Chapter 8:
Safety Analysis: Hazard Analysis Tasks

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.

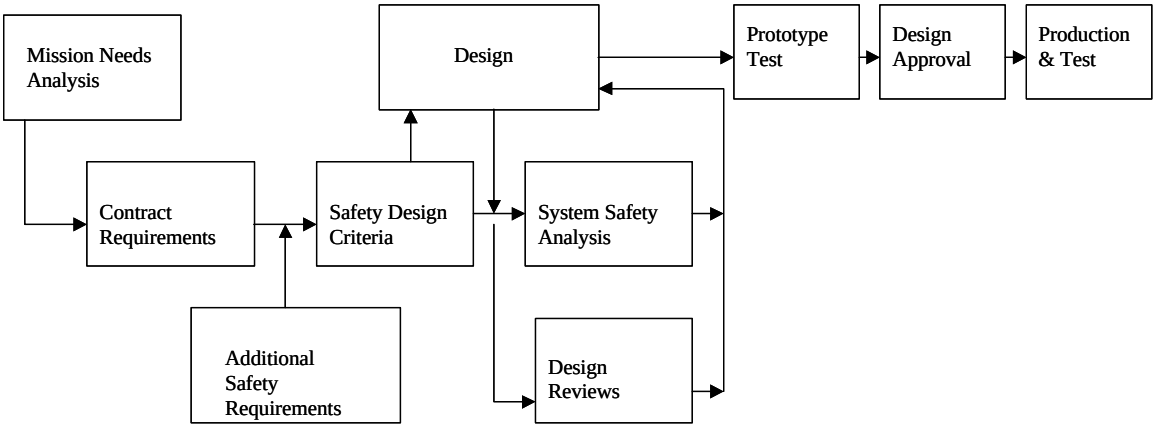

Figure 8-1: A Proactive System Safety Plan

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 (NAILS) 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:

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

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.

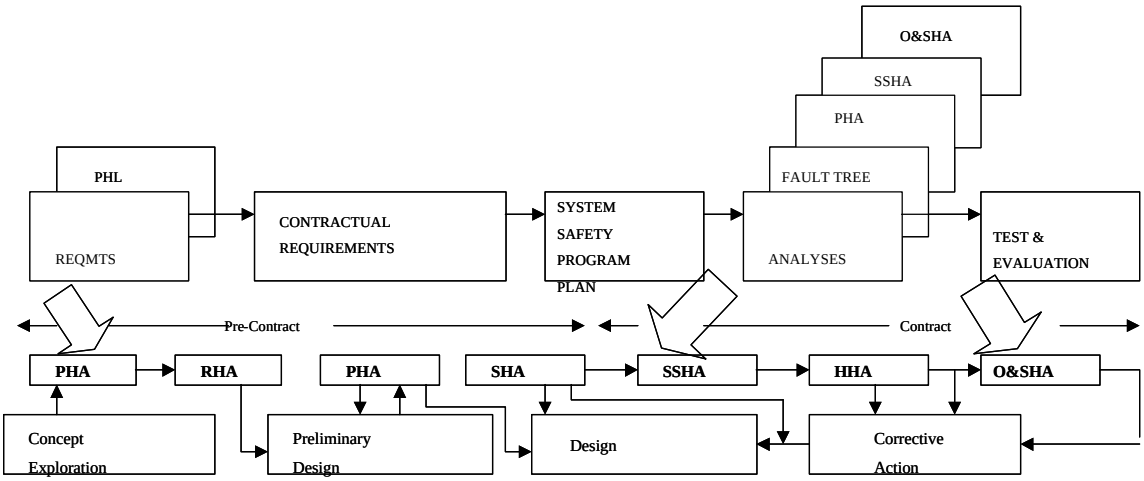

Figure 8-2: Hazard Analysis Relationships

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.

