. For example, planner may review the risks associated with a specific particular operation or task. After assessing all the advantages and evaluating the increased risk associated with it, even after application of all available risk controls, he decides the benefits do not outweigh the expected risk costs and it is better off in the long run not doing the operation or task.

**Avoiding** risk altogether requires canceling or delaying the job, or operation, but is an option that is rarely exercised due to operational importance. However, it may be possible to avoid specific risks: risks associated with a night operation may be avoided by planning the operation for daytime, likewise thunderstorms can be avoided by changing the route of flight.

**Delaying** a risk. It may be possible to delay a risk. If there is no time deadline or other operational benefit to speedy accomplishment of a risky task, then it is often desirable delay the acceptance of the risk. During the delay, the situation may change and the requirement to accept the risk may go away. During the delay additional risk control options may become available for one reason or another (resources become available, new technology becomes available, etc.) thereby reducing the overall risk.

Risk **transference** does not change probability or severity of the risk, but it may decrease the probability or severity of the risk actually experienced by the individual or organization accomplishing the activity. As a minimum, the risk to the original individual or organization is greatly decreased or eliminated because the possible losses or costs are shifted to another entity.

Risk is commonly **spread** out by either increasing the exposure distance or by lengthening the time between exposure events. Aircraft may be parked so that an explosion or fire in one aircraft will not propagate to others. Risk may also be spread over a group of personnel by rotating the personnel involved in a high-risk operation.

**Compensate** for a risk. We can create a redundant capability in certain special circumstances. Flight control redundancy is an example of an engineering or design redundancy. Another example is to plan for a back up, and then when a critical piece of equipment or other asset is damaged or destroyed we have capabilities available to bring on line to continue the operation.

Risk can be **reduced**. The overall goal of risk management is to plan operations or design systems that do not contain hazards and risks. However, the nature of most complex operations and systems makes it impossible or impractical to design them completely risk-free. As hazard analyses are performed, hazards will be identified that will require resolution. To be effective, risk management strategies must address the components of risk: probability, severity, or exposure. A proven order of precedence for dealing with risks and reducing the resulting risks is:

FAA System Safety Handbook, Appendix F  
December 30, 2000

*Plan or Design for Minimum Risk.* From the first, plan the operation or design the system to eliminate risks. Without hazards there is no probability, severity or exposure. If an identified risk cannot be eliminated, reduce the associated risk to an acceptable level. Flight control components can be designed so they cannot be incorrectly connected during maintenance operations as an example.

*Incorporate Safety Devices.* If identified hazards cannot be eliminated or their associated risk adequately reduced by modifying the operation or system elements or their inputs, that risk should be reduced to an acceptable level through the use of safety design features or devices. Safety devices can effect probability and reduce severity: an automobile seat belt doesn't prevent a collision but reduces the severity of injuries.

*Provide Warning Devices.* When planning, system design, and safety devices cannot effectively eliminate identified hazards or adequately reduces associated risk, warning devices should be used to detect the condition and alert personnel of the hazard. As an example, aircraft could be retrofitted with a low altitude ground collision warning system to reduce controlled flight into the ground risks. Warning signals and their application should be designed to minimize the probability of the incorrect personnel reaction to the signals and should be standardized. Flashing red lights or sirens are a common warning device that most people understand.

*Develop Procedures and Training.* Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training should be used. A warning system by itself may not be effective without training or procedures required to respond to the hazardous condition. The greater the human contribution to the functioning of the system or involvement in the operational process, the greater the chance for variability. However, if the system is well designed and the operation well planned, the only remaining risk reduction strategies may be procedures and training. Emergency procedure training and disaster preparedness exercises improve human response to hazardous situations.

In most cases it will not be possible to eliminate safety risk entirely, but it will be possible to significantly reduce it. There are many risk reduction options available. Examples are included in the next section.

### 3.1.1 THE RISK CONTROL OPTIONS MATRIX

The sample risk control options matrix, illustrated at Figure 3.1.1A, is designed to develop a detailed and comprehensive list of risk control options. These options are listed in priority order of preference, all things being equal, therefore start at the top and consider each option in turn. Add those controls that appear suitable and practical to a list of potential options. Examples of control options for each are suggested in Figure 3.1.1B. Many of the options may be applied at more than one level. For example, the training option may be applied to operators, supervisors, more senior leaders, or staff personnel.

Figure 3.1.1A Sample Risk Control Options Matrix

OPTIONS	OPERATOR	LEADER	STAFF	MGR
ENGINEER (Energy Mgt)				
Limit Energy				
Substitute Safer Form				
Prevent Buildup				
Prevent Release				
Provide Slow Release				

FAA System Safety Handbook, Appendix F  
December 30, 2000

OPTIONS	OPERATOR	LEADER	STAFF	MGR
Rechannel/separate In Time/Space				
Provide Special Maint of Controls				
<b>GUARD</b>				
On Source				
Barrier Between				
On Human or Object				
Raise Threshold (harden)				
<b>IMPROVE TASK DESIGN</b>				
Sequence of Events (Flow)				
Timing (within tasks, between tasks)				
Human-Machine Interface/Ergonomics				
Simplify Tasks				
Reduce Task Loads				
(physical, mental, emotional)				
Backout Options				
<b>LIMIT EXPOSURE</b>				
Number of People or Items				
Time				
Iterations				
<b>SELECTION OF PERSONNEL</b>				
Mental Criteria				
Emotional Criteria				
Physical Criteria				
Experience				
<b>TRAIN AND EDUCATE</b>				
Core Tasks (especially critical tasks)				
Leader Tasks				
Emergency/Contingency Tasks				
Safety Tasks				
Rehearsals				
<b>WARN</b>				
Signs/Color Coding				
Audio/Visual Alarms				
Briefings				
<b>MOTIVATE</b>				
Measurable Standards				
Essential Accountability				
Positive/negative Incentives				
Competition				
Demonstrations of Effects				
<b>REDUCE EFFECTS</b>				
Emergency Equipment				
Rescue Capabilities				

FAA System Safety Handbook, Appendix F  
December 30, 2000

OPTIONS	OPERATOR	LEADER	STAFF	MGR
Emergency Medical Care				
Emergency Procedures				
Damage Control Procedures/Plans				
Backups/Redundant Capabilities				
REHABILITATE				
Personnel				
Facilities/equipment				
Operational Capabilities				

**Figure 3.1.1B Example Risk Control Options Matrix**

OPTIONS	SOME EXAMPLES
ENGINEER (Energy Mgt.).	
Limit Energy	Lower voltages, small amount of explosives, reduce heights, and reduce speeds
Substitute Safer Form	Use air power, less hazardous chemicals, more stable explosives/chemicals
Prevent Buildup	Use automatic cutoffs, blowout panels, limit momentum, governors
Prevent Release	Containment, double/triple containment
Provide Slow Release	Use pressure relief valves, energy absorbing materials
Rechannel/separate in Time/Space	Automatic processes, deviators, barriers, distance
Provide Special Maint of Controls	Special procedures, special checks/audits
GUARD.	
On Source	Fire suppression systems, energy absorbing systems (crash walls, etc.)
Barrier between	Revetments, walls, distance
On Human or Object	Personal protective equipment, energy absorbing materials
Raise Threshold (harden)	Acclimatization, over-design, reinforcement, physical conditioning
IMPROVE TASK DESIGN.	
Sequence of Events (Flow)	Put tough tasks first before fatigue, don't schedule several tough tasks in a row
Timing (within tasks, between tasks)	Allow sufficient time to perform, to practice. Allow adequate time between tasks
Man-Machine Interface/Ergonomics	Assure equipment fits the people, and effective ergonomic design
Simplify Tasks	Provide job aids, reduce steps, provides tools like lifters communications aids

FAA System Safety Handbook, Appendix F  
December 30, 2000

OPTIONS	SOME EXAMPLES
Reduce Task Loads (physical, mental, emotional)	Set weight limits; automate mental calculations and some monitoring tasks. Avoid excessive stress, provide breaks, vacations, and spread risk among many
Bucket Options	Establish points where process reversal is possible when hazard is detected
<b>LIMIT EXPOSURE.</b>	
Number of People or Items	Only expose essential personnel & things
Time	Minimize the time of exposure -Don't bring the explosives until the last minute
Iterations	Don't do it as often
<b>SELECTION OF PERSONNEL.</b>	
Mental Criteria	Essential basic intelligence, and essential skills and proficiency
Emotional Criteria	Essential stability and maturity
Physical Criteria	Essential strength, motor skills, endurance, size
Experience	Demonstrated performance abilities
<b>TRAIN AND EDUCATE.</b>	
Core Tasks (especially critical tasks)	Define critical minimum abilities, train, test and score
Leader Tasks	Define essential leader tasks and standards, train, test and score
Emergency Contingency Tasks	Define, assign, train, verify ability
Safety Tasks	Hazard identification, risk controls, maintenance of standards
Rehearsals	Validate processes, validate skills, verify interfaces
<b>WARN.</b>	
Signs/Color Coding	Warning signs, instruction signs, traffic signs
Audio/Visual Alarms	Bells, flares, flashing lights, klaxons, whistles
Briefings	Refresher warnings, demonstrate hazards, refresh training
<b>MOTIVATE.</b>	
Measurable Standards	Define minimum acceptable risk controls, see that tasks are assigned
Essential Accountability	Check performance at an essential level of frequency and detail
Positive/negative Incentives	Meaningful individual & group rewards, punishment
Competition	Healthy individual and group competition on a fair basis
Demonstrations of Effects	Graphic, dynamic, but tasteful demonstrations of effects of unsafe acts
<b>REDUCE EFFECTS.</b>	
Emergency Equipment	Fire extinguishers, first aid materials, spill containment materials
Rescue Capabilities	A rescue squad, rescue equipment, helicopter rescue

OPTIONS	SOME EXAMPLES
Emergency Medical Care	Trained first aid personnel, medical facilities
Emergency Damage Control Procedures	Emergency responses for anticipated contingencies, coordinating agencies
Backups/Redundant Capabilities	Alternate ways to continue the operation if primaries are lost
REHABILITATE.	
Personnel	Rehabilitation services restore confidence
Facilities/equipment	Get key elements back in service
Operational Capabilities	Focus on restoration of the operation

#### 4.0 MAKE CONTROL DECISIONS TOOLS, DETAILS, AND EXAMPLES

Introduction. Making control decisions includes the basic options (reject, transfer, spread, etc.) as well as a comprehensive list of risk reduction options generated through use of the risk control options matrix by a decision-maker. The decision-making organization requires a procedure to establish, as a matter of routine, who should make various levels of risk decisions. Finally, after the best available set of risk controls is selected the decision-maker will make a final go/no-go decision.

Developing a decision-making process and system: Risk decision-making should be scrutinized in a risk decision system.

This system will produce the following benefits:

- Promptly get decisions to the right decision-makers
- Create a trail of accountability
- Assure that risk decisions involving comparable levels of risk are generally made at comparable levels of management
- Assure timely decisions
- Explicitly provide for the flexibility in the decision-making process required by the nature of operations.
- A decision matrix is an important part of a good decision-making system. These are normally tied directly to the risk assessment process.

Selecting the best combination of risk controls: This process can be made as simple as intuitively choosing what appears to be the best control or group of controls, or so complex they justify the use of the most sophisticated decision-making tools available. For most risks involving moderate levels of risk and relatively small investments in risk controls, the intuitive method is fully satisfactory. Guidelines for intuitive decisions are:

Don't select control options to produce the lowest level of risk, select the combination yielding the most operational supportive level of risk. This means keeping in mind the need to take risks when those appropriate risks are necessary for improved performance.

*Be aware that some risk controls are incompatible.* In some cases using risk control A will cancel the effect of risk control B. Obviously using both A and B is wasting resources. For example, a fully

FAA System Safety Handbook, Appendix F  
December 30, 2000

effective machine guard may make it completely unnecessary to use personnel protective equipment such as goggles and face shields. Using both will waste resources and impose a burden on operators.

*Be aware that some risk controls reinforce each other.* For example, a strong enforcement program to discipline violators of safety rules will be complemented by a positive incentive program to reward safe performance. The impact of the two coordinated together will usually be stronger than the sum of their impacts.

*Evaluate full costs versus full benefits.* Try to evaluate all the benefits of a risk and evaluate them against all of the costs of the risk control package. Traditionally, this comparison has been limited to comparisons of the incident/accident costs versus the safety function costs.

When it is supportive, choose redundant risk controls to protect against risk in-depth.

Keep in mind the objective is not risk control, it is optimum risk control.

Selecting risk controls when risks are high and risk control costs are important - cost benefit assessment. In these cases, the stakes are high enough to justify application of more formal decision-making processes. All of the tools existing in the management science of decision-making apply to the process of risk decision-making. Two of these tools should be used routinely and deserve space in this publication. The first is cost benefit assessment, a simplified variation of cost benefit analysis. Cost benefit analysis is a science in itself, however, it can be simplified sufficiently for routine use in risk management decision-making even at the lowest organizational levels. Some fiscal accuracy will be lost in this process of simplification, but the result of the application will be a much better selection of risk controls than if the procedures were not used. Budget personnel are usually trained in these procedures and can add value to the application. The process involves the following steps:

**Step 1.** Measure the full, lifecycle costs of the risk controls to include all costs to all involved parties. For example, a motorcycle helmet standard should account for the fact that each operator will need to pay for a helmet.

**Step 2.** Develop the best possible estimate of the likely lifecycle benefits of the risk control package to include any non-safety benefits expressed as a dollar estimate. For example, an ergonomics program can be expected to produce significant productivity benefits in addition to a reduction in cumulative trauma injuries.

**Step 3.** Let your budget expert's fine-tune your efforts.

**Step 4.** Develop the cost benefit ratio. You are seeking the best possible benefit-to-cost ratio but at least 2 to 1.

**Step 5.** Fine-tune the risk control package to achieve an improved "bang for the buck". The example at Figure 4.1A illustrates this process of fine-tuning applied to an ergonomics-training course (risk control).

Figure 4.1A Example Maximizing Bang for the Buck

Anyone can throw money at a problem. A manager finds the optimum level of resources producing an optimum level of effectiveness, i.e. maximum bang for the buck. Consider an ergonomics-training program involving training 400 supervisors from across the entire organization in a 4-hour (3 hours training, 1-hour admin) ergonomics-training course that will cost \$30,500 including student time. Ergonomics losses have been averaging \$300,000 per year and estimates are that the risk control will reduce this loss by 10% or \$30,000. On the basis of a cost benefit assessment over the next year (ignoring any out year considerations), this risk control appears to have a one year negative cost benefit ratio i.e. \$30,000 in benefit, versus a \$30,500 investment, a \$500 loss.

Apparently it is not a sound investment on a one-year basis. This is particularly true when we consider that most decision-makers will want the comfort of a 2 or 3 to 1 cost benefit ratio to insure a positive outcome. Can this project be turned into a winner?

We can make it a winner if able to access risk information concerning ergonomics injuries/illnesses from loss control office data, risk management concepts, and a useful tool called "Pareto's Law".

Pareto's Law, as previously mentioned, essentially states that 80% of most problems can be found in 20% of the exposure. For example, 80% of all traffic accidents might involve only 20% of the driver population. We can use this law, guided by our injury/illness data, to turn the training program into a solid winner. Here is what we might do.

**Step 1.** Let's assume that Pareto's Law applies to the distribution of ergonomics problems within this organization. If so, then 80% of the ergonomics problem can be found in 20% of our exposures. Our data can tell us which 20%. We can then target the 20% (80 students) of the original 400 students that are accounting for 80% of our ergonomics costs (\$240,000).

**Step 2.** Lets also assume that Pareto's Law applies to the importance of tasks that we intend to teach in the training course. If the three hours of training included 10 tasks, lets assume that two of those tasks (20%) will in fact account for 80% of the benefit of the course. Again our data should be able to indicate this. Lets also assume that by good luck, these two tasks only take the same time to teach as the other eight. We might now decide to teach only these two tasks which will require only 36 minutes (20% of 180 minutes). We will still retain 80% of the \$240,000 target value or \$192,000.

**Step 3.** Since the training now only requires 36 minutes, we will modify our training procedure to conduct the training in the workshops rather than in a classroom. This reduces our admin time from 1 hour (wash up, travel, get there well before it actually starts, and return to work) to 4 minutes. Our total training time is now 40 minutes.

**Summary.** We are still targeting \$192,000 of the original \$300,000 annual loss but our cost factor is now 80 employees for 40 minutes at \$15/hour, with our teaching cost cut to 1/5th of the \$6000 (80 students instead of 400) which is \$1200. We still have our staff cost so the total cost of the project is now \$2500. We will still get the 10% reduction in the remaining \$192,000 that we are still targeting, which totals \$19,200. Our cost benefit ratio is now a robust 7.68 to 1. If all goes well with the initial training and we actually demonstrate at 20% loss reduction, we may choose to expand the training to the next riskiest 20% of our 400 personnel which should also produce a very positive return.

