CHAPTER 14

System Safety Principles and Methods

DONALD W. SWALLOM, ROBERT M. LINDBERG and TONYA L. SMITH-JACKSON

14.1 INTRODUCTION

System safety is perhaps the most familiar of all the human systems integration (HSI) domains to the general population as the discipline that helps in the design of equipment to avoid accidents. System safety is the first (and sometimes the only) HSI domain to be involved whenever major accidents occur in defense, medicine, transportation, manufacturing, and energy. No one wishes people to die in accidents, but it is especially upsetting when the accidents are avoidable. System safety specializes in preventing accidents through helping design systems that are safe. System safety is both a philosophy and a practice that focuses on designing in ways to prevent accidents.

The philosophy behind system safety is based on the medical model of primary prevention (referred to as *loss prevention* in the safety arena), which means that the main emphasis is on the complete removal of hazards from the environment. System safety uses secondary prevention, or *loss control*, as a last resort if primary prevention is not feasible. In loss control, it is understood that the hazard cannot be removed from the work environment, but the system (including the human component) can be protected in such a way that exposure to hazards is less likely or the consequences of exposure are less severe. Loss control is a prevention approach in which it is relatively difficult to determine how much protection to apply.

System safety faces a continual problem in demonstrating how to increase system safety without decreasing system performance to unacceptable limits or making the system unaffordable. For example, heavier aircraft may provide greater crashworthiness than lighter ones, but greater weight can also decrease system performance and increase system cost in development and operation. Automation may remove the hazard from the environment, but complex and sometimes expensive technologies must become part of the system. Although not always the case, sometimes the cost of safety outweighs the accident prevention advantages.

Handbook of Human Systems Integration, Edited by Harold R. Booher.
ISBN 0-471-02053-2

The objective of the system safety discipline is to achieve a minimal level of risk within the constraints of operational effectiveness, time, and cost. System safety practitioners apply system safety principles and methods to accomplish such activities as hazard identification, hazard elimination, and risk control in the systems engineering process.

System safety and safety engineering extend as far back as 2100 BC, the estimated date of the first safety engineering manual, the Code of Hammurabi (Deitz et al., 2002; Kohn et al., 1996). This ancient Babylonian code focused on ship design, construction, loss control, and even specified the behavior of ship personnel, particularly when goods or lives were lost at sea. In the year 1743, the European-born doctor, Ulrich Ellenborg, identified lung diseases among builders that were caused by asbestos and identified other toxic substances that undermined the health of mine workers [Kohn et al., 1996; Occupational Safety and Health Administration (OSHA) online document]. The National Safety Congress convened in 1912 to organize efforts to protect the safety of the public [Kohn et al., 1996; National Safety Council (NSC), 2002]. This group later became the National Safety Council. The U.S. military beginning in World War II has also contributed to the development of the system safety discipline and, particularly, has developed specific methods and practices relevant to risk assessment.

There are a number of other historical contributors to system safety as well as safety engineering. Major attention was directed toward the protection of workers with the ratification of the Occupational Safety and Health Act in 1970 (OSHAct). OSHAct requires employers to adhere to standards of health and safety and provides regulatory authority to OSHA. More importantly, the passage of OSHAct and the establishment of OSHA forced employers to organize efforts within industry to protect the health and safety of workers, and, consequently, companies began to understand the importance of system approaches. For example, OSHA not only provides specific regulations as they apply to such system components as scaffolding, confined spaces, and materials handling, but it also addresses training practices, accident investigation, and process safety, all of which require careful integration with existing subsystems to be effective and compliant.

Today, system safety concepts are practiced within a wide range of industries, including: military, transportation, mining, manufacturing, nuclear, automotive, chemical processes, construction, and health care. Both federal and international standards have been developed that require system safety programs and methods to meet the objectives of comprehensive loss prevention and loss control.

The system safety engineer's primary job is to determine *how* the system can fail and cause death, injury, occupational illness, damage to or loss of equipment or property, loss of data, or damage to the environment. Knowing a system's potential for harm leads to the system design question: What can be done to eliminate or reduce that potential for harm?

The purpose of this chapter is to provide an overview of the analytical aspects of the system safety domain by discussing exemplary models, methods, and processes used by the system safety engineer to help identify and mitigate the potential harm from accidents. Before covering the details of these analytical approaches, we first define a number of terms familiar to system safety personnel. They include:

- Key safety definitions
- System safety engineering and management
- Safety groups and plans

14.1.1 Key Safety Definitions

There are several definitions that are useful to our discussion of system safety. Described in Table 14.1, they include:

- Safety
- Accidents
- Mishaps
- System
- System safety
- Hazards
- Risk
- Mishap risk
- Hazard severity
- Hazard probability
- Exposure

TABLE 14.1 Safety Definitions

Safety is condition in which there is low probability that harm will occur. Safety shares that definition with "security." However, security tends to mean freedom from harm from hostile person or group. Safety is more concerned with forms of harm from nonpersonal sources. The harm one might experience includes death, injury, occupational illness, damage to or loss of equipment or property, loss of data, or damage to the environment.
An *accident* is undesirable event or a series of undesirable events that result in harm.
A *mishap* is an accident. Mishap is terminology frequently used in DoD but is seldom used in commercial system safety practice.
A *system* is collection of things that work together. Military Standard 882, which delineates the Department of Defense practice of system safety, defines a system to be "an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective" (DoD, 2000).
System safety is "the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle" (DoD, 2000).
Hazards are the conditions or events in a system that can result in harm.
Risk is likelihood and severity of a loss. Conditions that require risk management include those that create significant risk of "death, injury, acute/chronic illness, disability, and/or reduced job performance of personnel who produce, test, operate, maintain, support, or dispose of the system" (DoD, 2001).
Mishap risk is expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (DoD, 2000). In life-cycle terms, mishap risk is the expected cost of mishaps stemming from a particular hazard over the life of the system.
Hazard probability is likelihood that adverse consequences from a specific hazard will occur.
Hazard severity is assessment of consequences of hazard. It is amount of harm that could potentially occur in one mishap due to specific hazard. It is degree of injury, occupational illness, property damage, equipment damage, or lost data in that mishap.
Exposure is time interval over which hazard occurs. Increasing exposure interval changes the probability of occurrence—as exposure interval increases, so does probability of occurrence.

14.1.2 System Safety Engineering and Management

System safety engineering deals with the tools of the trade, the principles and methodology of analyzing the hazards of system components, subsystems, and interfaces. One popular definition provided by Malasky (1982) states that system safety is:

> an optimum degree of safety, established within the constraints of operational effectiveness, time, and cost, and other application interfaces to safety, that is achievable throughout all phases of the system life cycle. (p. 17)

System safety should also be viewed as a systematic process to identify, eliminate, and control hazards. Figure 14.1 illustrates the overall process and specifically identifies opportunity windows that support system modification.