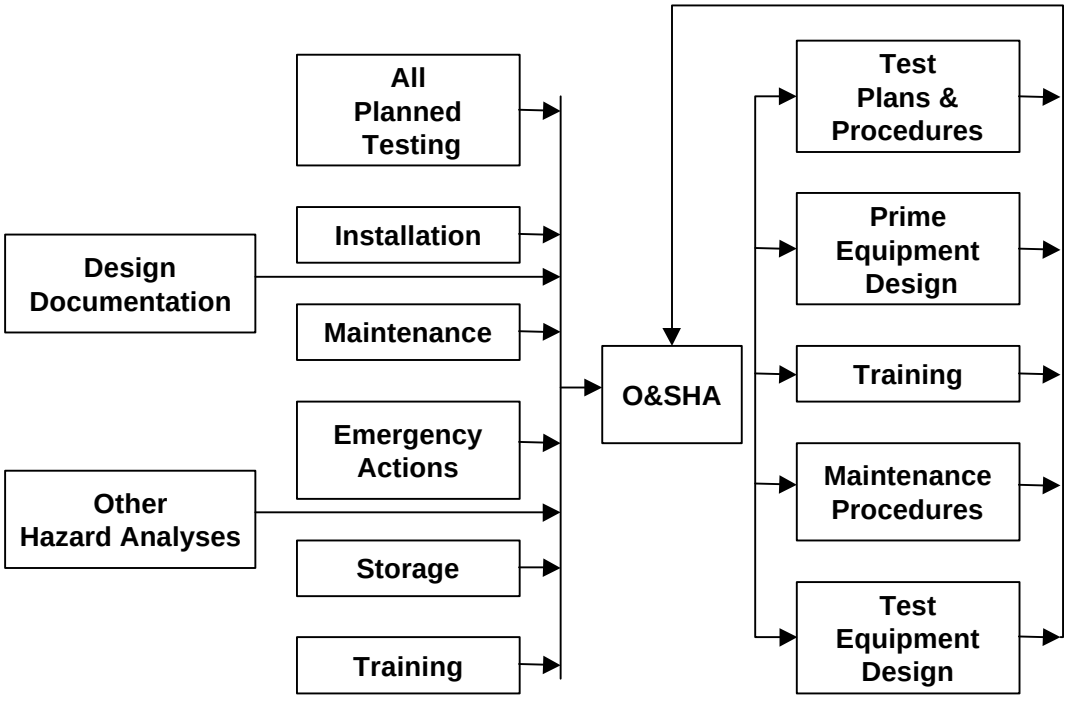

Figure 8-3: Operating & Support Hazard Analysis (O&SHA) Elements

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

- 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.

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:

- 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.

HAZARD: Failure to extend landing gear prior to landing an aircraft.

Resolution Method	Example
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 are 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.

The 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.

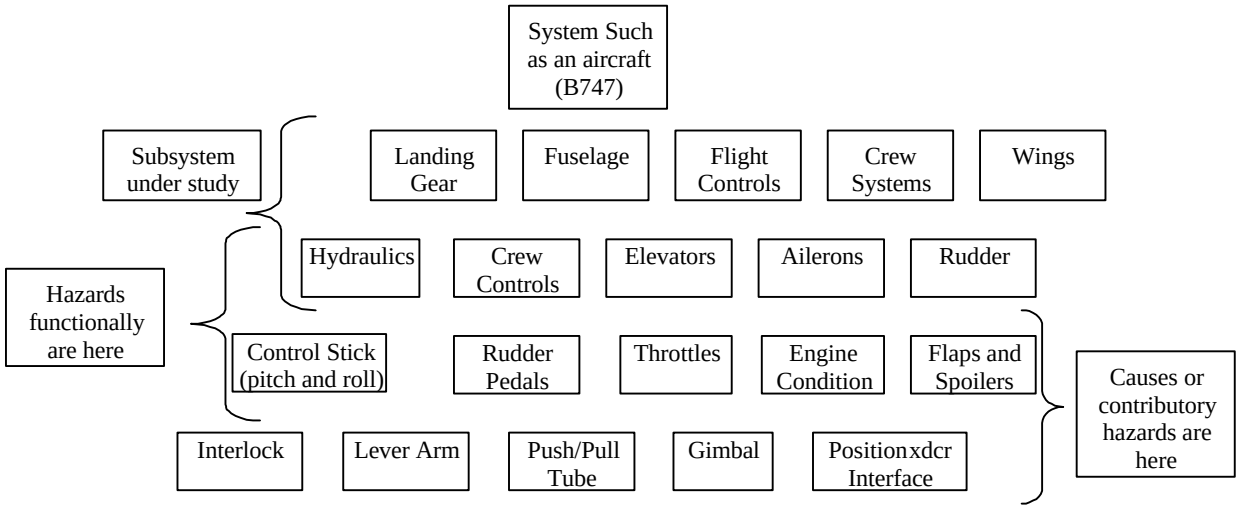

Figure 8-5 Level of Analysis

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., "0" 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.