Selecting risk controls when risks are high and risk control costs are important - use of decision matrices. An excellent tool for evaluating various risk control options is the decision matrix. On the vertical dimension of the matrix we list the operation supportive characteristics we are looking for in risk controls. Across the top of the matrix we list the various risk control options (individual options or packages of options). Then we rank each control option on a scale of 1 (very low) to 10 (very high) in each of the desirable characteristics. If we choose to, we can weight each desirable characteristic based on its operational significance and calculate the weighted score (illustrated below). All things being the same, the options with the higher scores are the stronger options. A generic illustration is provided at Figure 4.1B.

**Figure 4.1B Sample Decision Matrix**

RATING FACTOR	WEIGHT*	RISK CONTROL OPTIONS/PACKAGES					
		#1	#2	#3	#4	#5	#6
Low Cost	5	9/45	6/30	4/20	5/25	8/40	8/40
Easy to implement	4	10/40	7/28	5/20	6/24	8/32	8/32
Positive Operator involvement	5	8/40	2/10	1/5	6/30	3/15	7/35
Consistent with Culture	3	10/30	2/6	9/27	6/18	6/18	6/18
Easy to integrate	3	9/27	5/15	6/18	7/21	6/18	5/15
Easy to measure	2	10/20	10/20	10/20	8/16	8/16	5/10
Low risk (sure to succeed)	3	9/27	9/27	10/30	2/6	4/12	5/15
	TOTALS	229	136	140	140	151	165
* Weighting is optional and is designed to reflect the relative importance of the various factors.							

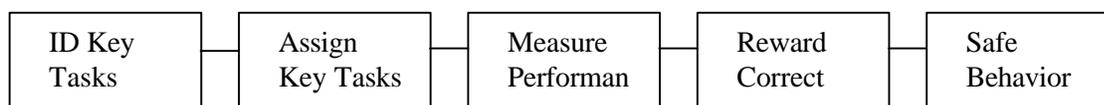
Summary. It is not unusual for a risk control package to cost hundreds of thousands of dollars and even millions over time. Millions of dollars and critical operations may be at risk. The expenditure of several tens of thousands of dollars to get the decision right is sound management practice and good risk management.

## 5.0 RISK CONTROL IMPLEMENTATION TOOLS AND DETAILS

## 5.1 Introduction

Figure 5.1A summarizes a Risk Control Implementation model. It is based on accountability being an essential element of risk management success. Organizations and individuals must be held accountable for the risk decisions and actions that they take or the risk control motivation is minimized. The model depicted at Figure 5.1A is the basis of positive accountability and strong risk control behavior.

**Figure 5.1A Implementation Model**



## 5.2 Applying the model

The example below illustrates each step in the model applied to the sometimes-difficult task of assuring that personnel consistently wear and use their protective clothing and equipment. The steps of the model should be applied as follows:

### 5.2.1 Identify key tasks

This step, while obvious however, is critical to actually define the key tasks with enough accuracy that effective accountability is justified. For example, in our example regarding use of protective clothing and equipment, it is essential to identify exactly when the use of such items is required. Is it when I enter the door of a work area? When I approach a machine? How close? What about on the loading dock? Exactly what items are to be worn? Is there any specific way that they should be worn? I can be wearing ear plugs but incorrectly have them stuck in the outer ear, producing little or no noise reduction benefit. Does this meet the requirement? The task needs to be defined with sufficient precision that personnel know what is expected of them and that what is expected of them produces the risk control desired. It is also important that the task be made as simple, pleasant, and trouble free as possible. In this way we significantly increase the ease with which the rest of the process proceeds.

### 5.2.2 Assign key tasks

Personnel need to know clearly what is expected of them especially if they are going to be held accountable for the task. This is normally not difficult. The task can be included in job descriptions, operating instructions, or in the task procedures contained in manuals. It can be very effectively be embedded in training. In less structured situations, it can be a clear verbal order or directive. It is important that the assignment of the task include the specifics of what is expected.

### 5.2.3 Measure performance

The task needs to include at least a basic level of measurement. It is important to note that measurement does not need to include every time the behavior is displayed. It is often perfectly practical to sample performance only once in large number of actions, perhaps as few as one in several hundred actions as long as the sample is a random example of routine behavior. Often the only one who needs to do the measuring is the individual responsible for the behavior. In other situations, the supervisor or an outside auditor may need to do the observing. Performance is compared to the standard, which should have been

FAA System Safety Handbook, Appendix F  
December 30, 2000

communicated to the responsible individual. This step of the process is the rigorous application of the old adage that “What is monitored (or measured) and checked gets done.”

#### **5.2.4 Reward correct behavior and correct inadequate behavior**

The emphasis should clearly be on reinforcing correct behavior. Reinforcement means any action that increases the likelihood that the person will display the desired behavior again. It can be as informal as a pat on the back or as formal as a major award or cash incentive. Correcting inadequate behavior should be done whenever inadequate behavior is observed. The special case of *punishment* should only be used when all other means of producing the desired behavior have failed.

#### **5.2.5 Risk control performance**

If the steps outlined above have been accomplished correctly, the result will be consistent success in controlling risk. Note that the unpleasantness of the task will dictate the extent of the rewards and corrective actions required. The harder the task for whatever reason, the more powerful the rewards and corrective actions needed will be. It is important to make risk control tasks as uncomplicated, and pleasant as possible.

### **6.0 SUPERVISE AND REVIEW DETAILS AND EXAMPLES**

Management involves moving a task or an organization toward a goal. To move toward a goal you must have three things. You must have a goal, you must know where you are in relation to that goal, and you must have a plan to reach it. An effective set of risk matrices provides two of the elements.

In regard to ORM, indicators should provide information concerning the success or lack of success of controls intended to mitigate a risk. These indicators could focus on those key areas identified during the assessment as being critical to minimizing a serious risk area. Additionally, matrices may be developed to generically identify operations/areas where ORM efforts are needed.

A representative set of risk measures that a maintenance shop leader could use to assess the progress of his shop toward the goal of improving safety performance. Similar indicators could be developed in the areas of environment, fire prevention, security, and other loss control areas.

The tool control effectiveness index. Establish key indicators of tool control program effectiveness (percentage of tool checks completed, items found by QA, score on knowledge quiz regarding control procedures, etc.). All that is needed is a sampling of data in one or more of these areas. If more than one area is sampled, the scores can be weighted if desired and rolled up into a single tool control index by averaging them. See Figure 6.1A for the example.

**Figure 6.1A Example Tool Control Effectiveness Measurement**

The percent of tool checks completed is 94%.  
 Items found by QA. Items were found in 2% of QA inspections (98% were to standard).  
 Tool control quiz score is 88%.  
 If all items are weighted equally ( $94+98+88$  divided by  $3 = 93.3$ ) then 93.3 is this quarter's tool control safety index. Of course, in this index, high scores are desirable.

FAA System Safety Handbook, Appendix F  
December 30, 2000

The protective clothing and equipment risk index. Shop personnel are using this index measures the effectiveness with which required protective clothing and equipment. Making spot observations periodically during the workday collects data. Data are recorded on a check sheet and are rolled-up monthly. The index is the percent safe observations of the total number of observations made as illustrated at Figure 6.1B.

#### **Figure 6.1B Example Safety Observation Measurement**

TOTAL OBSERVATIONS: 27 SAFE OBSERVATIONS: 21

The protective clothing and equipment safety index is 78 (21 divided by 27 = 78%).  
In this index high scores are desirable

The emergency procedures index. This index measures the readiness of the shop to respond to various emergencies such as fires, injuries, and hazmat releases. It is made up of a compilation of indicators as shown at Figure 6.1C A high score is desirable.

#### **Figure 6.1C Example Emergency Procedures Measurement**

Scores on emergency procedure quizzes  
Percentage of emergency equipment on hand and fully operational  
Scores on emergency response drills indicating speed, correct procedures, and other effectiveness indicators

The quality assurance score. This score measures a defined set of maintenance indicators tailored to the particular type of aircraft serviced. Quality Assurance (QA) personnel record deviations in these target areas as a percentage of total observations made. The specific types of deviations are noted. The score is the percentage of positive observations with a high score being desirable. Secondary scores could be developed for each type of deviation if desired.

The overall index. Any combination of the indicators previously mentioned, along with others as desired, can be rolled up into an overall index for the maintenance facility as illustrated at Figure 6.1D.

**Figure 6.1D Example Overall Measurement**

Tool control safety index: 93.3
Protective clothing and equipment safety index: 78.0
Emergency procedures index: 88.4
Quality Assurance Score: 97.9
TOTAL: 357.6
OR AVERAGE: 89.4
This index is the overall safety index for the maintenance facility. The goal is to push toward 100% or a maximum score of 400. This index would be used in our accountability procedures to measure performance and establish the basis for rewards or corrective action.

Once the data has been collected and analyzed, the results need to be provided to the unit. With this information the unit will be able to concentrate their efforts on those areas where improvement would produce the greatest gain.

Summary. It is not difficult to set up useful and effective measures of operational risk, particularly once the key risks have been identified during a risk assessment. Additionally, the workload associated with such indicators can be minimized by using data already collected and by collecting the data as an integrated routine aspect of operational processes.

## **Appendix G**

### **FAA ORDER 8040.4**

8040.4  
6/26/98

**ORDER**

U.S. DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION

8040.4

6/26/98

**SUBJ: SAFETY RISK MANAGEMENT**

---

1. **PURPOSE.** This order establishes the safety risk management policy and prescribes procedures for implementing safety risk management as a decision making tool within the Federal Aviation Administration (FAA). This order establishes the Safety Risk Management Committee.
2. **DISTRIBUTION.** This order is distributed to the division level in the Washington headquarters, regions, and centers, with limited distribution to all field offices and facilities.
3. **DEFINITIONS.** Appendix 1, Definitions, contains definitions used in this order.
4. **SCOPE.** This order requires the application of a flexible but formalized safety risk management process for all high-consequence decisions, except in situations deemed by the Administrator to be an emergency. A high-consequence decision is one that either creates or could be reasonably estimated to result in a statistical increase or decrease, as determined by the program office, in personal injuries and/or loss of life and health, a change in property values, loss of or damage to property, costs or savings, or other economic impacts valued at \$100,000,000 or more per annum. The objective of this policy is to formalize a common sense approach to risk management and safety risk analysis/assessment in FAA decisionmaking. This order is not intended to interfere with regulatory processes and activities. Each program office will interpret, establish, and execute the policy contained herein consistent with its role and responsibility. The Safety Risk Management Committee will consist of technical personnel with risk assessment expertise and be available for guidance across all FAA programs.
5. **SAFETY RISK MANAGEMENT POLICY.** The FAA shall use a formal, disciplined, and documented decisionmaking process to address safety risks in relation to high-consequence decisions impacting the complete product life cycle. The critical information resulting from a safety risk management process can thereby be effectively communicated in an objective and unbiased manner to decisionmakers, and from decisionmakers to the public. All decisionmaking authorities within the FAA shall maintain safety risk management expertise appropriate to their operations, and shall perform and document the safety risk management process prior to issuing the high-consequence decision. The choice of methodologies to support risk management efforts remains the responsibility of each program office. The decisionmaking authority shall determine the documentation format. The approach to safety risk management is composed of the following steps:
  - a. **Plan.** A case-specific plan for risk analysis and risk assessment shall be predetermined in adequate detail for appropriate review and agreement by the decisionmaking authority prior to commitment of resources. The plan shall additionally describe criteria for acceptable risk.

b. Hazard Identification. The specific safety hazard or list of hazards to be addressed by the safety risk management plan shall be explicitly identified to prevent ambiguity in subsequent analysis and assessment.

c. Analysis. Both elements of risk (hazard severity and likelihood of occurrence) shall be characterized. The inability to quantify and/or lack of historical data on a particular hazard does not exclude the hazard from this requirement. If the seriousness of a hazard can be expected to increase over the effective life of the decision, this should be noted. Additionally, both elements should be estimated for each hazard being analyzed, even if historical and/or quantitative data is not available.

d. Assessment. The combined impact of the risk elements in paragraph 5c shall be compared to acceptability criteria and the results provided for decisionmaking.

e. Decision. The risk management decision shall consider the risk assessment results conducted in accordance with paragraph 5d. Risk assessment results may be used to compare and contrast alternative options.

**6. PRINCIPLES FOR SAFETY RISK ASSESSMENT AND RISK CHARACTERIZATION.** In characterizing risk, one must comply with each of the following:

a. General. Safety risk assessments, to the maximum extent feasible:

- (1) Are scientifically objective.
- (2) Are unbiased.
- (3) Include all relevant data available.
- (4) Employ default or conservative assumptions only if situation-specific information is not reasonably available. The basis of these assumptions must be clearly identified.
- (5) Distinguish clearly as to what risks would be affected by the decision and what risks would not.
- (6) Are reasonably detailed and accurate.
- (7) Relate to current risk or the risk resulting from not adopting the proposal being considered.
- (8) Allow for unknown and/or unquantifiable risks.

b. Principles. The principles to be applied when preparing safety risk assessments are:

(1) Each risk assessment should first analyze the two elements of risk: severity of the hazard and likelihood of occurrence. Risk assessment is then performed by comparing the combined effect of their characteristics to acceptable criteria as determined in the plan (paragraph 5a).

(2) A risk assessment may be qualitative and/or quantitative. To the maximum extent practicable, these risk assessments will be quantitative.

8040.4  
6/26/98

- (3) The selection of a risk assessment methodology should be flexible.
- (4) Basic assumptions should be documented or, if only bounds can be estimated reliably, the range encompassed should be described.
- (5) Significant risk assessment assumptions, inferences, or models should:
  - (a) Describe any model used in the risk assessment and make explicit the assumptions incorporated in the model.
  - (b) Identify any policy or value judgments.
  - (c) Explain the basis for choices.
  - (d) Indicate the extent that the model and the assumptions incorporated have been validated by or conflict with empirical data.
- (6) All safety risk assessments should include or summarize the information of paragraphs 6a (3) and 6a(4) as well as 6b (4) and 6b (5). This record should be maintained by the organization performing the assessment in accordance with Order 1350.15B, Records Organization, Transfer, and Destruction Standards.

**7. ANALYSIS OF RISK REDUCTION BENEFITS AND COSTS.** For each high-consequence decision, the following tasks shall be performed:

- a. Compare the results of a risk assessment for each risk-reduction alternative considered, including no action, in order to rank each risk assessment for decisionmaking purposes. The assessment will consider future conditions, e.g., increased traffic volume.
- b. Assess the costs and the safety risk reduction or other benefits associated with implementation of, and compliance with, an alternative under final consideration.

**8. SUBSTITUTION RISKS.** Safety risk assessments of proposed changes to high-consequence decisions shall include a statement of substitution risks. Substitution risks shall be included in the risk assessment documentation.

**9. SAFETY RISK MANAGEMENT COMMITTEE.** This order establishes the Safety Risk Management Committee. Appendix 2, Safety Risk Management Committee, contains the committee charter. The committee shall provide a service to any FAA organization for safety risk management planning, as outlined in appendix 2, when requested by the responsible program office. It also meets periodically (e.g., two to four times per year) to exchange risk management ideas and information. The committee will provide advice and counsel to the Office of System Safety, the Assistant Administrator for System Safety, and other management officials when requested.

Jane F. Garvey  
Administrator

## APPENDIX 1. DEFINITIONS.

1. **COSTS.** Direct and indirect costs to the United States Government, State, local, and tribal governments, international trade impacts, and the private sector.
2. **EMERGENCY.** A circumstance that requires immediate action to be taken.
3. **HAZARD.** Condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event.
4. **HAZARD IDENTIFICATION.** Identification of a substance, activity, or condition as potentially posing a risk to human health or safety.
5. **HIGH-CONSEQUENCE DECISION.** Decision that either creates or could be reasonably estimated to result in a statistical increase or decrease in personal injuries and/or loss of life and health, a change in property values, loss of or damage to property, costs or savings, or other economic impacts valued at \$100,000,000 or more per annum.
6. **PRODUCT LIFE CYCLE.** The entire sequence from precertification activities through those associated with removal from service.
7. **MISHAP.** Unplanned event, or series of events, that results in death, injury, occupational illness, or damage to or loss of equipment or property.
8. **RISK.** Expression of the impact of an undesired event in terms of event severity and event likelihood.
9. **RISK ASSESSMENT.**
  - a. Process of identifying hazards and quantifying or qualifying the degree of risk they pose for exposed individuals, populations, or resources; and/or
  - b. Document containing the explanation of how the assessment process is applied to individual activities or conditions.
10. **RISK CHARACTERIZATION.** Identification or evaluation of the two components of risk, i.e., undesired event severity and likelihood of occurrence.
11. **RISK MANAGEMENT.** Management activity ensuring that risk is identified and eliminated or controlled within established program risk parameters.
12. **SAFETY RISK.** Expression of the probability and impact of an undesired event in terms of hazard severity and hazard likelihood.
13. **SUBSTITUTION RISK.** Additional risk to human health or safety, to include property risk, from an action designed to reduce some other risk(s).