System safety management (or risk management) deals with how the decisions are made based on the analysis done by the system safety engineers to eliminate or reduce the associated *mishap risk*. Other aspects of system safety management include defining and allocating the resources required for the safety effort and providing system safety interfaces with other system development efforts. Generally, system safety engineering and management provide decision makers with information to ensure mishap risk is evaluated in a reasoned and balanced way.

Department of Defense (DoD) regulations require the program manager to comply with environment, safety, and occupational health (ESOH) regulatory requirements, which in general is to prevent or avoid ESOH hazards, where possible, and manage those hazards where they cannot be avoided[1] (DoD, 2001).

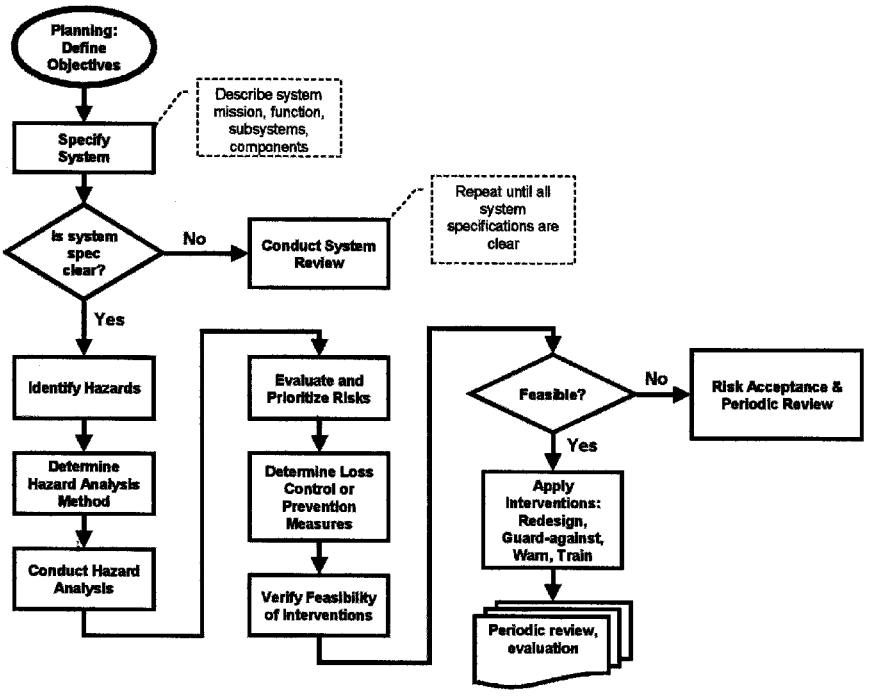


Figure 14.1 Conceptual model of the system safety process.

OSHA addresses system safety management in a number of regulations. For example, 29 CFR 1910.333 specifically addresses robot system safety. The standard outlines work management practices for continuous attended operation, maintenance, and repair. OSHA's lock-out/tag-out standard (LOTO; 29 CFR 1910.147) defines an "authorized employee." Employers cannot make designations of "authorized" employees for LOTO that conflict with the definition given in the OSHA standard. Other government agencies such as the Federal Aviation Administration (FAA)[2] and the National Aeronautics and Space Administration (NASA) also require compliance with safety directives.[3]

14.1.3 Safety Groups and Plans

A *system safety group* (SSG), *system safety working group* (SSWG), or a *system safety integrated product team* (SSIPT) is a formally chartered group of persons representing organizations involved in a system's design, use, and management. Organizations that specifically practice total safety management (TSM), may integrate their safety groups into a quality circle (Goetsch, 2002). These teams are organized to assist the program manager in achieving acceptable mishap risk. The system safety plan spells out how each group functions, the processes that will be used to determine acceptance of mishap risks, and how to obtain additional resources to eliminate or reduce risk. The name of the group depends on the level of responsibility. For example, an SSG may function at one level of management while the SSWG may work at a lower level in the organization.

A *system safety program plan* (SSPP) is based on the principles of safety and any government or company systems safety policies. The SSPP lays out how the organization will reduce mishap risk to an acceptable level and still achieve the program objectives. The plan includes organizational resources, responsibilities and relationships, methods of accomplishment, milestones, depth of effort, and integration with other program activities and related systems. The plan also spells out how the system safety team functions. For DoD programs, a *system safety management plan* (SSMP) delineates how the government will manage system safety. For contractors, the SSPP outlines contractual responsibilities for system safety through the use of company methods and processes.

14.1.4 Chapter Outline

The chapter covers three major topics as reflected in the following sections:

- Risk assessment model
- System safety methods and techniques
- System safety process

14.2 RISK ASSESSMENT MODEL

Almost all accident event sequences can be traced back to a process failure between the system, environment, and human interfaces. In a majority of accident investigations, human error (operator, maintainer) is determined to be the root cause of the system mishap. However, even if there is an equipment failure, the question still remains whether someone failed to design, test, or produce the equipment correctly. This is critical for HSI

because, carried to the extreme, almost all accident event sequences can be traced back to a human failure. Since people are not perfect, the system safety analysis process starts with the question, "What would a 'reasonable' worker know and do in the place of that person who failed?" Could the failure have been foreseen and a better decision made to prevent or minimize the mishap? But even reasonable people do not always foresee the results of their decisions. System safety, in that sense, is an effort to systematically provide knowledge to reasonable people so they can make the best decisions in the design of systems.

Although root causes of accidents are often attributed to human error somewhere within the system, it must be understood that the integration of system safety and HSI supports a slightly different view of "human error," as is found in other disciplines. In the case of the integrated system safety and HSI perspective, human error occurs because of design problems within the entire sociotechnical system, which includes such factors as training, management practices, machine design, human information processing, and even psychosocial stimuli such as stressors or culture. In addition, when investigations occur in environments that are applying a system safety/HSI approach, it is understood that accident causation can be explained by multiple factors that interact to produce hazardous situations.

14.2.1 Range of Outcomes

The first principle of the system safety model states that there is a range of possible outcomes from a hazard. One reason for the range of outcomes is that the hazard could manifest itself as a mishap at different times during the operation of the system. For example, if an aircraft or helicopter engine quits running while the vehicle is on the ground, the only damage is to the component and/or other engine parts. If the engine quits during cruise flight, engine debris may cause damage to the aircraft. If the engine fails during a critical phase of takeoff, the potential result is destruction of the aircraft and loss of life. A production line may introduce hazards anywhere from raw materials entry to export and waste disposal. Another reason for the range of outcomes is the interaction of more than one hazard in the mishap. If an electrical component fails and begins to arc, it may just burn up that component. If it arcs in conjunction with a fuel leak, it could result in a serious fire and loss of the whole system. Examples of the range of outcomes that could happen in a mishap are:

1. *Human Injury* Ranges from minor injury resulting in no days missed from work to death.
2. *Equipment Damage* Ranges from minor component damage requiring little repair to total system destruction.
3. *Environmental Damage* An example is a chemical spill that could range from a minor hazardous material spill requiring no reporting to a major environmental catastrophe.
4. *Health-Related Mishaps* These can range from short-term health impairment with 100 percent recovery to a lifetime health disability.
5. *Business-Related Mishap* These can range from loss of one computer file to the loss of an entire data storage site.

