Chapter 4:
Safety Assessments Before Investment Decision

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).

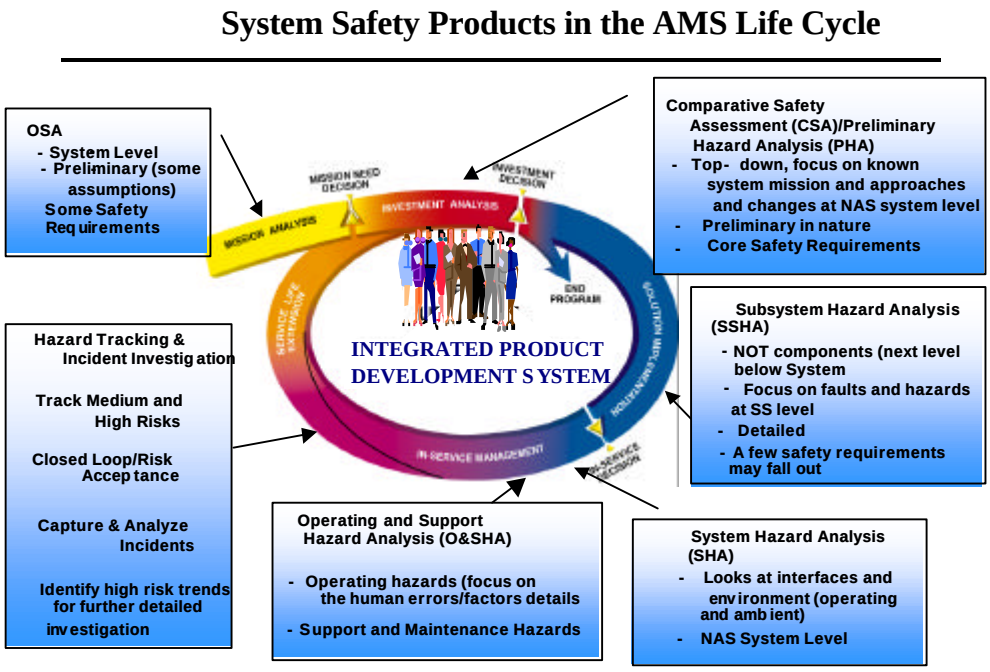

Figure 4-1: Safety Products in AMS Life Cycle

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

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

OPERATIONS ANALYSIS	*Purpose*: To understand the flow of events. *Method*: List events in sequence. May use time checks.
PRELIMINARY HAZARD ANALYSIS (PHA)	*Purpose*: 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. *Method*: 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.
"WHAT IF" TOOL	*Purpose*: To capture the input of operational personnel in a brainstorming-like environment. *Method*: Choose an area (not the entire operation), get a group and generate as many "what ifs" as possible.
SCENARIO PROCESS TOOL	*Purpose*: To use imagination and visualizations to capture unusual hazards. *Method*: Using the operations analysis as a guide, visualize the flow of events.
LOGIC DIAGRAM	*Purpose*: To add detail and rigor to the process through the use of graphic trees. *Method*: Three types of diagrams- positive, negative, and risk event.

CHANGE ANALYSIS	*Purpose*: To detect the hazard implications of both planned and unplanned change. *Method*: Compare the current situation to a previous situation.
CAUSE & EFFECT TOOL -- CHANGE ANALYSIS	*Purpose*: To add depth and increased structure to the Hazard ID process through the use of graphic trees. *Method*: 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. *Purpose*: To detect the hazard implications of both planned and unplanned change. *Method*: Compare the current situation to a previous situation.
CAUSE & EFFECT TOOL	*Purpose*: To add depth and increased structure to the Hazard ID process through the use of graphic trees. *Method*: 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.

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

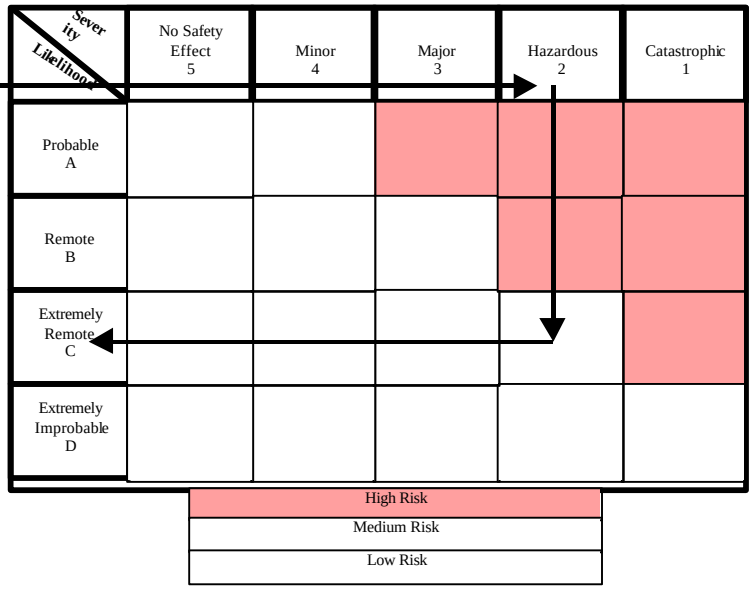

Figure 4-2: Target Level of Safety Determination

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

NAS System function	NAS System hazard	NAS System Controls
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

NAS System Function	NAS System Hazard	NAS System Controls	NAS System Requirements
Provide air to ground communicat-ions 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.