## APPENDIX 2. SAFETY RISK MANAGEMENT COMMITTEE

1. PURPOSE. The Safety Risk Management Committee provides a communication and support team to supplement the overall risk analysis capability and efficiency of key FAA organizations.
2. RESPONSIBILITIES. The Committee supports FAA safety risk management activities. It provides advice and guidance, upon request from responsible program offices, to help them fulfill their authority and responsibility to incorporate safety risk management as a decisionmaking tool. It serves as an internal vehicle for risk management process communication, for coordination of risk analysis methods, and for use of common practices where appropriate. This includes, but is not limited to:
  - a. Continuing the internal exchange of risk management information among key FAA organizations.
  - b. Fostering the exchange of risk management ideas and information with other government agencies and industry to avoid duplication of effort.
  - c. Providing risk analysis/management advice and guidance.
  - d. Identifying and recommending needed enhancements to FAA risk analysis/management capabilities and/or efficiencies upon request.
  - e. Maintaining a risk management resources directory that includes:
    - (1) FAA risk methodologies productively employed,
    - (2) Specific internal risk analysis/management expertise by methodology or tool and organizational contact point(s), and
    - (3) A central contact point for resource identification assistance.
  - f. Encouraging the establishment of an international directory of aviation safety information resources via the Internet.
  - g. Assisting in the identification of suitable risk analysis tools and initiate appropriate training in the use of these tools.
3. COMPOSITION. The Safety Risk Management Committee is composed of safety and risk management professionals representing all Associate/Assistant Administrators and the Offices of the Chief Counsel, Civil Rights, Government and Industry Affairs, and Public Affairs. The Assistant Administrator for System Safety will designate an individual to chair the committee. The chairperson is responsible for providing written notice of all meetings to committee members and, in coordination with the executive secretary, keeping minutes of the meetings.

8040.4

6/26/98

Appendix 2

4. ASSIGNMENTS. The Safety Risk Management Committee may form ad hoc working groups to address specific issues when requested by the responsible program office. Composition of those working groups will consist of member representatives from across the FAA. Working groups will be disbanded upon completion of their task. The Office of System Safety shall provide the position of executive secretary of the committee. The Office of System Safety shall also furnish other administrative support.
  
5. FUNDING. Resources for support staff and working group activities will be provided as determined by the Assistant Administrator for System Safety. Unless otherwise stated, each member is responsible for his/her own costs associated with committee membership.

## **APPENDIX H**

### **MIL-STD-882D**

MIL-STD-882D

**NOT MEASUREMENT  
SENSITIVE**

**MIL-STD-882D  
10 February 2000**

---

**SUPERSEDING  
MIL-STD-882C  
19 January 1993**

**DEPARTMENT OF DEFENSE  
STANDARD PRACTICE FOR  
SYSTEM SAFETY**



AMSC N/A

AREA SAFT

## MIL-STD-882D

## FOREWORD

1. This standard is approved for use by all Departments and Agencies within the Department of Defense (DoD).
2. The DoD is committed to protecting: private and public personnel from accidental death, injury, or occupational illness; weapon systems, equipment, material, and facilities from accidental destruction or damage; and public property while executing its mission of national defense. Within mission requirements, the DoD will also ensure that the quality of the environment is protected to the maximum extent practical. The DoD has implemented environmental, safety, and health efforts to meet these objectives. Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations. A key objective of the DoD system safety approach is to include mishap risk management consistent with mission requirements, in technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation. The DoD goal is zero mishaps.
3. This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified mishap risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority, and compliant with federal laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. Residual mishap risk associated with an individual system must be reported to and accepted by the appropriate authority as defined in DoD Regulation 5000.2-R. When MIL-STD-882 is required in a solicitation or contract and no specific references are included, then only those requirements presented in section 4 are applicable.
4. This revision applies the tenets of acquisition reform to system safety in Government procurement. A joint Government/Industrial process team oversaw this revision. The Government Electronic and Information Technology Association (GEIA), G-48 committee on system safety represented industry on the process action team. System safety information (e.g., system safety tasks, commonly used approaches, etc.) associated with previous versions of this standard are in the *Defense Acquisition Deskbook* (see 6.8). This standard practice is no longer the source for any safety-related data item descriptions (DIDs).
5. Address beneficial comments (recommendations, additions, and deletions) and any pertinent information that may be of use in improving this document to: HQ Air Force Materiel Command (SES), 4375 Chidlaw Road, Wright-Patterson AFB, OH 45433-5006. Use the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter or electronic mail.

## MIL-STD-882D

## CONTENTS

<u>PARAGRAPH</u>	<u>PAGE</u>
<u>FOREWORD</u> .....	ii
1. <u>SCOPE</u> .....	1
1.1 Scope.....	1
2. <u>APPLICABLE DOCUMENTS</u> .....	1
3. <u>DEFINITIONS</u> .....	1
3.1 Acronyms used in this standard .....	1
3.2 Definitions.....	1
3.2.1 Acquisition program .....	1
3.2.2 Developer .....	1
3.2.3 Hazard .....	1
3.2.4 Hazardous material .....	2
3.2.5 Life cycle.....	2
3.2.6 Mishap.....	2
3.2.7 Mishap risk.....	2
3.2.8 Program manager.....	2
3.2.9 Residual mishap risk.....	2
3.2.10 Safety .....	2
3.2.11 Subsystem .....	2
3.2.12 System.....	2
3.2.13 System safety.....	2
3.2.14 System safety engineering.....	2
4. <u>GENERAL REQUIREMENTS</u> .....	3
4.1 Documentation of the system safety approach.....	3
4.2 Identification of hazards.....	3
4.3 Assessment of mishap risk .....	3
4.4 Identification of mishap risk mitigation measures .....	3
4.5 Reduction of mishap risk to an acceptable level .....	4
4.6 Verification of mishap risk reduction .....	4
4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority .....	4
4.8 Tracking of hazards and residual mishap risk.....	4
5. <u>DETAILED REQUIREMENTS</u> .....	4
6. <u>NOTES</u> .....	5
6.1 Intended use.....	5
6.2 Data requirements.....	5
6.3 Subject term (key words) listing.....	6

## MIL-STD-882D

6.4	Definitions used in this standard .....	6
6.5	International standardization agreements.....	6
6.6	Explosive hazard classification and characteristic data .....	6
6.7	Use of system safety data in certification and other specialized safety approvals..	6
6.8	DoD acquisition practices .....	7
6.9	Identification of changes .....	7

APPENDIXES

A	Guidance for implementation of system safety efforts .....	8
---	--	---

	<u>CONCLUDING MATERIAL</u> .....	26
--	----------------------------------	----

TABLES

<u>TABLE</u>		<u>PAGE</u>
A-I.	Suggested mishap severity categories.....	18
A-II.	Suggested mishap probability levels.....	19
A-III.	Example mishap risk assessment values .....	20
A-IV.	Example mishap risk categories and mishap risk acceptance levels .....	20

## MIL-STD-882D

## 1. SCOPE

1.1 Scope. This document outlines a standard practice for conducting system safety.

The system safety practice as defined herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority and compliant with federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. When requiring MIL-STD-882 in a solicitation or contract and no specific paragraphs of this standard are identified, then apply only those requirements presented in section 4.

## 2. APPLICABLE DOCUMENTS

Sections 3, 4, and 5 of this standard contain no applicable documents. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples.

## 3. DEFINITIONS

3.1 Acronyms used in this standard. The acronyms used in this standard are defined as follows:

a. AMSDL	Acquisition Management System & Data Requirement List
b. ANSI	American National Standard Institute
c. DID	Data Item Description
d. DoD	Department of Defense
e. ESH	Environmental, Safety, and Health
f. GEIA	Government Electronic & Information Technology Association
g. MAIS	Major Automated Information System
h. MDAP	Major Defense Acquisition Program
i. USAF	United States Air Force

3.2 Definitions. Within this document, the following definitions apply (see 6.4):

3.2.1 Acquisition program. A directed, funded effort designed to provide a new, improved, or continuing system in response to a validated operational need.

3.2.2 Developer. The individual or organization assigned responsibility for a development effort. Developers can be either internal to the government or contractors.

3.2.3 Hazard. Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

## MIL-STD-882D

3.2.4 Hazardous material. Any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage.

3.2.5 Life cycle. All phases of the system's life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.

3.2.6 Mishap. An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.7 Mishap risk. An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

3.2.8 Program Manager (PM). A government official who is responsible for managing an acquisition program. Also, a general term of reference to those organizations directed by individual managers, exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated systems. This term will normally be used in lieu of any other titles, e.g.; system support manager, weapon program manager, system manager, and project manager.

3.2.9 Residual mishap risk. The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence (see 4.4).

3.2.10 Safety. Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

3.2.11 Subsystem. A grouping of items satisfying a logical group of functions within a particular system.

3.2.12 System. An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

3.2.13 System safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

3.2.14 System safety engineering. An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

## MIL-STD-882D

## 4. GENERAL REQUIREMENTS

This section defines the system safety requirements to perform throughout the life cycle for any system, new development, upgrade, modification, resolution of deficiencies, or technology development. When properly applied, these requirements should ensure the identification and understanding of all known hazards and their associated risks; and mishap risk eliminated or reduced to acceptable levels. The objective of system safety is to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management. This document delineates the minimum mandatory requirements for an acceptable system safety program for any DoD system. When MIL-STD-882 is required in a solicitation or contract, but no specific references are included, then only the requirements in this section are applicable. System safety requirements consist of the following:

4.1 Documentation of the system safety approach. Document the developer's and program manager's approved system safety engineering approach. This documentation shall:

- a. Describe the program's implementation using the requirements herein. Include identification of each hazard analysis and mishap risk assessment process used.
- b. Include information on system safety integration into the overall program structure.
- c. Define how hazards and residual mishap risk are communicated to and accepted by the appropriate risk acceptance authority (see 4.7) and how hazards and residual mishap risk will be tracked (see 4.8).

4.2 Identification of hazards. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended use or application. Consider and use historical hazard and mishap data, including lessons learned from other systems. Identification of hazards is a responsibility of all program members. During hazard identification, consider hazards that could occur over the system life cycle.

4.3 Assessment of mishap risk. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential negative impact of the hazard on personnel, facilities, equipment, operations, the public, and the environment, as well as on the system itself. The tables in Appendix A are to be used unless otherwise specified.

4.4 Identification of mishap risk mitigation measures. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority. The system safety design order of precedence for mitigating identified hazards is:

- a. Eliminate hazards through design selection. If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection.

## MIL-STD-882D

b. Incorporate safety devices. If unable to eliminate the hazard through design selection, reduce the mishap risk to an acceptable level using protective safety features or devices.

c. Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.

d. Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid using warning, caution, or other written advisory as the only risk reduction method.

4.5 Reduction of mishap risk to an acceptable level. Reduce the mishap risk through a mitigation approach mutually agreed to by both the developer and the program manager. Communicate residual mishap risk and hazards to the associated test effort for verification.

4.6 Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. Report all new hazards identified during testing to the program manager and the developer.

4.7 Review of hazards and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. Unless otherwise specified, the suggested tables A-I through A-III of the appendix will be used to rank residual risk. The program manager shall ensure that remaining hazards and residual mishap risk are reviewed and accepted by the appropriate risk acceptance authority (ref. table A-IV). The appropriate risk acceptance authority will include the system user in the mishap risk review. The appropriate risk acceptance authority shall formally acknowledge and document acceptance of hazards and residual mishap risk.

4.8 Tracking of hazards, their closures, and residual mishap risk. Track hazards, their closure actions, and the residual mishap risk. Maintain a tracking system that includes hazards, their closure actions, and residual mishap risk throughout the system life cycle. The program manager shall keep the system user advised of the hazards and residual mishap risk.

## 5. DETAILED REQUIREMENTS

Program managers shall identify in the solicitation and system specification any specific system safety engineering requirements including risk assessment and acceptance, unique classifications and certifications (see 6.6 and 6.7), or any mishap reduction needs unique to their program. Additional information in developing program specific requirements is located in Appendix A.

## MIL-STD-882D

## 6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use. This standard establishes a common basis for expectations of a properly executed system safety effort.

6.2 Data requirements. Hazard analysis data may be obtained from contracted sources by citing DI-MISC-80508, Technical Report - Study/Services. When it is necessary to obtain data, list the applicable Data Item Descriptions (DIDs) on the Contract Data Requirements List (DD Form 1423), except where the DoD Federal Acquisition Regulation Supplement exempts the requirement for a DD Form 1423. The developer and the program manager are encouraged to negotiate access to internal development data when hard copies are not necessary. They are also encouraged to request that any type of safety plan required to be provided by the contractor, be submitted with the proposal. It is further requested that any of the below listed data items be condensed into the statement of work and the resulting data delivered in one general type scientific report.

Current DIDs, that may be applicable to a system safety effort (check DoD 5010.12-L, Acquisition Management Systems and Data Requirements Control List (AMSDL) for the most current version before using), include:

<u>DID Number</u>	<u>DID Title</u>
DI-MISC-80043	Ammunition Data Card
DI-SAFT-80101	System Safety Hazard Analysis Report
DI-SAFT-80102	Safety Assessment Report
DI-SAFT-80103	Engineering Change Proposal System Safety Report
DI-SAFT-80104	Waiver or Deviation System Safety Report
DI-SAFT-80105	System Safety Program Progress Report
DI-SAFT-80106	Occupational Health Hazard Assessment
DI-SAFT-80184	Radiation Hazard Control Procedures
DI-MISC-80508	Technical Report - Study Services
DI SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-ADMN-81250	Conference Minutes
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-ILSS-81495	Failure Mode, Effects, Criticality Analysis Report

## MIL-STD-882D

6.3 Subject term (key word) listing.

Environmental  
Hazard  
Mishap  
Mishap probability levels  
Mishap risk  
Mishap severity categories  
Occupational Health  
Residual mishap risk  
System safety engineering

6.4 Definitions used in this standard. The definitions at 3.2 may be different from those used in other specialty areas. One must carefully check the specific definition of a term in question for its area of origination before applying the approach described in this document.

6.5 International standardization agreements. Certain provisions of this standard are the subject of international standardization agreements (AIR STD 20/23B, *Safety Design Requirements for Airborne Dispenser Weapons*, and STANAG No. 3786, *Safety Design Requirements for Airborne Dispenser Weapons*). When proposing amendment, revision, or cancellation of this standard that might modify the international agreement concerned, the preparing activity will take appropriate action through international standardization channels, including departmental standardization offices, to change the agreement or make other appropriate accommodations.

6.6 Explosive hazard classification and characteristic data. Any new or modified item of munitions or of an explosive nature that will be transported to or stored at a DoD installation or facility must first obtain an interim or final explosive hazard classification. The system safety effort should provide the data necessary for the program manager to obtain the necessary classification(s). These data should include identification of safety hazards involved in handling, shipping, and storage related to production, use, and disposal of the item.

6.7 Use of system safety data in certification and other specialized safety approvals. Hazard analyses are often required for many related certifications and specialized reviews. Examples of activities requiring data generated during a system safety effort include:

- a. Federal Aviation Agency airworthiness certification of designs and modifications
- b. DoD airworthiness determination
- c. Nuclear and non-nuclear munitions certification
- d. Flight readiness reviews
- e. Flight test safety review board reviews
- f. Nuclear Regulatory Commission licensing
- g. Department of Energy certification

Special safety-related approval authorities include USAF Radioisotope Committee, Weapon System Explosive Safety Review Board (Navy), Non-Nuclear Weapons and Explosives Safety Board (NNWESB), Army Fuze Safety Review Board, Triservice Laser Safety Review

## MIL-STD-882D

Board, and the DoD Explosive Safety Board. Acquisition agencies should ensure that appropriate service safety agency approvals are obtained prior to use of new or modified weapons systems in an operational or test environment.

6.8 DoD acquisition practices. Information on DoD acquisition practices is presented in the *Defense Acquisition Deskbook* available from the Deskbook Joint Program Office, Wright-Patterson Air Force Base, Ohio. Nothing in the referenced information is considered additive to the requirements provided in this standard.