14.2.2 Risk Analysis

Risk analysis makes use of both quantitative and qualitative methods to assess risk. As with all forms of risk, one quantitative measure is dollars. Risk is the cost of mishaps stemming from a particular hazard over the life of the system. This is a very important concept and one that is often misunderstood. If the system is operated long enough with no changes, the risk will indeed be realized as an actual cost at some future point in time. Risk of a hazard has two components, *hazard severity* and *hazard probability.* Sometimes a third component, *exposure*, is identified (see Table 14.1 for definitions).

Since there is a range of possible consequences of a hazard, the likelihood of the worst consequence may be far less than those of lesser consequence. Figure 14.2 graphs this relationship in a $20 million system. *As the severity of the hazard increases, the hazard probability decreases*. However, it should be noted that in real-life situations this paradigm is not always true.

Often the *risk curve* for a particular hazard follows the relationship where the severity (S) times the probability (P) is a constant ($S \times P = C$). From the Figure 14.2 one could ask: what is the probability of this hazard resulting in a loss of exactly $10,000? That probability might be 0.00001 occurrences during a life cycle of the system. So the risk is $10,000 per occurrence times 0.00001 occurrences per life cycle of the system equals $1. This is done for every $1 increase in mishap severity all the way up to a $20 million mishap. When the risks are added for each level of severity mishap, the total risk from the hazard is identified. Mathematically, this is the area under the risk curve. If this system operates for the whole life cycle, the likelihood of having a mishap that is exactly $10,000 is unlikely since the probability is 0.00001 or 1 in 10,000 life cycles. However, the total cost of the mishap should come close to the total calculated risk for the hazard. If 10 of the systems operate, the cost of the hazard per system will be closer to the calculated risk. If there are a thousand systems, it will be even closer. If there are an infinite number of systems, the cost per system will be the calculated risk.

There are several graphical representations used to illustrate risk levels and their relationship to probability and severity within different contexts. These same illustrations are used to aid in decision making regarding risk categorization. Figures 14.3 to 14.6 are examples. Figure 14.3 shows different levels of risk. Hazard 1 is high risk; hazards 2 and 3 are medium risk; and hazard 4 is low risk. Figure 14.4 depicts risk curves on logarithmic

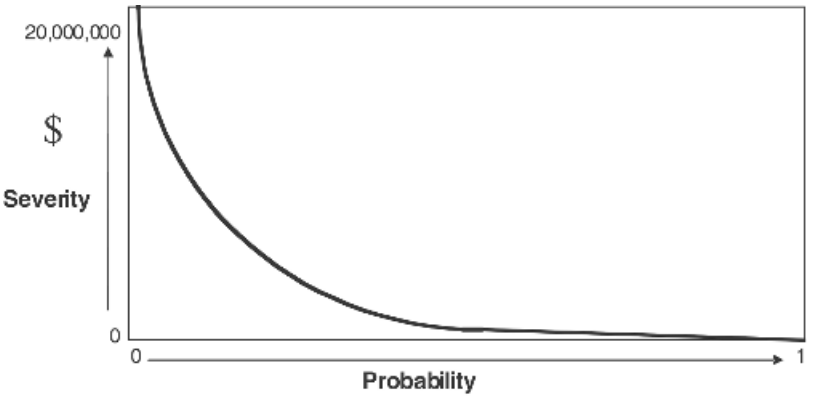


Figure 14.2 Relationship of severity and probability.

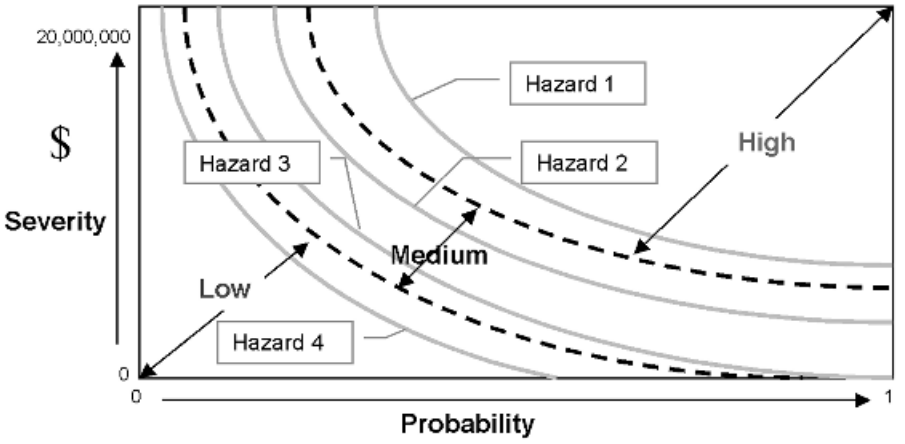


Figure 14.3 Risk curves on linear scales. [Adapted with permission from Clemens and Simmons (1998, pp. II-3 to II-6).]

scales. Note the curves now are closer to being straight lines. Figure 14.5 shows the hazard assessment matrix developed by DoD in 1993 as part of the MIL-STD-882. The hazard assessment matrix is a hybrid that is both quantitative and qualitative. The approach is to use qualitative descriptors of the severity and likelihood of a hazard to assign a hazard risk index (HRI). The HRI is a quantitative descriptor of risk. The matrix can be simplified to something like that shown in Figure 14.6.