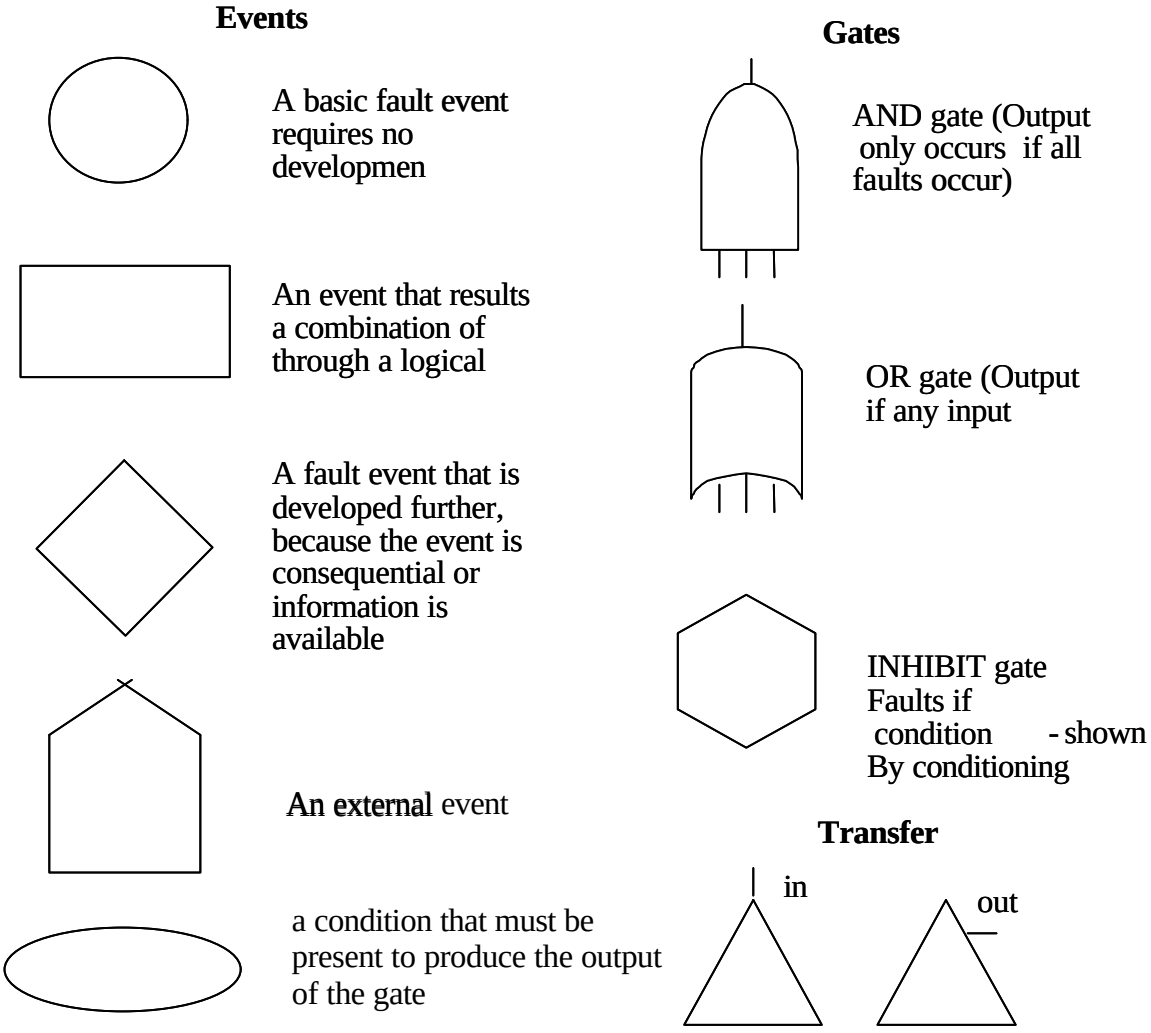

Figure 8-6 Fault Tree Symbols

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).