6.9 Identification of changes. Due to the extent of the changes, marginal notations are not used in this revision to identify changes with respect to the previous issue.

MIL-STD-882D  
APPENDIX A

GUIDANCE FOR IMPLEMENTATION OF  
A SYSTEM SAFETY EFFORT

A.1 SCOPE

A.1.1 Scope. This appendix provides rationale and guidance to fit the needs of most system safety efforts. It includes further explanation of the effort and activities available to meet the requirements described in section 4 of this standard. This appendix is not a mandatory part of this standard and is not to be included in solicitations by reference. However, program managers may extract portions of this appendix for inclusion in requirement documents and solicitations.

A.2 APPLICABLE DOCUMENTS

A.2.1 General. The documents listed in this section are referenced in sections A.3, A.4, and A.5. This section does not include documents cited in other sections of this appendix or recommended for additional information or as examples.

A.2.2 Government documents.

A.2.2.1 Specifications, standards, and handbooks. This section is not applicable to this appendix.

A.2.2.2 Other Government documents, drawings, and publications. The following other Government document forms a part of this document to the extent specified herein. Unless otherwise specified, the issue is that cited in the solicitation.

DoD 5000.2-R	Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs
--------------	--

(Copies of DoD 5000.2-R are available from the Washington Headquarters Services, Directives and Records Branch (Directives Section), Washington, DC or from the DoD Acquisition Deskbook).

A.2.3 Non-Government publications. This section is not applicable to this appendix.

A.2.4 Order of precedence. Since this appendix is not mandatory, in event of a conflict between the text of this appendix and the reference cited herein, the text of the reference takes precedence. Nothing in this appendix supersedes applicable laws and regulations unless a specific exemption has been obtained.

MIL-STD-882D  
APPENDIX A

### A.3 DEFINITIONS

A.3.1 Acronyms used in this appendix. No additional acronyms are used in this appendix.

A.3.2 Definitions. Additional definitions that apply to this appendix:

A.3.2.1 Development agreement. The formal documentation of the agreed-upon tasks that the developer will execute for the program manager. For a commercial developer, this agreement usually is in the form of a written contract.

A.3.2.2 Fail-safe. A design feature that ensures the system remains safe, or in the event of a failure, causes the system to revert to a state that will not cause a mishap.

A.3.2.3 Health hazard assessment. The application of biomedical knowledge and principles to identify and eliminate or control health hazards associated with systems in direct support of the life-cycle management of materiel items.

A.3.2.4 Mishap probability. The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap.

A.3.2.5 Mishap probability levels. An arbitrary categorization that provides a qualitative measure of the most reasonable likelihood of occurrence of a mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.6 Mishap risk assessment. The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

A.3.2.7 Mishap risk categories. An arbitrary categorization of mishap risk assessment values often used to generate specific action such as mandatory reporting of certain hazards to management for action, or formal acceptance of the associated mishap risk.

A.3.2.8 Mishap severity. An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard.

A.3.2.9 Mishap severity category. An arbitrary categorization that provides a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

A.3.2.10 Safety critical. A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component).

## MIL-STD-882D APPENDIX A

A.3.2.11 System safety management. All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the development, test, acquisition, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities.

### A.4 GENERAL REQUIREMENTS

A.4.1 General. System safety applies engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle. It draws upon professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the environmental, safety, and health mishap risk associated with a system. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given. The program manager and the developer must apply this emphasis during all phases of the system's life cycle. A safe design is a prerequisite for safe operations, with the goal being to produce an inherently safe product that will have the minimum safety-imposed operational restrictions.

A.4.1.1 System safety in environmental and health hazard management. DoD 5000.2-R has directed the integration of environmental, safety, and health hazard management into the systems engineering process. While environmental and health hazard management are normally associated with the application of statutory direction and requirements, the management of mishap risk associated with actual environmental and health hazards is directly addressed by the system safety approach. Therefore, environmental and health hazards can be analyzed and managed with the same tools as any other hazard, whether they affect equipment, the environment, or personnel.

A.4.2 Purpose (see 1.1). All DoD program managers shall establish and execute programs that manage the probability and severity of all hazards for their systems (DoD 5000.2-R). Provision for system safety requirements and effort as defined by this standard should be included in all applicable contracts negotiated by DoD. These contracts include those negotiated within each DoD agency, by one DoD agency for another, and by DoD for other Government agencies. In addition, each DoD in-house program will address system safety.

A.4.2.1 Solicitations and contracts. Apply the requirements of section 4 to acquisitions. Incorporate MIL-STD-882 in the list of contractual compliance documents, and include the potential of a developer to execute section 4 requirements as source selection evaluation criteria. Developers are encouraged to submit with their proposal a preliminary plan that describes the system safety effort required for the requested program. When directed by the program manager, attach this preliminary plan to the contract or reference it within the statement of work; so it becomes the basis for a contractual system safety program.

A.4.3 System safety planning. Before formally documenting the system safety approach, the program manager, in concert with systems engineering and associated system safety

MIL-STD-882D  
APPENDIX A

professionals, must determine what system safety effort is necessary to meet program and regulatory requirements. This effort will be built around the requirements set forth in section 4 and includes developing a planned approach for safety task accomplishment, providing qualified people to accomplish the tasks, establishing the authority for implementing the safety tasks through all levels of management, and allocating appropriate resources to ensure that the safety tasks are completed.

A.4.3.1 System safety planning subtasks. System safety planning subtasks should:

a. Establish specific safety performance requirements (see A.4.3.2) based on overall program requirements and system user inputs.

b. Establish a system safety organization or function and the required lines of communication with associated organizations (government and contractor). Establish interfaces between system safety and other functional elements of the program, as well as with other safety and engineering disciplines (such as nuclear, range, explosive, chemical, and biological). Designate the organizational unit responsible for executing each safety task. Establish the authority for resolution of identified hazards.

c. Establish system safety milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

d. Establish an incident alerting/notification, investigation, and reporting process, to include notification of the program manager.

e. Establish an acceptable level of mishap risk, mishap probability and severity thresholds, and documentation requirements (including but not limited to hazards and residual mishap risk).

f. Establish an approach and methodology for reporting to the program manager the following minimum information:

- (1) Safety critical characteristics and features.
- (2) Operating, maintenance, and overhaul safety requirements.
- (3) Measures used to eliminate or mitigate hazards.
- (4) Acquisition management of hazardous materials.

g. Establish the method for the formal acceptance and documenting of residual mishap risks and the associated hazards.

h. Establish the method for communicating hazards, the associated risks, and residual mishap risk to the system user.

MIL-STD-882D  
APPENDIX A

i. Specify requirements for other specialized safety approvals (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) as necessary (reference 6.6 and 6.7).

A.4.3.2 Safety performance requirements. These are the general safety requirements needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate them into the system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of: a hazard category developed through a mishap risk assessment matrix; an overall system mishap rate; demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable mishap risk assessment procedures. Listed below are examples of safety performance statements.

a. Quantitative requirements. Quantitative requirements are usually expressed as a failure or mishap rate, such as "The catastrophic system mishap rate shall not exceed  $x.xx \times 10^{-y}$  per operational hour."

b. Mishap risk requirements. Mishap risk requirements could be expressed as "No hazards assigned a Catastrophic mishap severity are acceptable." Mishap risk requirements could also be expressed as a level defined by a mishap risk assessment (see A.4.4.3.2.3), such as "No Category 3 or higher mishap risks are acceptable."

c. Standardization requirements. Standardization requirements are expressed relative to a known standard that is relevant to the system being developed. Examples include: "The system will comply with the laws of the State of XXXXX and be operable on the highways of the State of XXXXX" or "The system will be designed to meet ANSI Std XXX as a minimum."

A.4.3.3 Safety design requirements. The program manager, in concert with the chief engineer and utilizing systems engineering and associated system safety professionals, should establish specific safety design requirements for the overall system. The objective of safety design requirements is to achieve acceptable mishap risk through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources. Review these for safety design parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. Expand these requirements and criteria for inclusion in the associated follow-on or lower level specifications. See general safety system design requirements below.

a. Hazardous material use is minimized, eliminated, or associated mishap risks are reduced through design, including material selection or substitution. When using potentially hazardous materials, select those materials that pose the least risk throughout the life cycle of the system.

MIL-STD-882D  
APPENDIX A

- b. Hazardous substances, components, and operations are isolated from other activities, areas, personnel, and incompatible materials.
- c. Equipment is located so that access during operations, servicing, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous substances, high voltage, electromagnetic radiation, and cutting and puncturing surfaces).
- d. Protect power sources, controls, and critical components of redundant subsystems by physical separation or shielding, or by other acceptable methods.
- f. Consider safety devices that will minimize mishap risk (e.g., interlocks, redundancy, fail safe design, system protection, fire suppression, and protective measures such as clothing, equipment, devices, and procedures) for hazards that cannot be eliminated. Make provisions for periodic functional checks of safety devices when applicable.
- g. System disposal (including explosive ordnance disposal) and demilitarization are considered in the design.
- h. Implement warning signals to minimize the probability of incorrect personnel reaction to those signals, and standardize within like types of systems.
- i. Provide warning and cautionary notes in assembly, operation, and maintenance instructions; and provide distinctive markings on hazardous components, equipment, and facilities to ensure personnel and equipment protection when no alternate design approach can eliminate a hazard. Use standard warning and cautionary notations where multiple applications occur. Standardize notations in accordance with commonly accepted commercial practice or, if none exists, normal military procedures. Do not use warning, caution, or other written advisory as the only risk reduction method for hazards assigned to Catastrophic or Critical mishap severity categories.
- j. Safety critical tasks may require personnel proficiency; if so, the developer should propose a proficiency certification process to be used.
- k. Severity of injury or damage to equipment or the environment as a result of a mishap is minimized.
- l. Inadequate or overly restrictive requirements regarding safety are not included in the system specification.
- m. Acceptable risk is achieved in implementing new technology, materials, or designs in an item's production, test, and operation. Changes to design, configuration, production, or mission requirements (including any resulting system modifications and upgrades, retrofits, insertions of new technologies or materials, or use of new production or test techniques) are accomplished in a manner that maintains an acceptable level of mishap risk. Changes to the environment in which the system operates are analyzed to identify and mitigate any resulting hazards or changes in mishap risks.

MIL-STD-882D  
APPENDIX A

A.4.3.3.1 Some program managers include the following conditions in their solicitation, system specification, or contract as requirements for the system design. These condition statements are used optionally as supplemental requirements based on specific program needs.

A.4.3.3.1.1 Unacceptable conditions. The following safety critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the mishap risk associated with these situations to a level acceptable to the program manager.

- a. Single component failure, common mode failure, human error, or a design feature that could cause a mishap of Catastrophic or Critical mishap severity categories.
- b. Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of Catastrophic or Critical mishap severity categories.
- c. Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.
- d. Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.
- e. Hazard categories that are specified as unacceptable in the development agreement.

A.4.3.3.1.2 Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigating actions are implemented and verified.

- a. For non-safety critical command and control functions: a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.
- b. For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors.
- c. System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.
- d. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.
- e. System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

MIL-STD-882D  
APPENDIX A

f. System designs that provide an approved safety factor, or a fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

g. System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).

h. System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin.

i. System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction has been provided.

j. System designs that limit or control the use of hazardous materials.

A.4.3.4 Elements of an effective system safety effort. Elements of an effective system safety effort include:

a. Management is always aware of the mishap risks associated with the system, and formally documents this awareness. Hazards associated with the system are identified, assessed, tracked, monitored, and the associated risks are either eliminated or controlled to an acceptable level throughout the life cycle. Identify and archive those actions taken to eliminate or reduce mishap risk for tracking and lessons learned purposes.

b. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

c. Environmental protection, safety, and occupational health, consistent with mission requirements, are designed into the system in a timely, cost-effective manner. Inclusion of the appropriate safety features is accomplished during the applicable phases of the system life cycle.

d. Mishap risk resulting from harmful environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration) and human error in system operation and support is minimized.

e. System users are kept abreast of the safety of the system and included in the safety decision process.

A.4.4 System safety engineering effort. As stated in section 4, a system safety engineering effort consists of eight main requirements. The following paragraphs provide further descriptions on what efforts are typically expected due to each of the system safety requirements listed in section 4.

A.4.4.1 Documentation of the system safety approach. The documentation of the system safety approach should describe the planned tasks and activities of system safety management

MIL-STD-882D  
APPENDIX A

and system engineering required to identify, evaluate, and eliminate or control hazards, or to reduce the residual mishap risk to a level acceptable throughout the system life cycle. The documentation should describe, as a minimum, the four elements of an effective system safety effort: a planned approach for task accomplishment, qualified people to accomplish tasks, the authority to implement tasks through all levels of management, and the appropriate commitment of resources (both manning and funding) to ensure that safety tasks are completed. Specifically, the documentation should:

a. Describe the scope of the overall system program and the related system safety effort. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.

b. Describe the safety tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety and reference where they are specified or described. Include the organizational relationships between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization including the review and approval authority of those tasks.

c. Describe specific analysis techniques and formats to be used in qualitative or quantitative assessments of hazards, their causes, and effects.

d. Describe the process through which management decisions will be made (for example, timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, and program deviations). Include a description on how residual mishap risk is formally accepted and this acceptance is documented.

e. Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability levels, and the system safety design order of precedence that should be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for mishap risk assessment including a description of the acceptable and unacceptable risk levels (if applicable). Include system safety definitions that modify, deviate from, or are in addition to those in this standard or generally accepted by the system safety community (see *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook*) (see A.6.1).

f. Describe how resolution and action relative to system safety will be implemented at the program management level possessing resolution authority.

g. Describe the verification (e.g., test, analysis, demonstration, or inspection) requirements for ensuring that safety is adequately attained. Identify any certification requirements for software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).

MIL-STD-882D  
APPENDIX A

h. Describe the mishap or incident notification, investigation, and reporting process for the program, including notification of the program manager.

i. Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned data. Include a description on how a system hazard log is developed and kept current (see A.4.4.8.1).

j. Describe how the user is kept abreast of residual mishap risk and the associated hazards.

A.4.4.2 Identification of hazards. Identify hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended usage or application. Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

A.4.4.2.1 Approaches for identifying hazards. Numerous approaches have been developed and used to identify system hazards. A key aspect of many of these approaches is empowering the design engineer with the authority to design safe systems and the responsibility to identify to program management the hazards associated with the design. Hazard identification approaches often include using system users in the effort. Commonly used approaches for identifying hazards can be found in the *Defense Acquisition Deskbook* and System Safety Society's *System Safety Analysis Handbook* (see A.6.1)

A.4.4.3 Assessment of mishap risk. Assess the severity and probability of the mishap risk associated with each identified hazard, i.e., determine the potential impact of the hazard on personnel, facilities, equipment, operations, the public, or environment, as well as on the system itself. Other factors, such as numbers of persons exposed, may also be used to assess risk.

A.4.4.3.1 Mishap risk assessment tools. To determine what actions to take to eliminate or control identified hazards, a system of determining the level of mishap risk involved must be developed. A good mishap risk assessment tool will enable decision makers to properly understand the level of mishap risk involved, relative to what it will cost in schedule and dollars to reduce that mishap risk to an acceptable level.

A.4.4.3.2 Tool development. The key to developing most mishap risk assessment tools is the characterization of mishap risks by mishap severity and mishap probability. Since the highest system safety design order of precedence is to eliminate hazards by design, a mishap risk assessment procedure considering only mishap severity will generally suffice during the early design phase to minimize the system's mishap risks (for example, just don't use hazardous or toxic material in the design). When all hazards cannot be eliminated during the early design phase, a mishap risk assessment procedure based upon the mishap probability as well as the mishap severity provides a resultant mishap risk assessment. The assessment is used to establish priorities for corrective action, resolution of identified hazards, and notification to management of the mishap risks. The information provided here is a suggested tool and set of definitions that can be used. Program managers can develop tools and definitions appropriate to their individual programs.

MIL-STD-882D  
APPENDIX A

A.4.4.3.2.1 Mishap severity. Mishap severity categories are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table A-I. The dollar values shown in this table should be established on a system by system basis depending on the size of the system being considered to reflect the level of concern.

**TABLE A-I. Suggested mishap severity categories.**

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding \$10K but less than \$200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding \$2K but less than \$10K, or minimal environmental damage not violating law or regulation.

NOTE: These mishap severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the program manager and the developer as to the meaning of the terms used in the category definitions. Other risk assessment techniques may be used provided that the user approves them.

A.4.4.3.2.2 Mishap probability. Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be

MIL-STD-882D  
APPENDIX A

derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table A-II.