The above discussion illustrates the theory behind the risk matrix, but in practice a system safety engineer will take the worst credible consequence of a hazard to assign a risk assessment code from the matrix instead of dealing with the entire risk curve. The "worst credible consequence" is the most severe outcome of a hazard that can reasonably be expected to occur during the life cycle of a system. From Figure 14.6, the risk assessment code assigned could be 1A through 4F. The risk of the worst credible consequence then

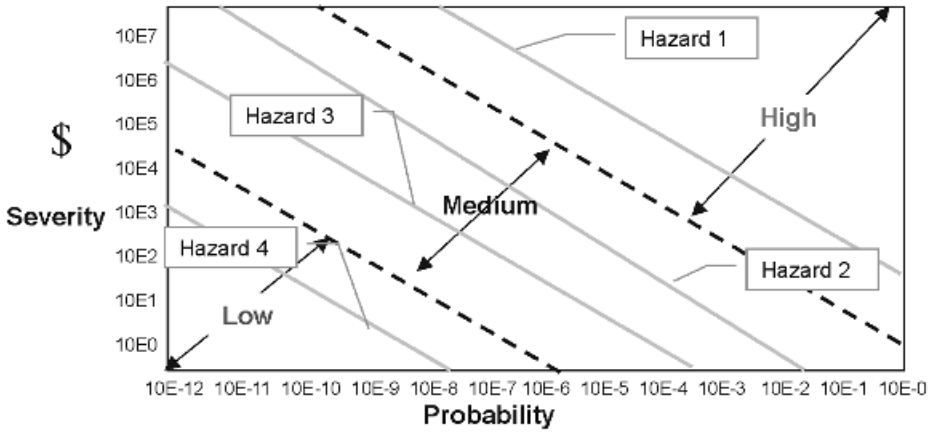
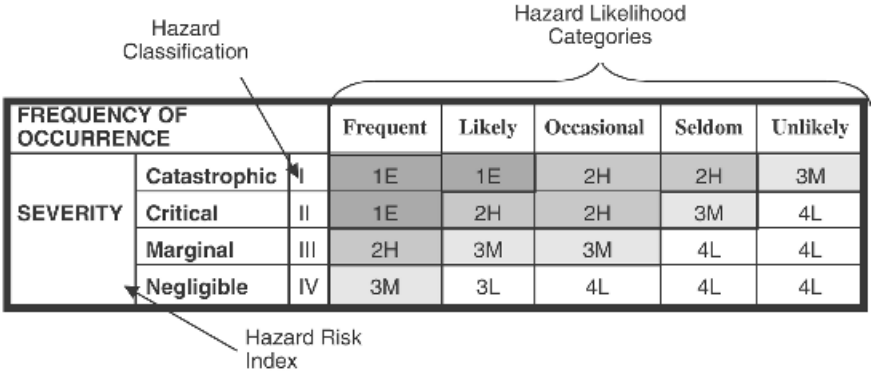


Figure 14.4 Risk curves on log scales. [Adapted with permission from Clemens and Simmons (1998, pp. II-3 to II-6).]



FREQUENCY OF OCCURRENCE			Frequent	Likely	Occasional	Seldom	Unlikely
SEVERITY	Catastrophic	I	1E	1E	2H	2H	3M
	Critical	II	1E	2H	2H	3M	4L
	Marginal	III	2H	3M	3M	4L	4L
	Negligible	IV	3M	3L	4L	4L	4L

Abbreviations: Extremely high (E), High (H), Moderate (M), and Low (L)
Hazard Risk Index Labels : 1 = Unacceptable, 2 = Undesirable with management waiver required, 3 = Acceptable with management review, 4 = Acceptable without review.

Figure 14.5 Hazard assessment matrix with hazard risk indices (HRI) embedded. **Abbreviations:** Extremely high (E), high (H), moderate (M), and low (L). Hazard risk index labels: 1 = unacceptable, 2 = undesirable with management waiver required, 3 = acceptable with management review, 4 = acceptable without review. [Adapted from Kohn et al. (1996), p. 205; DoD (1993); Roland and Moriarty (1990), pp. 200, 204.]

represents the whole risk curve. In this manner, a system safety engineer can assign a risk code early in the program before there is a mature design or any substantial analysis. This early estimate of the risk helps allocate resources for further analysis and risk reduction.

Table 14.2 describes each probability level, ranging from "frequent" to "improbable," for a DoD aircraft program. These probability levels are also reflected in Figure 14.6.

Table 14.3 describes each severity level, ranging from 4, "negligible" to 1, "catastrophic" for a DoD aircraft program. These severity levels are also reflected in Figure 14.6.

Using these tables, a safety engineer can assign a risk assessment code that can be used to prioritize risk or hazard mitigation actions and determine if the risk is acceptable. The

	Hazard Probability					
Severity	Impossible F	Improbable E	Remote D	Occasional C	Probable B	Frequent A
Catastrophic 1						
Critical 2						
Marginal 3						
Negligible 4						

Figure 14.6 Simplified risk matrix. [Adapted with permission from Clemens and Simmons (1998, pp. II-3 to II-6).]

TABLE 14.2 Hazard Probability Levels

Level	Description	Specific Individual Aircraft	Fleet	Probability [Occurrences per Flight Hour (p)]
A	Frequent	Likely to occur often in life of aircraft	Continuously experienced	$p > 10^{-1}$
B	Probable	Will occur several times in life of aircraft	Will occur frequently	$10^{-1} \geq p > 10^{-3}$
C	Occasional	Likely to occur some time in life of aircraft	Will occur several times	$10^{-3} \geq p > 10^{-5}$
D	Remote	Unlikely but possible to occur in life of aircraft	Unlikely but can reasonably be expected to occur	$10^{-5} \geq p > 10^{-7}$
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible	$10^{-7} \geq p$
F	Impossible	Cannot occur	Cannot occur	$10^{-9} \geq p$

Source: Adapted from *Air Force System Safety Handbook* (2000), p. 22.

assigned risk assessment code is likely to change as the program progresses. It may be that an analysis of the design shows that the initial risk assessment was too optimistic and a higher risk code should be assigned. If all goes well in the system safety effort and the redesign of the system, the hazard will be assigned a lower risk code that will be more acceptable to the risk acceptance authority.

Total system risk is the sum of the known and unknown risk of all system hazards. *Residual risk* is the risk that remains after all risk reduction efforts have been brought to

TABLE 14.3 Hazard Severity Levels

Category	Description
1	Catastrophic: Death or permanent total disability; system loss or mishap damage greater then or equal to $1 million.
2	Critical: Severe injury or severe occupational illness (permanent partial disability); mishap damage greater than $200,000 but less then $1 million.
3	Marginal: Minor injury or minor occupational illness (no permanent effect); mishap damage greater than or equal to 20,000 but less than $200,000.
4	Negligible: Less than minor injury or occupational illness (no lost workdays); mishap damage less than $20,000.

Source: Adapted from *Air Force System Safety Handbook* (2000, p. 22).

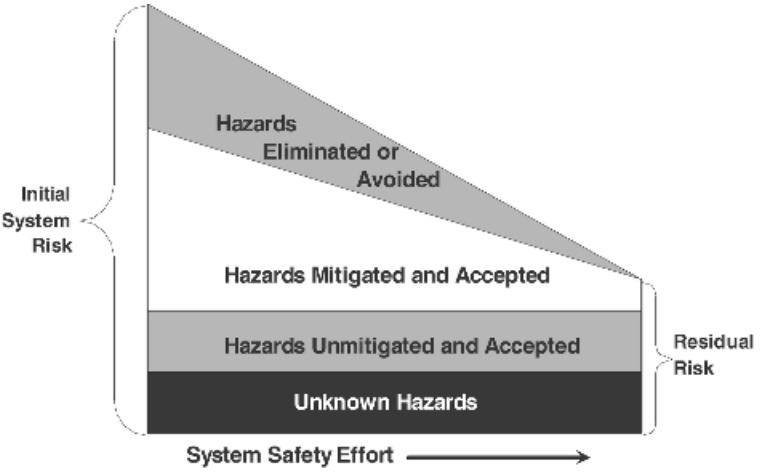


Figure 14.7 Residual risk.

bear on a hazard. If a hazard is not eliminated, then some mishap risk still "resides" in the system. Figure 14.7 illustrates this concept. The initial system risk is the risk before the system safety effort began. The four components of risk are: hazards that are eliminated or avoided, hazards that are mitigated and then accepted, hazards unmitigated and accepted, and hazards that are never discovered.