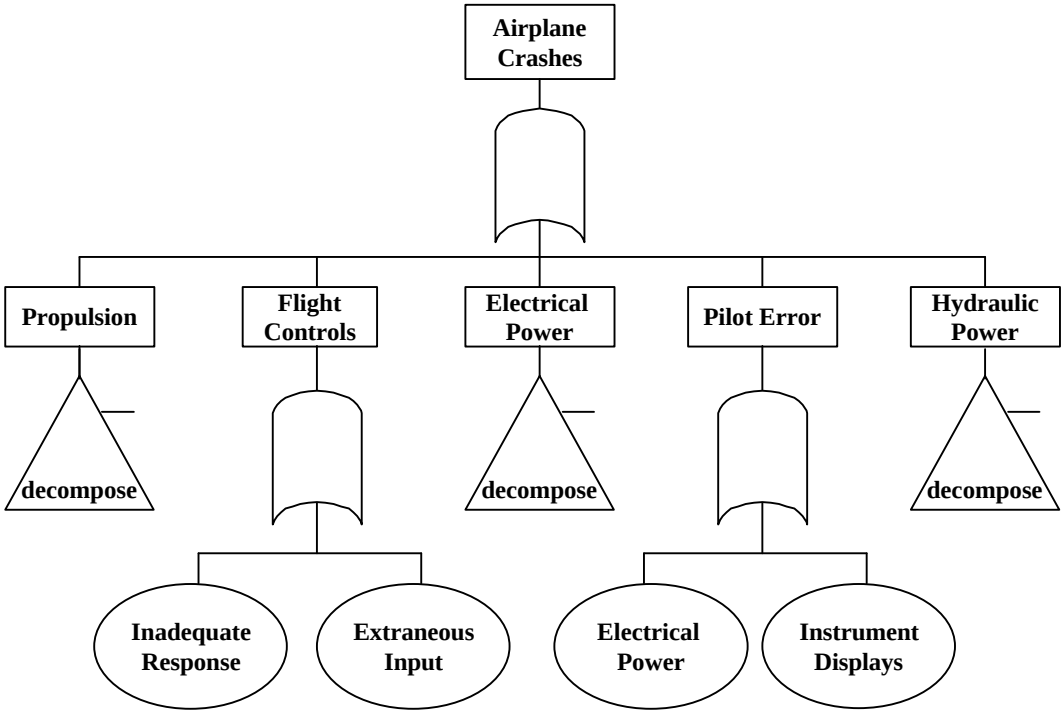

Figure 8-6: Sample Top Level Fault Tree

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.

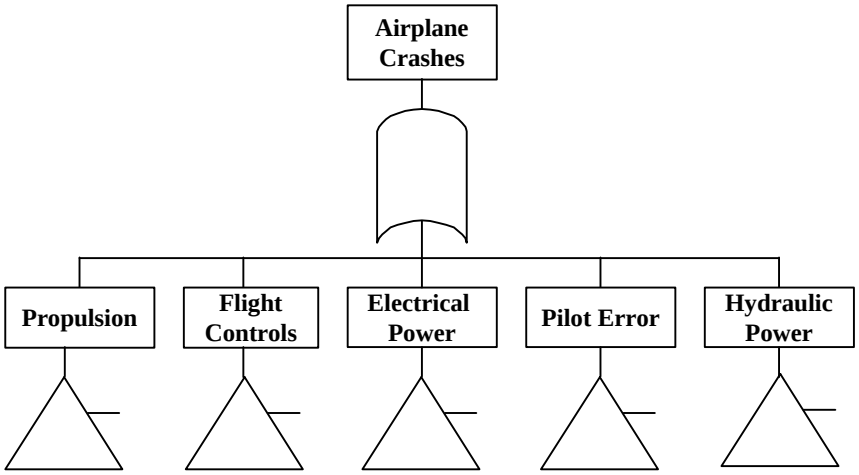

Figure 8-7: More Comprehensive Fault Tree

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 6×10^5 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.

- 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.