**TABLE A-II. Suggested mishap probability levels.**

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than $10^{-1}$ in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than $10^{-1}$ but greater than $10^{-2}$ in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than $10^{-2}$ but greater than $10^{-3}$ in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than $10^{-3}$ but greater than $10^{-6}$ in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than $10^{-6}$ in that life.	Unlikely to occur, but possible.

\*Definitions of descriptive words may have to be modified based on quantity of items involved.

\*\*The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

A.4.4.3.2.3 Mishap risk assessment. Mishap risk classification by mishap severity and mishap probability can be performed by using a mishap risk assessment matrix. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is then often used to rank different hazards as to their associated mishap risks. An example of a mishap risk assessment matrix is shown at Table A-III.

MIL-STD-882D  
APPENDIX A

**TABLE A-III. Example mishap risk assessment values.**

SEVERITY	Catastrophic	Critical	Marginal	Negligible
PROBABILITY				
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

A.4.4.3.2.4 Mishap risk categories. Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table A-IV includes an example listing of mishap risk categories and the associated assessment values. In the example, the system management has determined that mishap risk assessment values 1 through 5 constitute “High” risk while values 6 through 9 constitute “Serious” risk.

**TABLE A-IV. Example mishap risk categories and mishap risk acceptance levels.**

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

\*Representative mishap risk acceptance levels are shown in the above table. Mishap risk acceptance is discussed in paragraph A.4.4.7. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

A.4.4.3.2.5 Mishap risk impact. The mishap risk impact is assessed, as necessary, using other factors to discriminate between hazards having the same mishap risk value. One might discriminate between hazards with the same mishap risk assessment value in terms of mission capabilities, or social, economic, and political factors. Program management will closely consult with the using organization on the decisions used to prioritize resulting actions.

A.4.4.3.3 Mishap risk assessment approaches. Commonly used approaches for assessing mishap risk can be found in the *Defense Acquisition Deskbook* and System Safety Society’s *System Safety Analysis Handbook* (see A.6.1)

## MIL-STD-882D APPENDIX A

A.4.4.4 Identification of mishap risk mitigation measures. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority.

A.4.4.4.1 Prioritize hazards for corrective action. Hazards should be prioritized so that corrective action efforts can be focused on the most serious hazards first. A categorization of hazards may be conducted according to the mishap risk potential they present.

A.4.4.4.2 System safety design order of precedence (see 4.4). The ultimate goal of a system safety program is to design systems that contain no hazards. However, since the nature of most complex systems makes it impossible or impractical to design them completely hazard-free, a successful system safety program often provides a system design where there exist no hazards resulting in an unacceptable level of mishap risk. As hazard analyses are performed, hazards will be identified that will require resolution. The system safety design order of precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk are evaluated so that an acceptable method for mishap risk reduction can be agreed to.

A.4.4.5 Reduction of mishap risk to an acceptable level. Reduce the system mishap risk through a mitigation approach mutually agreed to by the developer, program manager and the using organization.

A.4.4.5.1 Communication with associated test efforts. Residual mishap risk and associated hazards must be communicated to the system test efforts for verification.

A.4.4.6 Verification of mishap risk reduction. Verify the mishap risk reduction and mitigation through appropriate analysis, testing, or inspection. Document the determined residual mishap risk. The program manager must ensure that the selected mitigation approaches will result in the expected residual mishap risk. To provide this assurance, the system test effort should verify the performance of the mitigation actions. New hazards identified during testing must be reported to the program manager and the developer.

A.4.4.6.1 Testing for a safe design. Tests and demonstrations must be defined to validate selected safety features of the system. Test or demonstrate safety critical equipment and procedures to determine the mishap severity or to establish the margin of safety of the design. Consider induced or simulated failures to demonstrate the failure mode and acceptability of safety critical equipment. When it cannot be analytically determined whether the corrective action taken will adequately control a hazard, conduct safety tests to evaluate the effectiveness of the controls. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation. Integrate testing of safety systems into appropriate system test and demonstration plans to the maximum extent possible.

MIL-STD-882D  
APPENDIX A

A.4.4.6.2 Conducting safe testing. The program manager must ensure that test teams are familiar with mishap risks of the system. Test plans, procedures, and test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation should be reviewed to ensure that:

- a. Safety is adequately demonstrated.
- b. The testing will be conducted in a safe manner.
- c. All additional hazards introduced by testing procedures, instrumentation, test hardware, and test environment are properly identified and controlled.

A.4.4.6.3 Communication of new hazards identified during testing. Testing organizations must ensure that hazards and safety discrepancies discovered during testing are communicated to the program manager and the developer.

A.4.4.7 Review and acceptance of residual mishap risk by the appropriate authority. Notify the program manager of identified hazards and residual mishap risk. For long duration programs, incremental or periodic reporting should be used.

A.4.4.7.1 Residual mishap risk. The mishap risk that remains after all planned mishap risk management measures have been implemented is considered residual mishap risk. Residual mishap risk is documented along with the reason(s) for incomplete mitigation.

A.4.4.7.2 Residual mishap risk management. The program manager must know what residual mishap risk exists in the system being acquired. For significant mishap risks, the program manager is required to elevate reporting of residual mishap risk to higher levels of appropriate authority (such as the Program Executive Officer or Component Acquisition Executive) for action or acceptance. The program manager is encouraged to apply additional resources or other remedies to help the developer satisfactorily resolve hazards providing significant mishap risk. Table A-IV includes an example of a mishap risk acceptance level matrix based on the mishap risk assessment value and mishap risk category.

A.4.4.7.3 Residual mishap risk acceptance. The program manager is responsible for formally documenting the acceptance of the residual mishap risk of the system by the appropriate authority. The program manager should update this residual mishap risk and the associated hazards to reflect changes/modifications in the system or its use. The program manager and using organization should jointly determine the updated residual mishap risk prior to acceptance of the risk and system hazards by the risk acceptance authority, and should document the agreement between the user and the risk acceptance authority.

A.4.4.8 Tracking hazards and residual mishap risk. Track hazards, their closures, and residual mishap risk. A tracking system for hazards, their closures, and residual mishap risk must be maintained throughout the system life cycle. The program manager must keep the system user apprised of system hazards and residual mishap risk.

## MIL-STD-882D APPENDIX A

A.4.4.8.1 Process for tracking of hazards and residual mishap risk. Each system must have a current log of identified hazards and residual mishap risk, including an assessment of the residual mishap risk (see A.4.4.7). As changes are integrated into the system, this log is updated to incorporate added or changed hazards and the associated residual mishap risk. The Government must formally acknowledge acceptance of system hazards and residual mishap risk. Users will be kept informed of hazards and residual mishap risk associated with their systems.

A.4.4.8.1.1 Developer responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The developer (see 3.2.2) is responsible for communicating information to the program manager on system hazards and residual mishap risk, including any unusual consequences and costs associated with hazard mitigation. After attempting to eliminate or mitigate system hazards, the developer will formally document and notify the program manager of all hazards breaching thresholds set in the safety design criteria. At the same time, the developer will also communicate the system residual mishap risk.

A.4.4.8.1.2 Program manager responsibilities for communications, acceptance, and tracking of hazards and residual mishap risk. The program manager is responsible for maintaining a log of all identified hazards and residual mishap risk for the system. The program manager will communicate known hazards and associated risks of the system to all system developers and users. As changes are integrated into the system, the program manager shall update this log to incorporate added or changed hazards and the residual mishap risk identified by the developer. The program manager is also responsible for informing system developers about the program manager's expectations for handling of newly discovered hazards. The program manager will evaluate new hazards and the resulting residual mishap risk, and either recommend further action to mitigate the hazards, or formally document the acceptance of these hazards and residual mishap risk. The program manager will evaluate the hazards and associated residual mishap risk in close consultation and coordination with the ultimate end user, to assure that the context of the user requirements, potential mission capability, and the operational environment are adequately addressed. Copies of the documentation of the hazard and risk acceptance will be provided to both the developer and the system user. Hazards for which the program manager accepts responsibility for mitigation will also be included in the formal documentation. For example, if the program manager decides to execute a special training program to mitigate a potentially hazardous situation, this approach will be documented in the formal response to the developer. Residual mishap risk and hazards must be communicated to system test efforts for verification.

### A.5 SPECIFIC REQUIREMENTS

A.5.1 Program manager responsibilities. The program manager must ensure that all types of hazards are identified, evaluated, and mitigated to a level compliant with acquisition management policy, federal (and state where applicable) laws and regulations, Executive Orders, treaties, and agreements. The program manager should:

A.5.1.1 Establish, plan, organize, implement, and maintain an effective system safety effort that is integrated into all life cycle phases.

MIL-STD-882D  
APPENDIX A

A.5.1.2 Ensure that system safety planning is documented to provide all program participants with visibility into how the system safety effort is to be conducted.

A.5.1.3 Establish definitive safety requirements for the procurement, development, and sustainment of the system. The requirements should be set forth clearly in the appropriate system specifications and contractual documents.

A.5.1.4 Provide historical safety data to developers.

A.5.1.5 Monitor the developer's system safety activities and review and approve delivered data in a timely manner, if applicable, to ensure adequate performance and compliance with safety requirements.

A.5.1.6 Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

A.5.1.7 Evaluate new lessons learned for inclusion into appropriate databases and submit recommendations to the responsible organization.

A.5.1.8 Establish system safety teams to assist the program manager in developing and implementing a system safety effort.

A.5.1.9 Provide technical data on Government-furnished Equipment or Government-furnished Property to enable the developer to accomplish the defined tasks.

A.5.1.10 Document acceptance of residual mishap risk and associated hazards.

A.5.1.11 Keep the system users apprised of system hazards and residual mishap risk.

A.5.1.12 Ensure the program meets the intent of the latest MIL-STD 882.

A.5.1.13 Ensure adequate resources are available to support the program system safety effort.

A.5.1.14 Ensure system safety technical and managerial personnel are qualified and certified for the job.

## A.6 NOTES

A.6.1 DoD acquisition practices and safety analysis techniques. Information on DoD acquisition practices and safety analysis techniques is available at the referenced Internet sites. Nothing in the referenced information is considered binding or additive to the requirements provided in this standard.

A.6.1.1 *Defense Acquisition Deskbook*. Wright-Patterson Air Force Base, Ohio: Deskbook Joint Program Office.

MIL-STD-882D  
APPENDIX A

A.6.1.2 *System Safety Analysis Handbook*. Unionville, VA: System Safety Society.

MIL-STD-882D

CONCLUDING MATERIAL

Custodians:

Army - AV

Navy - AS

Air Force - 40

Preparing activity:

Air Force - 40

Project SAFT - 0038

Reviewing activities:

Army - AR, AT, CR, MI

Navy - EC, OS, SA, SH

Air Force - 10, 11, 13, 19

## STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

### INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7, and send to preparing activity.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

<b>I RECOMMEND A CHANGE:</b>	1. <b>DOCUMENT NUMBER</b> <b>MIL-STD-882</b>	2. <b>DOCUMENT DATE (YYYYMMDD)</b> <b>20000210</b>
3. <b>DOCUMENT TITLE</b> <b>System Safety</b>		
4. <b>NATURE OF CHANGE</b> ( <i>Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.</i> )		
5. <b>REASON FOR RECOMMENDATION</b>		
6. <b>SUBMITTER</b>		
a. <b>NAME</b> ( <i>Last, First, Middle Initial</i> )		b. <b>ORGANIZATION</b>
c. <b>ADDRESS</b> ( <i>Include zip code</i> )	d. <b>TELEPHONE</b> ( <i>Include Area Code</i> ) (1) Commercial (2) DSN ( <i>if applicable</i> )	7. <b>DATE SUBMITTED</b> (YYYYMMDD)
8. <b>PREPARING ACTIVITY</b>		
a. <b>NAME</b> Headquarters, Air Force Materiel Command System Safety Division		b. <b>TELEPHONE</b> ( <i>Include Area Code</i> ) (1) Commercial (937) 257-6007 (2) DSN 787-6007
b. <b>ADDRESS</b> ( <i>Include Zip Code</i> ) HQ AFMC/SES 4375 Chidlaw Road Wright Patterson AFB, Ohio 45433-5006		<b>IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:</b> Defense Standardization Program Office (DLSC-LM) 8725 John J. Kingman Road, Suite 2533 Fort Belvoir, Virginia 22060-6621 Telephone 703 767-6888 DSN 427-6888

## Appendix J

### Software Safety

<b>SOFTWARE SAFETY .....</b>	<b>1</b>
<b>J.0 SOFTWARE SAFETY DURING LIFE CYCLE PHASES.....</b>	<b>2</b>

FAA System Safety Handbook, Appendix J: Software Safety  
December 30, 2000

## J.0 Software Safety During Life Cycle Phases

The safety process should support a structured program life cycle model that incorporates both the system design and engineering process and the software acquisition process. Prominent software life cycle models include the waterfall and spiral methodologies. Although different models may carry different lifecycle emphasis, the adopted model should not affect the safety process itself. For discussion purposes only, this enclosure adopts a waterfall model (subject to IEEE/IEA Standard for Information Technology-software life cycle processes No. 12207.) For brevity, only the development phase of the Standard is addressed in terms of the relationship to software safety activities.

### J.1 Safety Critical Software Development

A structured development environment and an organization using state-of-the-art methods are prerequisites to developing dependable safety critical software. The following requirements and guidelines are intended to carry out the cardinal safety rule and its corollary that no single event or action shall be allowed to initiate a potentially hazardous event. The system, upon detection of an unsafe condition or command, shall inhibit the potentially hazardous event sequence and originate procedures/functions to bring the system to a predetermined "safe" state.

The purpose of this section is to describe the software safety activities that should be incorporated into the software development phases of project development. The software safety information that should be included in the documents produced during these phases is also discussed. The term "software components" is used in a general sense to represent important software development products such as software requirements, software designs, software code or program sets, software tests, etc.

### J.2 Software Concept and Initiation Phase

For most projects this lifecycle phase involves system level requirements and design development. Although most project work during this phase is concentrated on the subsystem level, software development has several tasks that must be initiated. These include the creation of important software documents and plans that will determine how, what, and when important software products will be produced or activities will be conducted. Each of the following documents should address software safety issues:

<b>Document</b>	<b>Software Safety Section</b>
System Safety Plan	Include software as a subsystem. Identify tasks.
Software Concepts Document	Identify safety critical processes.
Software Management Plan, and Software Configuration Management Plan	Coordination with systems safety tasks, flowdown incorporation of safety requirements. Applicability to safety critical software.
Software Security Plan	Security of safety critical software
Software Quality Assurance Plan	Support to software safety, verification of software safety requirements, safety participation in software reviews and inspections.

### J.3 Software Requirements Phase

The cost of correcting software faults and errors escalates dramatically as the development life cycle progresses, making it important to correct errors and implement correct software requirements from the very beginning. Unfortunately, it is generally impossible to eliminate all errors. Software developers must therefore work toward two goals: developing complete and correct requirements, and correcting code to develop fault-tolerant designs that will detect and compensate for software faults. The second goal is required because the first is usually impossible to accomplish.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

This section of the handbook describes the software safety team involvement in developing safety requirements for software. The software safety requirements can be top-down (flowed down from system requirements) and/or bottom-up (derived from hazard analyses). In some organizations, top-down flow is the only permitted route for requirements into software, and in those cases, newly derived bottom-up safety requirements must be flowed back into the system specification.

The requirements of software components are typically expressed as functions with corresponding inputs, processes, and outputs, plus additional requirements on interfaces, limits, ranges, precision, accuracy, and performance. There may also be requirements on the data of the program set - its attributes, relationships, and persistence, among others.

Software safety requirements are derived from the system and subsystem safety requirements developed to mitigate hazards identified in the Preliminary, System, and Subsystems Hazard Analyses.

Also, the assigned safety engineer flows requirements to systems engineering. The systems engineering group and the software development group have a responsibility to coordinate and negotiate requirement flowdown to be consistent with the software safety requirement flowdown.

The software safety organization should flow requirements into the Software Requirements Document (SRD) and the Software Interface Specification (SIS) or Interfaces Control Document (ICD). Safety-related requirements must be clearly identified in the SRD

SIS activities identify, define, and document interface requirements internal to the sub-system in which software resides, and between system (including hardware and operator interfaces), subsystem, and program set components and operation procedures. Note that the SIS is sometimes effectively contained in the SRD, or within an Interface Control Document (ICD) which defines all system interfaces, including hardware to hardware, hardware to software, and software to software.