14.3 SYSTEM SAFETY METHODS AND TECHNIQUES

There are a large number of methods and techniques available to help the system safety analyst. To aid analysis efforts, the System Safety Society (http://www.nm-esh.org/sss/ssshdbk.html) documents 101 safety analysis methods and techniques (Table 14.4) in the *System Safety Analysis Handbook* (Stephans and Talso, 1997). From this extensive tool kit, an experienced system safety engineer can select appropriate methods or techniques to identify and assess the risk of system hazards.

Although Table 14.4 identifies a large number of tools, they quickly reduce to a manageable number in actual systems application. Many of the methods and techniques are variations of one another or are methods specifically adapted to a particular type of system (nuclear, aircraft, facility, etc.) or type of hazard (human factors, explosive, electrical, fire, confined space, etc.). Some methods have been found to be less reliable than others and, consequently, are used less often. Further, many of these techniques are common to other HSI domains and are covered in the chapters for those domains (see, e.g., Chapter 13 for human factors analyses and Chapter 15 for health hazards assessment).

One caveat when conducting risk analyses is to first select the group that will conduct the analysis. No single individual should conduct a risk analysis because the quality of an analysis can be undermined by biases or oversights. Thus, a group analysis increases the chance that a comprehensive analysis is conducted.

TABLE 14.4 Summary of System Safety Techniques and Methodologies

No.	Technique	Purpose	Application
1	Accident analysis	Evaluate accident scenarios	In conjunction with PHA or SSHA
2	Action error analysis	Analyze interactions between machines and humans	Human interface with automated or other processes
3	Barrier analysis	Analyze unwanted flow of hazardous energy	Systems analysis, occupational safety reviews, and accident analysis
4	Bent pin analysis (BPA)	Represent failures within cable connections	Electrical cable systems
5	Cable failure matrix (CFMA)	Represent failures within cable assemblies	Electrical cable assemblies; use with BPA
6	Cause–consequence analysis	Evaluate accident consequences	Similar to FTA or ETA
7	Change analysis	Examine potential effects of modification	All systems
8	Checklist analysis	Identify hazards using list of known deficiencies and accident situations	Evaluate compliance to standards
9	Chemical process Quantitative risk analysis (CPQRA)	Quantitative risk assessment within chemical process industry	Processes of all types
10	Common cause analysis	Identify common causes of accident sequences	All systems; extensively used in nuclear power industry
11	Comparison to criteria (CTC)	Structured format to guide compliance review	Any system designed to standards
12	Confined space safety	Systematic evaluation of spaces with limited egress	Implements OSHA requirements; supports PHA or SSHA
13	Contingency analysis	Prepare for emergencies by identifying potential accidents and measures to mitigate	All systems wherein advance preparation is needed
14	Control rating code (CRC) method	Produce safety effectiveness ratings	Systems, facilities, and equipment
15	Critical incident technique	Use historical information to identify and ameliorate hazards	Any system with human operators
16	Criticality analysis	Rank potential failure modes	Used with FMEA
17	Critical path analysis	Network modeling and analysis	Control and monitor complex safety management efforts
18	Cryogenic systems safety analysis	Specifically examine cryogenic systems	Use with PHA or SSHA

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
19	Damage mode and effects analysis	Provide early criteria for damage or vulnerability assessment	Uses results of FMEA
20	Deactivation safety analysis	Identify significant safety and health concerns integral to facility deactivation process	Facilities clean up and deactivation
21	Digraph utilization within system safety	Model failure effect scenarios	Model complex systems similar to FTA
22	Electromagnetic compatibility (EMC) analysis and testing	Prevent EM interference and protect form EMR	Any system requiring electrical circuit protection
23	Energy analysis	Evaluate safety through "energetics"	Any system that contains, stores, or uses energy in any form
24	Energy trace and barrier analysis (ETBA) for hazard discovery and analysis	Safety analysis through meticulous tracing of energy flow	Any system; often used with MORT and STEP
25	Energy trace checklist	Evaluate safety through "energetics" and lists of known energy hazards	Used with PHA or SSHA; defines system hazards
26	Environmental risk analysis	Assess risk of environmental noncompliance	Any system that produces potentially toxic or hazardous materials
27	Event and causal factor charting	Reconstruct accident event and determine root cause(s)	Any accident or mishap
28	Event tree analysis (ETA)	Organize, characterize, and quantify potential accidents	All systems wherein unwanted events can be anticipated
29	Explosive safety analysis	Evaluate potential effects of hazards involving handling, storing, and working explosives	Any situation involving gram to ton quantities of explosives
30	External events analysis	Focus attention on events outside the system under examination	In conjunction with PSAR or FSAR
31	Facilities system safety analysis	Apply system safety to a facility and its operation	Used to comply with OSHA 1910.119
32	Failure modes and effects analysis (FMEA)	Determine and evaluate effects of subcomponent failures on system	Any system, subsystem, component, procedure, interface, etc.

(*continued*)

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
33	Failure modes, effects, and criticality analysis (FMECA)	Tabulate all system failure modes	Essentially a reliability tool
34	Fault hazard analysis	Systematically examine a system or facility using inductive analysis	Any system, subsystem, component, procedure, interface, etc.
35	Fault isolation methodology	Safety analysis of computer-controlled unmanned systems	Large electromechanical hardware/software systems
36	Fault tree analysis (FTA)	Postulate undesirable end event and examine contributing events	All systems wherein undesirable end events can be foreseen
37	Fire hazards analysis	Examine fire hazards using system safety techniques	Any system with fire safety concerns
38	Flow analysis	Evaluate effects of flow of fluids or energy	All systems that transport or control flow of fluids or energy.
39	Hazard analysis	Application of quantitative methods to solve safety problems	A generic technique that can be applied to chemical processes and similar systems.
40	Hazard and operability study (HAZOP)	Group review using structured brainstorming	Began with chemical industry. Any process or product using brainstorming
41	Hazard mode effects analysis	Introductory technique to determine if further safety analysis is necessary	Any project with safety concerns
42	Hardware/software safety analysis	Integrated hardware/software safety analysis	Used with PHA or SSHA
43	Health hazard assessment (HHA)	Detailed review of hazardous materials	Any system
44	Human error analysis	Evaluate any system where human error is of concern	Any system with human interfaces
45	Human factors analysis	Evaluate functions, tasks, resources among humans and machines	Any system with active human involvement
46	Human reliability analysis (HRA)	Assess factors of human reliability	Any system with active human involvement
47	Interface analysis	Identify potential hazards occurring due to interface incompatibilities	All systems with subsystems or components
48	Job safety analysis	Assess efficient and safe ways of task performance	Human operator functions

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
49	Laser safety analysis	Assess hazards associated with nonionizing radiation	All laser operations
50	Management oversight and risk tree (MORT) analysis	Analyze system to determine detailed information	All systems and processes
51	Materials compatibility analysis	Analyze physical degradation due to materials incompatibility	Aerospace, military, nuclear, marine, and chemical systems and processes
52	Maximum credible accident/worst case	Determine upper bounds of potential accident environment	All systems
53	Modeling	Create visual representation of complex safety program or process	Large and complex safety programs wherein a review tool is desirable
54	Naked man	Evaluate basic system to determine need for controls	Any system; particularly applicable to confined spaces
55	Network logic analysis	Examine a system in terms of Boolean mathematical representation	All systems that can be represented in bimodal elemental form
56	Nuclear criticality analysis	Ensure nuclear safety by eliminating possibility of a nuclear reaction	All facilities that handle fissile material
57	Nuclear explosives process hazard analysis	Identify high consequence (nuclear) activities to reduce possibility of nuclear explosive accident	Nuclear or similar high-risk activities
58	Nuclear safety analysis	Implement safety analysis requirements for nuclear facilities	All nuclear facilities and operations; DOE and NRC have rigid requirements
59	Nuclear safety cross-check analysis	Verifies software designs associated with nuclear systems	At present applies to military nuclear weapon systems
60	Operating and support hazard analysis	Identify and evaluate hazards associated with system operation	Operational phase of the systems acquisition cycle
61	Operational readiness review	Demonstrate the safety of startup or restart of a nuclear facility	DOE requirement; systematic approach to any complex facility
62	Petri net analysis	Model system components at an abstract level	Software control systems
63	Preliminary hazard analysis (PHA)	Initial analysis at early stages of system design	All systems

(*continued*)

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
64	Preliminary hazard list	List hazards at early stages of system design for management	Used with PHA or SSHA
65	Probabilistic hybrid analytical system evaluation	Describes the potential for failure and help in weighing cost–benefit analysis	Modeling where inputs lack precise definition of have dependence
66	Probabilistic risk assessment (PRA)	Quantified analysis of low probability, high severity events	Initially nuclear power industry, now any system with catastrophic accident potential
67	Procedure analysis	Step-by-step review of operational tasks	Systems involving human operators
68	Process hazard analysis	Management of highly hazardous chemicals	Requirement of 29 CFR 1910.119 for chemical process industry
69	Production system hazard analysis	Identify hazards associated with the manufacturing process	Transition from development engineering to production process
70	Prototype development	Modeling or simulation analysis of preproduction product	All manufacturing systems
71	Radiological hazard safety analysis	Structured approach to characterization and categorization of radiological hazards	Broadly applicable to all facilities engaged in managing radioactive materials
72	Relative ranking	Rank hazardous attributes (risk) of process	Any system wherein a ranking approach exists or can be constructed
73	Repetitive failure analysis	Model recurring events that prevent system from performing its function	Currently used in nuclear industry; potential for transfer to other fields
74	Risk-based decision analysis	Efficient approach for making rational and defensible decisions in complex situations	Applies to a wide spectrum of safety and economic analysis
75	Root cause analysis	Identify causal factors relating to a mishap or near- miss incident	Any system; widely used in aerospace and nuclear industries
76	Safety review	Generic assessment process	Any existing system

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
77	Scenario analysis	Evaluation by postulating accident scenarios	All systems, particularly novel systems where there is little experience
78	Seismic analysis	Ensure structures and equipment resist failure in seismic event	Physical structures and equipment
79	Sequentially timed events plot (STEP)	Define and assess systems (accident analysis)	Any system that can be modeled
80	Single-point failure analysis	Identify those failures that would result in catastrophic events	Hardware and software systems and formalized human operator procedures
81	Sneak-circuit analysis	Identify unintended paths or sequences	Control and energy-delivery circuits of all kinds
82	Software failure modes and effects analysis (SFMEA)	Identify software-related design deficiencies	Any software process
83	Software fault tree analysis	Identify root causes(s) of undesired software events	Predominantly, software controlled hardware systems
84	Software hazard analysis	Eliminate software hazards during development process	All software development processes
85	Software sneak circuit analysis (SSCA)	Identify program logic that could cause undesired events	All software programs
86	Statistical process control	Understand and control variations in process	Any process where sufficient data can be obtained
87	Structural safety analysis	Validate mechanical structures	Any physical entity with a structural design
88	Subsystem hazard analysis	Identify hazards as a result of subsystem design	Any component (or group of components) at the less-than-system level
89	System hazard analysis (SHA)	Concatenate the results of SSHA	Any complex program
90	Systemic inspection	Review or audit a process or facility	Virtually without limit
91	Systematic occupational safety analysis	Evaluate facility from an OSHA standpoint	Any operation with personnel involved
92	Task analysis	Safety analysis of operation on task-by-task basis	Any operation with personnel involved
93	Technique for human error prediction (THERP)	Provide quantitative measure of human operator error	Any operation with personnel involved

(*continued*)

TABLE 14.4 (*Continued*)

No.	Technique	Purpose	Application
94	Test safety analysis (TSA)	Ensure safe environment during systems and prototype testing	Any test program
95	Threat hazard analysis	Evaluate potential threats (enemy) and self-induced (accident) throughout life cycle	Weapons systems; mandatory requirement of Mil-STD-2105B
96	Time/loss analysis (T/LA) for emergency response evaluation	Evaluate loss outcomes resulting from mishaps	Emergencies of all types
97	Uncertainty analysis	Identify the incertitude of result based on confidence levels	Any quantified safety analysis
98	Walkthrough task analysis	Determine and correct direct/root causes of unplanned occurrences	Any operation or process
99	What-if analysis	Identify hazards through a brainstorming approach	Any operation or system
100	What-if/checklist analysis	Logical identification of hazards combing two techniques	Any system
101	Wind/tornado analysis	Analysis of hazards resulting from all types of winds	All structures and buildings

Source: Stephans, R. and Talso, W., (Eds) *System Safety Analysis Handbook*, 1997, pp. 3–4 to 3–7. Reproduced with permission System Safety Society.