### **J.3.1 Development of Software Safety Requirements**

Software safety requirements are obtained from several sources, and are of two types: generic and specific. The generic category of software safety requirement is derived from sets of requirements that can be used in different programs and environments to solve common software safety problems. Examples of generic software safety requirements and their sources are given in **Section J.1.4.3** Generic Software Safety Requirements. Specific software safety requirements are system unique functional capabilities or constraints that are identified in three ways:

- Through top down analysis of system design requirements (from specifications): The system requirements may identify system hazards up-front, and specify which system functions are safety critical. The (software) safety organization participates or leads the mapping of these requirements to software.
- From the Preliminary Hazard Analysis (PHA): The PHA looks down into the system from the point of view of system hazards. Preliminary hazard causes are mapped to, or interact with, software. Software hazard control features are identified and specified as requirements.
- Through bottom up analysis of design data, (e.g. flow diagrams, FMEAs, fault trees etc.)

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

Design implementations allowed but not anticipated by the system requirements are analyzed and new hazard causes are identified. Software hazard controls are specified via requirements when the hazard causes map to, or interact with, software.

### **J.3.2 Safety Requirements Flowdown**

Generic safety requirements are established “a priori” and placed into the system specification and/or overall project design specifications. From there they are flowed into lower level unit and module specifications. Other safety requirements, derived from bottom-up analysis, are flowed up from subsystems and components to the system level requirements. These new system level requirements are then flowed down across all affected subsystems. During the System Requirements Phase, subsystems and components may not be well defined. In this case, bottom-up analysis might not be possible until the Architectural Design Phase or even later.

An area of concern in the flowdown process is incomplete analysis, and/or inconsistent analysis of highly complex systems, or use of ad hoc techniques by biased or inexperienced analysts. The most rigorous (and most expensive) method of addressing this concern is adoption of formal methods for requirements analysis and flowdown. Less rigorous and less expensive ways include checklists and/or a standardized structured approach to software safety as discussed below and throughout this guidebook.

The following section contain a description of the type of analysis and gives the methodology by defining the task, the resources required to perform the analysis, and the expected output from the analyses.

#### ***Checklists and cross references***

Tools and methods for requirement flow down analyses include checklists and cross-references. A checklist of required hazard controls and their corresponding safety requirements should be created and maintained. Then they can be used throughout the development life cycle to ensure proper flow down and mapping to design, code and test.

- Develop a systematic checklist of software safety requirements and any hazard controls, ensuring they correctly and completely include (and cross reference) the appropriate specifications, hazard analyses test and design documents. This should include both generic and specific safety requirements.
- Develop a hazard requirement flowdown matrix that maps safety requirements and hazard controls to system/software functions and to software modules and components. Where components are not yet defined, flow to the lowest level possible and tag for future flowdown.

#### ***Requirements Criticality Analysis***

Criticality analysis identifies program requirements that have safety implications. A method of applying criticality analysis is to analyze the risks of the software/hardware system and identify those that could present catastrophic or critical risks. This approach evaluates each program requirement in terms of the safety objectives derived for the software component.

The evaluation will determine whether the requirement has safety implications and, if so, the requirement is designated “safety critical”. It is then placed into a tracking system to ensure traceability of software requirements throughout the software development cycle from the highest-level specification all the way to the code and test documentation. All of the following techniques are focused on safety critical software components.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

The system safety organization coordinates with the project system engineering organization to review and agree on the criticality designations. At this point the systems engineers may elect to make design changes to reduce the criticality levels or consolidate modules reducing the number of critical modules.

At this point, some bottom-up analyses can be performed. Bottom-up analyses identify requirements or design implementations that are inconsistent with, or not addressed by, system requirements. Bottom-up analyses can also reveal unexpected pathways (e.g., sneak circuits) for reaching hazardous or unsafe states. System requirements should be corrected when necessary.

It is possible that software components or subsystems might not be defined during the Requirements Phase, so those portions of the Criticality Analysis would be deferred to the Architectural Design Phase. In any case, the Criticality Analysis will be updated during the Architectural Design Phase to reflect the more detailed definition of software components.

The methodology for Requirements Criticality Analysis is:

- All software requirements are analyzed in order to identify additional potential system hazards that the system PHA did not reveal and to identify potential areas where system requirements were not correctly flowed to the software. Identified potential hazards are then addressed by adding or changing the system requirements and reflowing them to hardware, software and operations as appropriate.
- At the system level: identify hardware or software items that receive/pass/initiate critical signals or hazardous commands.
- At the software requirements level: identify software functions or objects that receive/pass/initiate critical signals or hazardous commands.
- This safety activity examines the system/software requirements and design to identify unsafe conditions for resolution such as out-of-sequence, wrong event, inappropriate magnitude, incorrect polarity, inadvertent command, adverse environment, deadlocking, and failure-to-command modes.
- The software safety requirements analysis considers such specific requirements as the characteristics discussed below as critical software characteristics.

The following resources are available for the Requirements Criticality Analysis. Note: documents in brackets correspond to terminology from DOD-STD-2167. Other document names correspond to NASA-STD-2100.91.

- Software Development Activities Plan [Software Development Plan] Software Assurance Plan [None], Software Configuration Management Plan [Same] and Risk Management Plan [Software Development Plan].
- System and Subsystem Requirements [System/Segment Specification (SSS), System/Segment Design Document].
- Requirements Document [Software Requirements Specifications].
- External Interface Requirements Document [Interface Requirements Specifications] and other interface documents.
- Functional Flow Diagrams and related data.

FAA System Safety Handbook, Appendix J: Software Safety  
December 30, 2000

- Program structure documents.
- Storage and timing analyses and allocations.
- Background information relating to safety requirements associated with the contemplated testing, manufacturing, storage, repair, installation, use, and final disposition of the system.
- Information from the system PHA concerning system energy, toxic, and other hazardous event sources, especially ones that may be controlled directly or indirectly by software.
- Historical data such as lessons learned from other systems and problem reports.

Output products are the following:

- Updated Safety Requirements Checklist
- Definition of Safety Critical Requirements.

The results and findings of the Criticality Analyses should be fed to the System Requirements and System Safety Analyses. For all discrepancies identified, either the requirements should be changed because they are incomplete or incorrect, or else the design must be changed to meet the requirements. The analysis identifies additional hazards that the system analysis did not include, and identifies areas where system or interface requirements were not correctly assigned to the software.

The results of the criticality analysis may be used to develop Formal Inspection checklists for performing the formal inspection process described later in INSERT REFERENCE.

### ***Critical Software Characteristics***

Many characteristics are governed by requirements, but some may not be.

All characteristics of safety critical software must be evaluated to determine if they are safety critical. Safety critical characteristics should be controlled by requirements that receive rigorous quality control in conjunction with rigorous analysis and test. Often all characteristics of safety critical software are themselves safety critical.

Characteristics to be considered include at a minimum:

- Specific limit ranges
- Out of sequence event protection requirements (e.g., if-then statements)
- Timing
- Relationship logic for limits. Allowable limits for parameters might vary depending on operational mode or mission phase. Expected pressure in a tank varies with temperature, for example.
- Voting logic
- Hazardous command processing requirements (fault response)
- Fault detection, isolation, and recovery

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

- Redundancy management/switchover logic; what to switch and under what circumstances, should be defined as methods to control hazard causes identified in the hazards analyses. For example, equipment that has lost control of a safety critical function should be switched to a good spare before the time to criticality has expired. Hot standby units (as opposed to cold standby) should be provided where a cold start time would exceed time to criticality.

This list is not exhaustive and often varies depending on the system architecture and environment.

### J.3.3 Generic Software Safety Requirements

The generic category of software safety requirements are derived from sets of requirements and best practices used in different programs and environments to solve common software safety problems. Similar processors/platforms and/or software can suffer from similar or identical design problems. Generic software safety requirements capture these lessons learned and provide a valuable resource for developers.

Generic requirements prevent costly duplication of effort by taking advantage of existing proven techniques and lessons learned rather than reinventing techniques or repeating mistakes. Most development programs should be able to make use of some generic requirement; however, they should be used with care.

As technology evolves, or as new applications are implemented, new "generic" requirements will likely arise, and other sources of generic requirements might become available. A partial listing of generic requirement sources is shown below:

- EWRR (Eastern and Western Range Regulation) 127-1, Section 3.16.4 Safety Critical Computing System Software Design Requirements.
- AFISC SSH 1-1 System Safety Handbook - Software System Safety, Headquarters Air Force Inspection and Safety Center.
- EIA Bulletin SEB6-A System Safety Engineering in Software Development (Electrical Industries Association)
- Underwriters Laboratory - UL 1998 Standard for Safety - Safety-Related Software, January 4th, 1994

A listing of many of the generic software safety requirements is presented in the table below.

The failure of safety critical software functions shall be detected, isolated, and recovered from such that catastrophic and critical hazardous events are prevented from occurring.
Software shall perform automatic Failure Detection, Isolation, and Recovery (FDIR) for identified safety critical functions with a time to criticality under 24 hours
Automatic recovery actions taken shall be reported. There shall be no necessary response from ground operators to proceed with the recovery action.
The FDIR switchover software shall be resident on an available, non-failed control platform which is different from the one with the function being monitored.
Override commands shall require multiple operator actions.
Software shall process the necessary commands within the time to criticality of a hazardous event.
Hazardous commands shall only be issued by the controlling application, or by authorized ground personnel.
Software that executes hazardous commands shall notify ground personnel upon execution or provide the

FAA System Safety Handbook, Appendix J: Software Safety  
December 30, 2000

reason for failure to execute a hazardous command.
Prerequisite conditions (e.g., correct mode, correct configuration, component availability, proper sequence, and parameters in range) for the safe execution of an identified hazardous command shall be met before execution.
In the event that prerequisite conditions have not been met, the software shall reject the command and alert the ground personnel.
Software shall make available status of all software controllable inhibits to the ground personnel.
Software shall accept and process ground personnel commands to activate/deactivate software controllable inhibits.
Software shall provide an independent and unique command to control each software controllable inhibit.
Software shall incorporate the capability to identify and status each software inhibits associated with hazardous commands.
Software shall make available current status on software inhibits associated with hazardous commands to the ground personnel.
All software inhibits associated with a hazardous command shall have a unique identifier.
Each software inhibit command associated with a hazardous command shall be consistently identified using the rules and legal values.
If an automated sequence is already running when a software inhibit associated with a hazardous command is activated, the sequence shall complete before the software inhibit is executed.
Software shall have the ability to resume control of an inhibited operation after deactivation of a software inhibit associated with a hazardous command.
The state of software inhibits shall remain unchanged after the execution of an override.
Software shall provide error handling to support safety critical functions.
Software shall provide caution and warning status to the ground personnel.
Software shall provide for ground personnel forced execution of any automatic safing, isolation, or switchover functions.
Software shall provide for ground personnel forced termination of any automatic safing, isolation, or switchover functions.
Software shall provide procession for ground personnel commands in return to the previous mode or configuration of any automatic safing, isolation, or switchover function.
Software shall provide for ground personnel forced override of any automatic safing, isolation, or switchover functions.
Software shall provide fault containment mechanisms to prevent error propagation across replaceable unit interfaces.
Software (including firmware) Power On Self Test (POST) utilized within any replaceable unit or component shall be confined to that single system process controlled by the replaceable unit or component.
Software (including firmware) POST utilized within any replaceable unit or component shall terminate in a safe state.
Software shall initialize, start, and restart replaceable units to a safe state.
For systems solely using software for hazard risk mitigation, software shall require two independent command messages for a commanded system action that could result in a critical or catastrophic hazard.
Software shall require two independent operator actions to initiate or terminate a system function that could result in a critical hazard.
Software shall require three independent operator actions to initiate or terminate a system function that could result in a catastrophic hazard.
Operational software functions shall allow only authorized access.
Software shall provide proper sequencing (including timing) of safety critical commands.
Software termination shall result in a safe system state.
In the event of hardware failure, software faults that lead to system failures, or when the software detects a configuration inconsistent with the current mode of operation, the software shall have the capability to place

FAA System Safety Handbook, Appendix J: Software Safety  
December 30, 2000

the system into a safe state.
When the software is notified of or detects hardware failures, software faults that lead to system failures, or a configuration inconsistent with the current mode of operation, the software shall notify the crew, ground operators, or the controlling executive.
Hazardous processes and safing processes with a time to criticality such that timely human intervention may not be available, shall be automated (i.e., not require ground personnel intervention to begin or complete).
The software shall notify ground personnel during or immediately after execution of an automated hazardous or safing process.
Unused or undocumented codes shall be incapable of producing a critical or catastrophic hazard.
All safety critical elements (requirements, design elements, code modules, and interfaces) shall be identified as "safety critical."
An application software set shall ensure proper configuration of inhibits, interlocks, and safing logic, and exception limits at initialization.

**Table J-1: Generic Software Safety Requirements listing**

### ***Coding Standards***

Coding Standards, a class of generic software requirements, are, in practice, "safe" subsets of programming languages. These are needed because most compilers can be unpredictable in how they work. For example, dynamic memory allocation is predictable. In applications where some portions of memory are safety critical, it is important to control which memory elements are assigned in a particular compilation process; the defaults chosen by the compiler might be unsafe. Some attempts have been made at developing coding safety standards (safe subsets).

### ***Timing, Sizing and Throughput Considerations***

System design should properly consider real-world parameters and constraints, including human operator and control system response times, and flow these down to software. Adequate margins of capacity should be provided for all these critical resources. This section provides guidance for developers in specifying software requirements to meet the safety objectives. Subsequent analysis of software for Timing, Throughput and Sizing considerations is discussed elsewhere in this appendix.

**Time to Criticality:** Safety critical systems sometimes have a characteristic "time to criticality", which is the time interval between a fault occurring and the system reaching an unsafe state. This interval represents a time window in which automatic or manual recovery and/or safing actions can be performed, either by software, hardware, or by a human operator. The design of safing/recovery actions should fully consider the real-world conditions and the corresponding time to criticality. Automatic safing can only be a valid hazard control if there is ample margin between worst case (long) response time and worst case (short) time to criticality.

**Automatic safing** is often required if the time to criticality is shorter than the realistic human operator response time, or if there is no human in the loop. This can be performed by either hardware or software or a combination depending on the best system design to achieve safing.

**Control system design** can define timing requirements. Based on the established body of classical and modern dynamic control theory, such as dynamic control system design, and multivariable design in the s-domain (Laplace transforms) for analog continuous processes. Systems engineers are responsible for overall control system design. Computerized control systems use sampled data (versus continuous data). Sampled analog processes should make

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

use of Z-transforms to develop difference equations to implement the control laws. This will also make most efficient use of real-time computing resources.

**Sampling rates** should be selected with consideration for noise levels and expected variations of control system and physical parameters. For measuring signals that are not critical, the sample rate should be at least twice the maximum expected signal frequency to avoid aliasing. For critical signals, and parameters used for closed loop control, it is generally accepted that the sampling rate must be much higher; at least a factor of ten above the system characteristic frequency is customary.

**Dynamic memory allocation:** ensure adequate resources are available to accommodate usage of dynamic memory allocation, without conflicts. Identify and protect critical memory blocks. Poor memory management has been a leading factor in several critical failures.

**Memory Checking:** Self-test of memory usage can be as part of BIT/self-test to give advance warning of imminent saturation of memory.

**Quantization:** Digitized systems should select word-lengths long enough to reduce the effects of quantization noise to ensure stability of the system. Selection of word-lengths and floating-point coefficients should be appropriate with regard to the parameters being processed in the context of the overall control system. Too short word-lengths can result in system instability and misleading readouts. Too long word-lengths result in excessively complex software and heavy demand on CPU resources, scheduling and timing conflicts etc.

**Computational Delay:** Computers take a finite time to read data and to calculate and output results, so some control parameters will always be out of date. Controls systems must accommodate this. Also, check timing clock reference datum, synchronization and accuracy (jitter). Analyze task scheduling (e.g., with Rate Monotonic Analysis (RMA)).

### J.4 Structured Design Phase Techniques

Structured design techniques greatly reduce the number of errors, especially requirements errors which are the most expensive to correct and may have the most impact on the overall safety of a system. These Structured Analysis and Design methods for software have been evolving over the years, each with its approach to modeling the needed world-view into software. The most recent analysis/design methods are Object Oriented Analysis & Design (OOA & OOD) and Formal Methods. To date, the most popular analysis methods have been Functional Decomposition, Data Flow (or Structured Analysis), and Information Modeling. OOA actually incorporates some of the techniques of all of these within its method, at lower levels, once the system is cast into objects with attributes and services. In the discussion of Structured Analysis, "analysis" is considered as a process for evaluating a problem space (a concept or proposed system) and rendering it into requirements that reflect the needs of the customer. Functional Decomposition has been, and still is, a popular method for representing a system. Functional Decomposition focuses on what functions, and sub-functions, the system needs to perform and the interfaces between those functions. The general complaints with this method are 1) the functional capability is what most often changes during the design life cycle and is thus very volatile, and 2) it is often hard to see the connection between the proposed system as a whole and the functions determined to create that system. A detailed discussion of Structured Analysis and Formal Methods appears in Appendix D of this handbook.