A detailed discussion of all of these techniques is beyond the scope of this chapter. However, a few techniques that are unique to the system safety HSI domain are described below. Items discussed are:

1. Preliminary hazard analysis
2. Event tree analysis
3. Fault tree analysis
4. Failure mode and effects analysis
5. Fault hazard analysis
6. Subsystem hazard analysis
7. System hazard analysis
8. Cause–consequence analysis

14.3.1 Preliminary Hazard Analysis

The preliminary hazard analysis (PHA) activity is a safety engineering and software safety engineering function performed to identify the system hazards and their preliminary causal factors during system development. The hazards are formally documented to include information regarding the description of the hazard, causal factors, the effects of the hazard, and preliminary design considerations for hazard control by mitigating each cause. This analysis is preliminary and is used to provide early design considerations that may or may not become design requirements. The PHA activity can be used even before the system has been physically designed. For example, during the conceptual design phase of a system (when no prototypes or mockups exist), a PHA can be conducted using a team of safety personnel associated with the design of that system. Performing the analysis includes assessing hazardous components, safety-related interfaces between subsystems, environmental constraints, operation, test and support activities, emergency procedures, test and support facilities, and safety-related equipment and safeguards. The hazard analysis can start with a listing of hazards and a simple worksheet analysis, or can be conducted by using a series of "what if" scenarios. Figure 14.8 shows a sample Preliminary Hazard List and Preliminary Hazard Analysis Worksheet (U.S. Army, 1990). The actual hazard analysis process can become quite involved. Figure 14.9 outlines an example process flow for conducting PHAs (Clemens and Simmons, 1998, p. III-6).

The PHA becomes the springboard documentation to launch the subsystem hazard analysis (SSHA) and system hazard analysis (SHA) analyses as the design matures and progresses through the development life cycle. Preliminary hazards can be eliminated (or officially closed through the SSWG if they are deemed to be inappropriate for the design. For more comprehensive information readers should refer to texts devoted solely to system safety techniques and methods such as Li (1999), Clemens and Simmons (1998), Alberico et al. (1999), and Stephans and Talso (1997).

14.3.2 Event Tree Analysis

The event tree analysis (ETA) is an analytical tool that can be used to organize, characterize, and quantify potential accidents in a methodical manner. An event tree models the sequence of events that results from a single initiating event. The ETA concept uses forward logic; in other words, events are graphed from an initiating event (starting

Preliminary Hazard List

Part	Hazard	Cause	Effects	Hazard Category	Comments

Preliminary Hazard Analysis Worksheet

Part	Hazard	Cause	Effects	Hazard Category	Corrective or Preventive Action

Figure 14.8 Sample preliminary hazard list and preliminary hazard analysis worksheet.

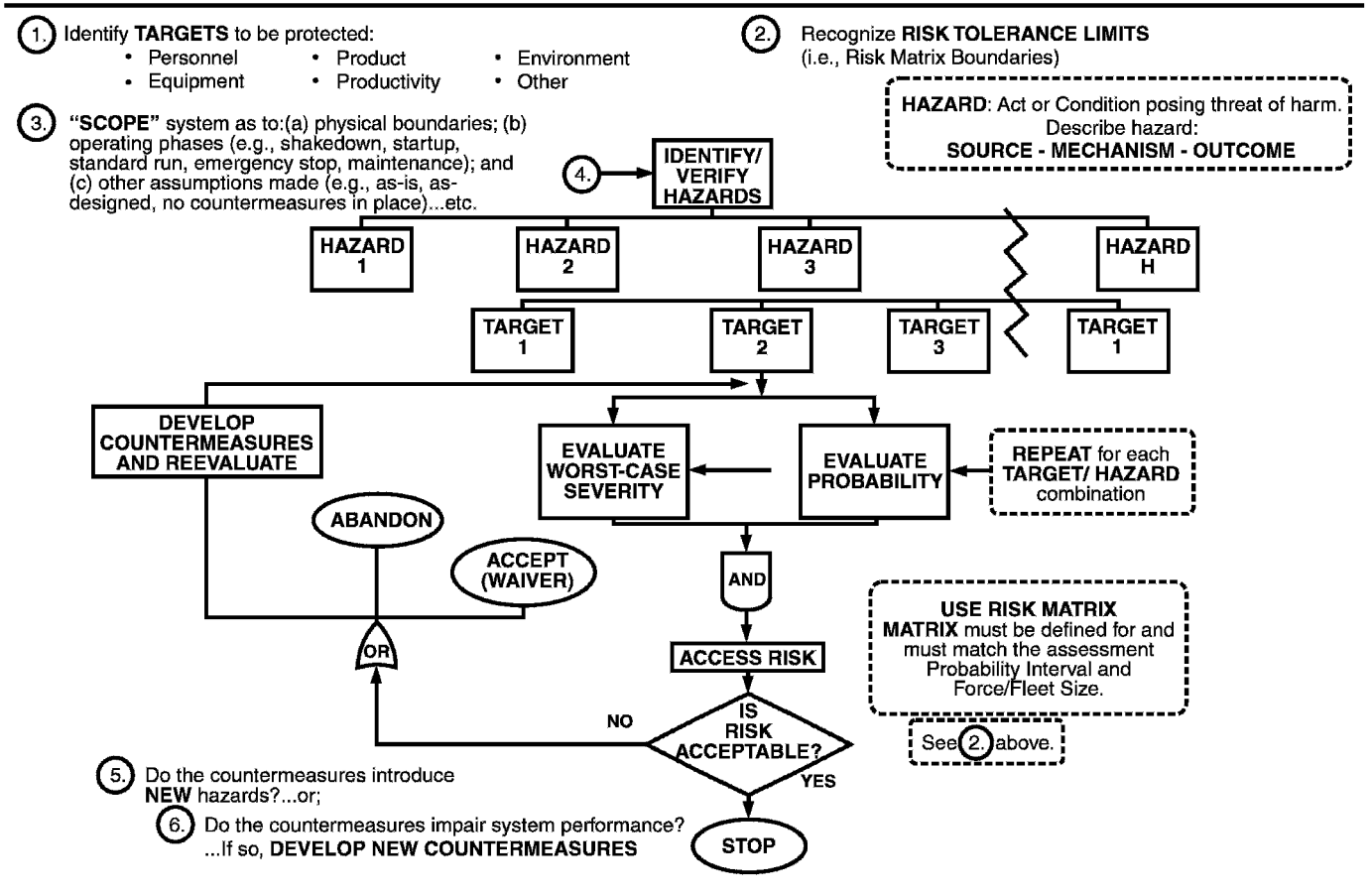


Figure 14.9 Preliminary hazard analysis process flow.

point) to the consequent or resulting events. This logic approach is inductive, which means that the logic flows from the specific to the general. The process begins by selecting initiating events, both desired and undesired, and developing consequences through consideration of system/component failure-and-success alternatives. Identification of initiating events may be based on review of the system design and operation, the results of another analysis such as a failure modes and events analysis (FMEA), or personal operating experience acquired at a similar facility. The safety professional should then postulate the success and failure of the mitigating systems and continue through all alternate paths, considering each consequence as a new initiating event. Figure 14.10 is an example of an ETA using a building fire.