#### J.4.1 Architectural Design Analysis

The software architectural design process develops the high level design that will implement the software requirements. All software safety requirements developed above are incorporated into the high-level software design as part of this process. The design process includes identification of safety design features and methods (e.g., inhibits, traps, interlocks and assertions) that will be used throughout the software to

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

implement the software safety requirements. After allocation of the software safety requirements to the software design, Safety Critical Computer Software Components (SCCSCs) are identified. Bottom-up safety analysis is performed on the architectural design to identify potential hazards, to define and analyze SCCSCs and the early test plans are reviewed to verify incorporation of safety related testing. Analyses included in the Architectural Design Phase are:

- Update Criticality Analysis
- Conduct Hazard Risk Assessment
- Analyze Architectural Design
- Interdependence Analysis
- Independence Analysis
- Update Timing/Sizing Analysis

### **J.4.2 Update Criticality Analysis**

The software functions begin to be allocated to modules and components at this stage of development. Thus the criticality assigned during the requirements phase now needs to also be allocated to the appropriate modules and components.

Software for a system, while often subjected to a single development program, actually consists of a set of multi-purpose, multifunction entities. The software functions need to be subdivided into many modules and further broken down to components.

Some of these modules will be safety critical, and some will not. The criticality analysis provides the appropriate initial criticality designation for each software function. The safety activity relates identified hazards from the following analyses previously described to the Computer Software Components (CSCs) that may affect or control the hazards.

This analysis identifies all those software components that implement software safety requirements or components that interface with SCCSCs that can affect their output. The designation *Safety Critical Computer Software Component* (SCCSC) should be applied to any module, component, subroutine or other software entity identified by this analysis.

### **J.4.3 Conduct Risk Assessment**

The safety activity performs a system risk assessment to identify and prioritize those SCCSCs that warrant further analysis beyond the architectural design level. System risk assessment of hazards as described in the NHB 1700 series of documents, consists of ranking risks by severity level versus probability of occurrence. This high-severity/high probability risks are prioritized higher for analysis and corrective action than low-severity/low probability risks.

While Requirements Criticality and Update Criticality analysis simply assign a Yes or No to whether each component is safety critical, the Risk Assessment process takes this further. Each SCCSCs is prioritized for analysis and corrective action according to the five levels of Hazard Prioritization ranking given previously.

### **J.4.4 Analyze Architectural Design**

The safety activity analyzes the Architectural Design of those SCCSCs identified in the preceding paragraphs to ensure all safety requirements are specified correctly and completely in the Architectural Design. In addition, the safety activity determines where in the Architectural Design, and under what conditions

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

unacceptable hazards occur. This is done by postulating credible faults/failures and evaluating their effects on the system. Input/output timing, multiple event, out-of-sequence event, failure of event, wrong event, inappropriate magnitude, incorrect polarity, adverse environment, deadlocking, and hardware failure sensitivities are included in the analysis.

Methods used for FMEA (Failure Modes and Effects Analysis) can be used substituting software components for hardware components in each case. A widely used FMEA procedure is MIL-STD-1629, which is based on the following eight steps. Formal Inspections (described earlier), design reviews and animation/simulation augment this process.

1. Define the system to be analyzed
2. Construct functional block diagrams
3. Identify all potential item and interface failure modes
4. Evaluate each failure mode in terms of the worst potential consequences
5. Identify failure detection methods and compensating provisions
6. Identify corrective design or other actions to eliminate / control failure
7. Identify impacts of the corrective change
8. Document the analysis and summarize the problems which could not be corrected

### ***Design Reviews***

Design data is reviewed to ensure it properly reflects applicable software safety requirements. Design changes are generated where necessary. Applicability matrices, compliance matrices, and compliance checklists can be used to assist in completing this task. Output products are engineering change requests, hazard reports (to capture design decisions affecting hazard controls and verification) and action items.

### ***Animation/Simulation***

Simulators, prototypes (or other dynamic representations of the required functionality as specified by the design), and test cases to exercise crucial functions can be developed. Run the tests and observe the system response. Requirements can be modified as appropriate. Documented test results can confirm expected behavior or reveal unexpected behavior. The status of critical verifications is captured by hazard reports.

## **J.4.5 Interface Analysis**

### **Interdependence Analysis**

Examine the software to determine the interdependence among CSCs, modules, tables, variables, etc. Elements of software that directly or indirectly influences SCCSCs are also identified as SCCSCs, and as such should be analyzed for their undesired effects. For example, shared memory blocks used by two or more SCCSCs. The inputs and outputs of each SCCSC are inspected and traced to their origin and destination.

### ***Independence Analysis***

The safety activity evaluates available design documentation to determine the independence/dependence and interdependence of SCCSCs to both safety-critical and non-safety-critical CSCs. Those CSCs that are found to affect the output SCCSCs are designated as SCCSCs. Areas where FCR (Fault Containment Region) integrity is compromised are identified. The methodology is to map the safety critical functions to the software modules and map the software modules to the hardware hosts and FCRs. Each input and output of each SCCSC should be inspected. Resources are definition of safety critical functions needing to independent

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

design descriptions, and data diagrams. Design changes to achieve valid FCRs and corrections to SCCSC designations may be necessary

### **J.5 Detailed Design Analysis**

During the Detailed Design phase, more detailed software artifacts are available, permitting rigorous analyses to be performed. Detailed Design Analyses can make use of artifacts such as detailed design specifications, emulators and Pseudo-Code Program Description Language products (PDL). Preliminary code produced by code generators within case tools should be evaluated. Many techniques to be used on the final code can be "dry run" on these design products. In fact, it is recommended that all analyses planned on the final code should undergo their first iteration on the code-like products of the detailed design. This will catch many errors before they reach the final code where they are more expensive to correct. The following techniques can be used during this design phase. Description of each technique follows the list.

- J.5.1 Design Logic Analysis
- J.5.2 Design Data Analysis
- J.5.3 Design Interface Analysis
- J.5.4 Design Constraint Analysis
- J.5.6 Software Fault Tree Analysis (SFTA)
- J.5.7 Petri-Nets
- J.5.8 Dynamic Flowgraph Analysis
- J.5.9 Measurement of Complexity
- J.5.10 Safe Subsets of Programming languages
- J.5.11 Formal Methods and Safety-Critical Considerations
- J.5.12 Requirements State Machines

#### **J.5.1 Design Logic Analysis (DLA)**

Design Logic Analysis (DLA) evaluates the equations, algorithms, and control logic of the software design. Logic analysis examines the safety-critical areas of a software component. A technique for identifying safety-critical areas is to examine each function performed by the software component. If it responds to, or has the potential to violate one of the safety requirements, it should be considered critical and undergo logic analysis. A technique for performing logic analysis is to analyze design descriptions and logic flows and note discrepancies.

The ultimate, fully rigorous DLA uses the application of Formal Methods (FM). Where FM is inappropriate, because of its high cost versus software of low cost or low criticality, simpler DLA can be used. Less formal DLA involves a human inspector reviewing a relatively small quantity of critical software artifacts (e.g. PDL, prototype code), and manually tracing the logic. Safety critical logic to be inspected can include failure detection/diagnosis; redundancy management, variable alarm limits, and command inhibit logical preconditions.

Commercial automatic software source analyzers can be used to augment this activity, but should not be relied upon absolutely since they may suffer from deficiencies and errors, a common concern of COTS tools and COTS in general.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

### **J.5.2 Design Data Analysis**

Design data analysis evaluates the description and intended use of each data item in the software design. Data analysis ensures that the structure and intended use of data will not violate a safety requirement. A technique used in performing design data analysis is to compare description-to-use of each data item in the design logic.

Interrupts and their effect on data must receive special attention in safety-critical areas. Analysis should verify that interrupts and interrupt handling routines do not alter critical data items used by other routines.

The integrity of each data item should be evaluated with respect to its environment and host. Shared memory, and dynamic memory allocation can affect data integrity. Data items should also be protected from being overwritten by unauthorized applications. Considerations of EMI affecting memory should be reviewed in conjunction with system safety.

### **J.5.3 Design Interface Analysis**

Design interface analysis verifies the proper design of a software component's interfaces with other components of the system. This analysis will verify that the software component's interfaces have been properly designed. Design interface analysis verifies that control and data linkages between interfacing components have been properly designed. Interface requirements specifications are the sources against which the interfaces are evaluated.

Interface characteristics to be addressed should include data encoding, error checking and synchronization. The analysis should consider the validity and effectiveness of checksums and CRCs. The sophistication of error checking implemented should be appropriate for the predicted bit error rate of the interface. An overall system error rate should be defined, and budgeted to each interface. Examples of interface problems:

- Sender sends eight-bit word with bit 7 as parity, but recipient believes bit 0 is parity.
- Sender transmits updates at 10 Hz, but receiver only updates at 1 Hz.
- Sender encodes word with leading bit start, but receiver decodes with trailing bit start.
- Interface deadlock prevents data transfer (e.g., Receiver ignores or cannot recognize "ready to send").
- User reads data from wrong address.
- Sender addresses data to wrong address.

In a language such as C, or C++ where data typing is not strict, sender may use different data types than reviewer expects. (Where there is strong data typing, the compilers will catch this).

### **J.5.4 Design Constraint Analysis**

Design constraint analysis evaluates restrictions imposed by requirements, the real world and environmental limitations, as well as by the design solution. The design materials should describe all known or anticipated restrictions on a software component. These restrictions may include those listed below. Design constraint analysis evaluates the ability of the software to operate within these constraints.

- Update timing and sizing constraints
- Equations and algorithms limitations.
- Input and output data limitations (e.g., Range, resolution, accuracy).
- Design solution limitations.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

- Sensor/actuator accuracy and calibration.
- Noise, EMI.
- Digital word-length (quantization/roundoff noise/errors).
- Actuator power / energy capability (motors, heaters, pumps, mechanisms, rockets, valves, etc.)
- Capability of energy storage devices (e.g., Batteries, propellant supplies).
- Human factors, human capabilities and limitations.
- Physical time constraints and response times.
- Off nominal environments (fail safe response).
- Friction, inertia, backlash in mechanical systems.
- Validity of models and control laws versus actual system behavior.
- Accommodations for changes of system behavior over time: wear-in, hardware wear-out, end of life performance versus beginning of life performance degraded system behavior and performance.

### **J.5.5 Rate Monotonic Analysis**

Rate Monotonic Analysis is a useful analysis technique for software. It ensures that time critical activities will be properly verified.

### **J.5.6 Software Fault Tree Analysis (SFTA)**

It is possible for a system to meet requirements for a correct state and to also be unsafe. It is unlikely that developers will be able to identify, prior to the fielding of the system, all correct but unsafe states which could occur within a complex system. In systems where the cost of failure is high, special techniques or tools such as Fault Tree Analysis (FTA) need to be used to ensure safe operation. FTA can provide insight into identifying unsafe states when developing safety critical systems. Fault trees have advantages over standard verification procedures. Fault trees provide the focus needed to give priority to catastrophic events, and they assist in determining environmental conditions under which a correct or incorrect state becomes unsafe.

### **J.5.7 Petri-Nets**

Petri-nets are a graphical technique that can be used to model and analyze safety-critical systems for such properties as reachability, recoverability, deadlock, and fault tolerance. Petri-nets allow the identification of the relationships between system components such as hardware and software, and human interaction or effects on both hardware and software. Real-time Petri-net techniques can also allow analysts to build dynamic models that incorporate timing information. In so doing, the sequencing and scheduling of system actions can be monitored and checked for states that could lead to unsafe conditions.

The Petri-net modeling tool is different from most other analysis methods in that it clearly demonstrates the dynamic progression of state transitions. Petri-nets can also be translated into mathematical logic expressions that can be analyzed by automated tools. Information can be extracted and reformed into analysis assisting graphs and tables that are relatively easy to understand (e.g., reachability graphs, inverse Petri-net graphs, critical state graphs). Some of the potential advantages of Petri-nets over other safety analysis techniques include the following:

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

- Petri-nets can be used to derive timing requirements in real-time systems.
- Petri-nets allow the user to describe the system using graphical notation, and thus they free the analyst from the mathematical rigor required for complex systems.
- They can be applied through all phases of system development. Early use of Petri-nets can detect potential problems resulting in changes at the early stages of development where such changes are relatively easy and less costly than at later stages.
- They can be applied for the determination of worst case analysis and the potential risks of timing failures.
- A system approach is possible with Petri-nets since hardware, software and human behavior can be modeled using the same language.
- Petri-nets can be used at various levels of abstraction.
- Petri-nets provide a modeling language which can be used for both formal analysis and simulation.

Adding time and probabilities to each Petri-net allows incorporation of timing and probabilistic information into the analysis. The model may be used to analyze the system for other features besides safety.

Unfortunately, Petri-nets require a large amount of detailed analysis to build even relatively small systems, thus making them very expensive. In order to reduce expenses, a few alternative Petri-net modeling techniques have been proposed, each tailored to perform a specific type of safety analysis. For example, time Petri-net (TPN), take account for time dependency factor of real-time systems; inverse Petri-net, specifically needed to perform safety analysis, uses the previously discussed backward modeling approach to avoid modeling all of the possible reachable status; and critical state inverse Petri-nets, which further refine inverse Petri-net analysis by only modeling reachable states at predefined criticality levels.

Petri-net analysis can be performed at any phase of the software development cycle; though, it is highly recommended for reasons of expense and complexity that the process be started at the beginning of the development cycle and expanded for each of the succeeding phases. Petri-net, inverse Petri-net and critical state Petri-nets are all relatively new technologies, are costly to implement, and absolutely require technical expertise on the part of the analyst. Petri net analysis is a complex subject, and is treated in more detail in Appendix C of this handbook.

### **J.5.8 Dynamic Flowgraph Analysis**

Dynamic Flowgraph Analysis is a new technique, not yet widely used and still in the experimental phase of evaluation. It does appear to offer some promise, and in many respects combines the benefits of conventional J.5.6 Software Fault Tree Analysis (SFTA) and J.5.7 Petri-Nets .

The Dynamic Flowgraph Methodology (DFM) is an integrated, methodical approach to modeling and analyzing the behavior of software-driven embedded systems for the purpose of dependability assessment and verification. The methodology has two fundamental goals: 1) to identify how events can occur in a system; and 2) identify an appropriate testing strategy based on an analysis of system functional behavior. To achieve these goals, the methodology employs a modeling framework in which models expressing the logic of the system being analyzed are developed in terms of contributing relationships between physical variables and temporal characteristics of the execution of software modules.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

Models are analyzed to determine how a certain state (desirable or undesirable) can be reached. This is done by developing timed fault trees which take the form of logical combinations of static trees relating the system parameters at different points in time. The resulting information concerning the hardware and software states that can lead to certain events of interest can then be used to increase confidence in the system, eliminate unsafe execution paths, and identify testing criteria for safety critical software functions.

### **J.5.9 Measurement of Complexity**

Software's complexity should be evaluated in order to determine if the level of complexity may contribute to areas of concern for workability, understandability, reliability and maintainability. Highly complex data and command structures are difficult, if not impossible, to test thoroughly and can lead to errors in logic either in the initial build or in subsequent updates. Not all paths can usually be thought out or tested for and this leaves the potential for the software to perform in an unexpected manner. Highly complex data and command structures may be necessary, however, there usually are techniques for avoiding too high a level of programming interweaving.

Linguistic, structural, and combined metrics exist for measuring the complexity of software and while discussed below briefly.

Use complexity estimation techniques, such as McCabe or Halstead. If an automated tool is available, the software design and/or code can be run through the tool. If there is no automated tool available, examine the critical areas of the detailed design and any preliminary code for areas of deep nesting, large numbers of parameters to be passed, intense and numerous communication paths, etc. (Refer to references cited above.) Resources are the detailed design, high level language description, source code, and automated complexity measurement tool(s).

Output products are complexity metrics, predicted error estimates, and areas of high complexity identified for further analysis or consideration for simplification.

Several automated tools are available on the market which provides these metrics. The level and type of complexity can indicate areas where further analysis, or testing, may be warranted. Beware, however, these metrics should be used with caution as they may indicate that a structure, such as a CASE statement, is highly complex while in reality that complexity leads to a simpler, more straight forward method of programming and maintenance, thus decreasing the risk of errors.

Linguistic measurements measure some property of the text without regard for the contents (e.g., lines of code, number of statements, number and type of operators, total number and type of tokens, etc). Halstead's Metrics is a well known measure of several of these arguments.

Structural metrics focuses on control-flow and data-flow within the software and can usually be mapped into a graphics representation. Structural relationships such as the number of links and/or calls, number of nodes, nesting depth, etc. are examined to get a measure of complexity. McCabe's Cyclomatic Complexity metric is the most well known and used metric for this type of complexity evaluation.

### **J.5.10 Safe Subsets of Programming languages**

Safety specific coding standards are developed which identify requirements for annotation of safety-critical code and limitation on use of certain language features which can reduce software safety. The purpose of this section is to provide a technical overview of safety-critical coding practices for developers and safety engineers, primarily those involving restricting the use of certain programming language constructs.

The use of software to control safety-critical processes is placing software development environments (i.e. languages, compilers, utilities, etc.) under increased scrutiny. When computer languages are taught, students

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

are seldom warned of the limitations and insecurities that the environment possesses. An insecurity is a feature of a programming language whose implementation makes it impossible or extremely difficult to detect some violation of the language rules, by mechanical analysis of a program's text. The computer science profession has only recently focused on the issues of the inherent reliability of programming environments for safety-critical applications.

This section will provide an introduction on the criteria for determining which languages are well suited for safety-critical applications. In addition, an overview of a safe subset of the ADA language will be discussed with the rationale for rejecting language constructs. Reading knowledge of Pascal, ADA, C or another modern high level block structured language is required to understand the concepts that are being discussed.

There are two primary reasons for restricting a language definition to a subset: 1) some features are defined in an ambiguous manner and 2) some features are excessively complex. A language is considered suitable for use in a safety-critical application if it has a precise definition (complete functionality as well), is logically coherent, and has a manageable size and complexity. The issue of excessive complexity makes it virtually impossible to verify certain language features. Overall, the issues of logical soundness and complexity will be the key toward understanding why a language is restricted to a subset for safety-critical applications.

An overview of the insecurities in the ADA language standard is included in this entry. Only those issues that are due to the ambiguity of the standard will be surveyed. The problems that arise because a specific implementation (e.g., a compiler) is incorrect can be tracked by asking the compiler vendor for a historical list of known bugs and defect repair times. This information should give a user a basis with which to compare the quality of product and service of different vendors.

### ***Insecurities Common to All Languages***

All programming languages have insecurities either in their definition or their implementation. The evolutionary trend of computer languages shows a trend of newer languages trying to correct the shortfalls of older generation languages (even though some individuals complain about additional restrictions).

Probably the most common misuse in practically all-programming languages is that of uninitialized variables. This mistake is very hard to catch because unit testing will not flag it unless explicitly designed to do so. The typical manifestation of this error is when a program that has been working successfully is run under different environmental conditions and the results are not as expected.

Calls to de-allocate memory should be examined to make sure that not only is the pointer released but that the memory used by the structure is released.

The order of evaluation of operands when side effects from function calls modify the operands is generally dismissed as poor programming practice but in reality is an issue that is poorly defined (no standard of any type has been defined) and arbitrarily resolved by implementers of language compilers.

### ***Method of Assessment***

The technique used to compare programming languages will not deal with differences among manufacturers of the same language. Compiler vendor implementations, by and large, do not differ significantly from the intent of the standard, however standards are not unambiguous and they are interpreted conveniently for marketing purposes. One should be aware that implementations will not adhere 100% to the standard because of the extremely large number of states a compiler can produce. The focus of this study then is to review the definition of a few languages for certain characteristics that will provide for the user a shell against inadvertent misuse. When evaluating a language, the following questions should be asked of the language as a minimum:

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

- Can it be shown that the program cannot jump to an arbitrary location?
- Are there language features that prevent an arbitrary memory location from being overwritten?
- Are the semantics of the language defined sufficiently for static code analysis to be feasible?
- Is there a rigorous model of both integer and floating point arithmetic within the standard?
- Are there procedures for checking that the operational program obeys the model of the arithmetic when running on the target processor?
- Are the means of typing strong enough to prevent misuse of variables?
- Are there facilities in the language to guard against running out of memory at runtime?
- Does the language provide facilities for separate compilation of modules with type checking across module boundaries?
- Is the language well understood so designers and programmers can write safety-critical software?
- Is there a subset of the language which has the properties of a safe language as evidenced by the answers to the other questions?

### J.5.11 Formal Methods and Safety-Critical Considerations

In the production of safety-critical systems or systems that require high assurance, Formal Methods\* provide a methodology that gives the highest degree of assurance for a trustworthy software system. Assurance cannot be measured in a quantitative, objective manner for software systems that require reliability figures that are of the order of one failure in  $10^9$  hours of operation. An additional difficulty that software reliability cannot address to date, in a statistically significant manner, is the difference between catastrophic failures and other classes of failures.

Formal Methods have been used with success on both military and commercial systems that were considered safety-critical applications. The benefits from the application of the methodology accrue to both safety and non-safety areas. Formal Methods do not guarantee a precise quantifiable level of reliability; at present they are only acknowledged as producing systems that provide a high level of assurance.

On a qualitative level the following list identifies different levels of application of assurance methods in software development. They are ranked by the perceived level of assurance achieved with the lowest numbered approaches representing the highest level of assurance. Each of the approaches to software development is briefly explained by focusing on that part of the development that distinguishes it from the other methods.

**Formal development down to object code** requires that formal mathematical proofs be carried out on the executable code.

**Formal development down to source code** requires that the formal specification of the system undergo proofs of properties of the system.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

**Rigorous development down to source code** is when requirements are written in a formal specification language and emulators of the requirements are written. The emulators serve the purpose of a prototype to test the code for correctness of functional behavior.

**Structured development to requirements analysis then rigorous development down to source code** performs all of the steps from the previous paragraph. The source code undergoes a verification process that resembles a proof but falls short of one.

**Structured development down to source code** is the application of the structured analysis/structured design method. It consists of a conceptual diagram that graphically illustrates functions, data structures, inputs, outputs, and mass storage and their interrelationships. Code is written based on the information in the diagram.

**Ad hoc** techniques encompass all of the non-structured and informal techniques (i.e. hacking, code a little then test a little).

### J.5.12 Requirements State Machines

Requirements State Machines (RSM) are sometimes called Finite State Machines (FSM). An RSM is a model or depiction of a system or subsystem, showing states and the transitions between the states. Its goal is to identify and describe ALL possible states and their transitions. RSM analysis can be used on its own, or as a part of a structured design environment, e.g., object oriented design or formal methods.

Whether or not formal methods are used to develop a system, a high level RSM can be used to provide a view into the architecture of an implementation without being engulfed by all the accompanying detail. Semantic analysis criteria can be applied to this representation and to lower level models to verify the behavior of the RSM and determine that its behavior is acceptable. The analysis criteria will be listed in a section below and in subsequent sections because they are applicable at practically every stage of the development life cycle.

#### **Characteristics of State Machines**

A formal description of state machines can be obtained from texts on Automata Theory. This description will only touch on those properties that are necessary for a basic understanding of the notation and limitations. State machines use graph theory notation for their representation. A state machine consists of states and transitions. The state represents the condition of the machine and the transition represent changes between states. The transitions are directed (direction is indicated by an arrow), that is, they represent a directional flow from one state to another. A trigger or input that is labeled on the transition induces the transition from one state to another. Generally the state machine produces an output.

The state machine models should be built to abstract different levels of hierarchy. The models are partitioned in a manner that is based on considerations of size and logical cohesiveness. An uppermost level model should contain at most 15 to 20 states; this limit is based on the practical consideration of comprehensibility. In turn, each of the states from the original diagram can be exploded in a fashion similar to the bubbles in a data flow diagram/control flow diagram (DFD/CFD) (from a structured analysis/structured design methodology) to the level of detail required. An RSM model of one of the lower levels contains a significant amount of detail about the system.

The states in each diagram are numbered and classified as one of the following attributes: Passive, Startup, Safe, Unsafe, Shutdown, Stranded and Hazard. For the state machine to represent a viable system, the diagram must obey certain properties that will be explained later in this work.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

The *passive* state represents an inert system, that is, nothing is being produced. However, in the passive state, input sensors are considered to be operational. Every diagram of a system contains at least one passive state. A passive state may transition to an unsafe state.

The *startup* state represents the initialization of the system. Before any output is produced, the system must have transitioned into the startup state where all internal variables are set to known values. A startup state must be proven to be safe before continuing work on the remaining states. If the initialization fails, a timeout may be specified and a state transition to an unsafe or passive state may be defined.

### ***Properties of Safe State Machines***

There are certain properties that the state machine representation should exhibit in order to provide some degree of assurance that the design obeys certain safety rules. The criteria for the safety assertions are based on logical considerations and take into account input/output variables, states, trigger predicates, output predicates, trigger to output relationship and transitions.

### ***Input/Output Variables***

All information from the sensors should be used somewhere in the RSM. If not, either an input from a sensor is not required or, more importantly, an omission has been made from the software requirements specification. For outputs it can be stated that, if there is a legal value for an output that is never produced, then a requirement for software behavior has been omitted.

### ***State Attributes***

The state attributes of the RSM are to be labeled according to the scheme in Chapter 10.

## **J.6 Code Analysis**

Code analysis verifies that the coded program correctly implements the verified design and does not violate safety requirements. In addition, at this phase of the development effort, many unknown questions can be answered for the first time. For example, the number of lines of code, memory resources and CPU loads can be seen and measured, where previously they were only predicted, often with a low confidence level. Sometimes significant redesign is required based on the parameters of the actual code. Code permits real measurements of size, complexity and resource usage. Code Analyses include:

- Code Logic Analysis
- Software Fault Tree Analysis (SFTA)
- Petri-Nets
- Code Data Analysis
- Code Interface Analysis
- Measurement of Complexity
- Code Constraint Analysis
- Safe Subsets of Programming languages
- Formal Methods and Safety-Critical Considerations
- Requirements State Machines

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

Some of these code analysis techniques mirror those used in detailed design analysis. However, the results of the analysis techniques might be significantly different than during earlier development phases, because the final code may differ substantially from what was expected or predicted.

Each of these analyses, contained in this section, should be undergoing their second iteration, since they should have all been applied previously to the code-like products (PDL) of the detailed design.

There are some commercial tools available which perform one or more of these analyses in a single package. These tools can be evaluated for their validity in performing these tasks, such as logic analyzers, and path analyzers. However, unvalidated COTS tools, in themselves, cannot generally be considered valid methods for formal safety analysis. COTS tools are often useful to reveal previously unknown defects.

Note that the definitive formal code analysis is that performed on the final version of the code. A great deal of the code analysis is done on earlier versions of code, but a final check on the final version is essential. For safety purposes it is desirable that the final version have no “instrumentation” (i.e., extra code added), in order to see where erroneous jumps go. One may need to run the code on an instruction set emulator that can monitor the code from the outside, without adding the instrumentation.

### **J.6.1 Code Logic Analysis**

Code logic analysis evaluates the sequence of operations represented by the coded program. Code logic analysis will detect logic errors in the coded software. Performing logic reconstruction, equation reconstruction and memory decoding conduct this analysis.

Logic reconstruction entails the preparation of flow charts from the code and comparing them to the design material descriptions and flow charts.

Equation reconstruction is accomplished by comparing the equations in the code to the ones provided with the design materials.

Memory decoding identifies critical instruction sequences even when they may be disguised as data. The analyst should determine whether each instruction is valid and if the conditions under which it can be executed are valid. Memory decoding should be done on the final un-instrumented code. Employment of Fault Trees and Petri Nets has been discussed in the previous section of this appendix.

### **J.6.2 Code Data Analysis**

Code data analysis concentrates on data structure and usage in the coded software. Data analysis focuses on how data items are defined and organized. Ensuring that these data items are defined and used properly is the objective of code data analysis. This is accomplished by comparing the usage and value of all data items in the code with the descriptions provided in the design materials.

Of particular concern to safety is ensuring the integrity of safety critical data against being inadvertently altered or overwritten. For example, check to see if interrupt processing is interfering with safety critical data. Also, check the “typing” of safety critical declared variables.

### **J.6.3 Code Interface Analysis**

Code interface analysis verifies the compatibility of internal and external interfaces of a software component. A software component is composed of a number of code segments working together to perform required tasks. These code segments must communicate with each other, with hardware, other software components, and human operators to accomplish their tasks. Check that parameters are properly passed across interfaces.

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

Each of these interfaces is a source of potential problems. Code interface analysis is intended to verify that the interfaces have been implemented properly. Hardware and human operator interfaces should be made part of the "Design Constraint Analysis" discussed below.

### **J.6.4 Measurement of Complexity**

As a goal, software complexity should be minimized to reduce likelihood of errors. Complex software also is more likely to be unstable, or suffer from unpredictable behavior. Modularity is a useful technique to reduce complexity. Complexity can be measured via McCabe's metrics and similar techniques.

### **J.6.5 Update Design Constraint Analysis**

The criteria for design constraint analysis applied to the detailed design can be updated using the final code. At the code phase, real testing can be performed to characterize the actual software behavior and performance in addition to analysis.

The physical limitations of the processing hardware platform should be addressed. Timing, sizing and throughput analyses should also be repeated as part of this process to ensure that computing resources and memory available are adequate for safety critical functions and processes.

Underflows/overflows in certain languages (e.g., ADA) give rise to "exceptions" or error messages generated by the software. These conditions should be eliminated by design if possible; if they cannot be precluded, then error handling routines in the application must provide appropriate responses, such as retry, restart, etc.

### **J.6.6 Code Inspection Checklists (including coding standards)**

Coding standards are based on style guides and safe subsets of programming languages. Checklists should be developed during formal inspections to facilitate inspection of the code to demonstrate conformance to the coding standards.

### ***Fagan Formal Inspections (FIs)***

FIs are one of the best methodologies available to evaluate the quality of code modules and program sets. Many projects do not schedule any formal project-level software reviews during coding. When software is ready to be passed on to subsystems for integration, projects may elect to conduct an Integration Readiness Review when audit or inspection reports and problem reports may be evaluated. Other than these reports, the only formal documentation usually produced are the source code listings from configuration management.

### **J.6.7 Formal Methods**

Generation of code is the ultimate output of Formal Methods. In a "pure" Formal Methods system, analysis of code is not required. In practice, however, attempts are often made to "apply" Formal Methods to existing code after the fact. In this case the analysis techniques of the previous sections (0 through 0) may be used to "extract" the logic of the code, and then compare the logic to the formal requirements expressions from the Formal Methods.

### **J.6.8 Unused Code Analysis**

A common real world coding error is generation of code that is logically excluded from execution; that is, preconditions for the execution of this code will never be satisfied. Such code is undesirable for three reasons; a) it is potentially symptomatic of a major error in implementing the software design; b) it introduces unnecessary complexity and occupies memory or mass storage which is often a limited resource; and c) the unused code might contain routines which would be hazardous if they were inadvertently executed (e.g., by a hardware failure or by a Single Event Upset. SEU is a state transition caused by a high-speed subatomic particle passing through a semiconductor - common in nuclear or space environments).

## FAA System Safety Handbook, Appendix J: Software Safety December 30, 2000

There is no particular technique for identifying unused code; however, unused code is often identified during the course of performing other types of code analysis. Unused code can be found during unit testing with COTS coverage analyzer tools.

Care should be taken during logical code analyses to ensure that every part of the code is eventually exercised at some time during all possible operating modes of the system.

### **J.7 Test Phase**

Two sets of analyses should be performed during the testing phase: analyses before the fact to ensure validity of tests, and analyses of the test results. Tests are devised to verify all safety requirements where testing has been selected as appropriate verification method. This is not considered here as analysis. Analysis before the fact should, as a minimum, consider test coverage for safety critical Must-Work-Functions.

#### **J.7.1 Test Coverage**

For small pieces of code it is sometimes possible to achieve 100% test coverage (i.e., to exercise every possible state and path of the code). However, it is often not possible to achieve 100 % test coverage due to the enormous number of permutations of states in a computer program execution, versus the time it would take to exercise all those possible states. Also there is often a large indeterminate number of environmental variables, too many to completely simulate.

Some analysis is advisable to assess the optimum test coverage as part of the test planning process. There is a body of theory that attempts to calculate the probability that a system with a certain failure probability will pass a given number of tests.

Techniques known as “white box” testing can be performed, usually at the modular level. Statistical methods such as Monte Carlo simulations can be useful in planning "worst case" credible scenarios to be tested.

#### **J.7.2 Test Results Analysis**

Test results are analyzed to verify that all safety requirements have been satisfied. The analysis also verifies that all identified hazards have been eliminated or controlled to an acceptable level of risk. The results of the test safety analysis are provided to the ongoing system safety analysis activity. All test discrepancies of safety critical software should be evaluated and corrected in an appropriate manner.

#### **J.7.3 Independent Verification and Validation**

For high value systems with high-risk software, an IV&V organization is usually involved to oversee the software development. The IV&V organization should fully participate in the validation of test analysis.