14.3.3 Fault Tree Analysis

The purpose of a fault tree analysis (FTA) is to assess a system by identifying a postulated undesirable end event and examining the range of potential events that could lead to that state or condition. The FTA can model the failure of a single event or multiple failures that lead to a single system failure. The FTA is a deductive approach meaning that the logic flows from general to specific, or moves from an event that is a result to the events that produced the result. The method identifies an undesirable event and the contributing elements (faults/conditions) that would precipitate it. The contributors are interconnected with the undesirable event, using network paths through Boolean logic gates. Figure 14.11 demonstrates a basic graphical depiction of the relationships between events and conditions that are associated with a car and a train on the section of a track simultaneously. See Stephans and Talso (1997) for specifics on particular FTA techniques.

The box with the words "Car and Train on Track at Same Time" in Figure 14.11 represents the top event that involves a fictional scenario in which an accident occurred

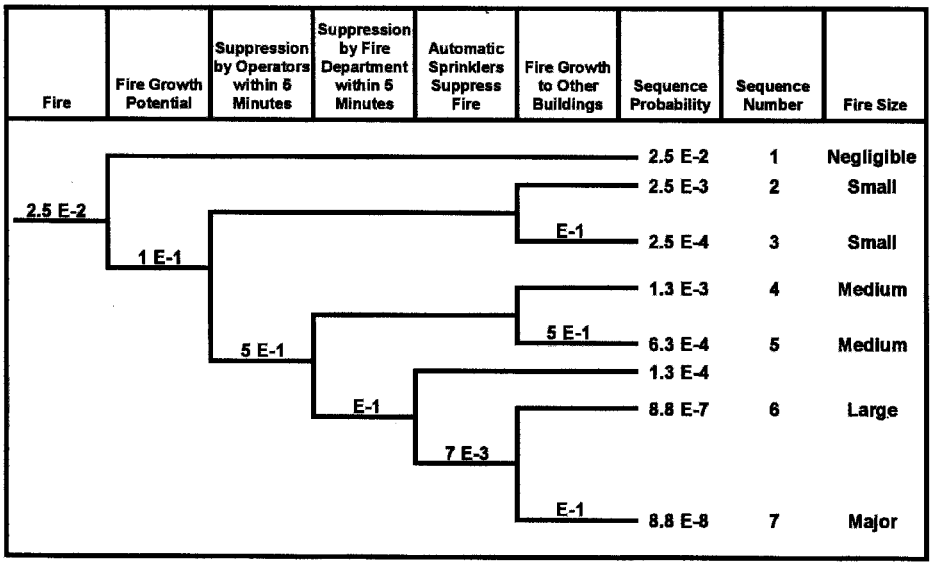


Figure 14.10 Example of an event tree analysis for a building fire. (Reprinted with permission, System Safety Society, Stephens and Talso, 1997.)

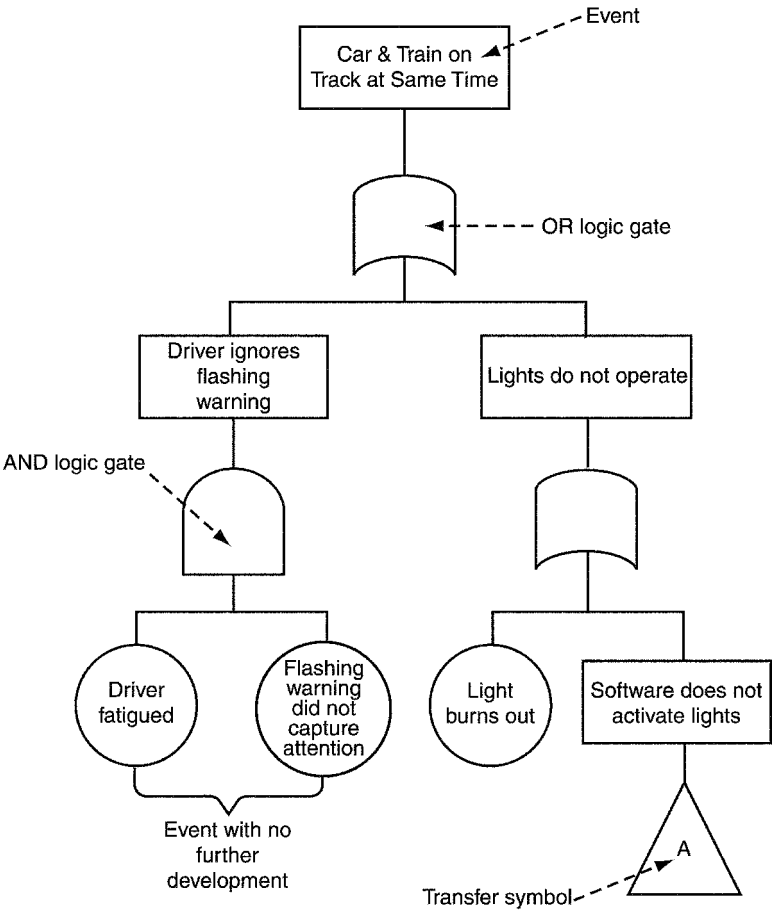


Figure 14.11 Fault tree of a car and train accident scenario.

due to a train collision with a car. The circles represent those basic events that are not analyzed further. The object that looks like a quarter moon on its side is an OR gate. It indicates that any of the events or conditions that lead to it can cause the mishap. Another symbol is the AND gate, which looks like a half moon lying on its flat side and indicates that all the conditions below it must exist for the next event to take place. Transfer symbols are used to indicate continuation to or from another analysis. Fault trees are useful for helping to focus efforts on safety critical areas, visually displaying logic, and showing the relationships between conditions and events. Further, FTA helps the safety engineer to completely understand the subsystem or component being analyzed and help identify the root causes of the top event. If probability data is available for the basic events, then the probability of the top event can be mathematically determined.

However, FTA has limitations. One problem is that the top event of a fault tree must be clearly defined and limited in scope to be effective. If the top event is not clearly defined the analysis will become confusing and possibly misleading. Another limitation is that human factors failures are difficult to model with this type of analysis. It is also important

to understand that FTA is subjective; thus, no two fault trees will be the same when done by two different assessors. Still, another limitation is that FTA can be expensive because of costs in obtaining data. Finally, a fairly mature systems design is required before FTA can be used effectively.

14.3.4 Failure Mode and Effects Analysis

Another common analysis method is the failure mode and effects analysis (FMEA). This analysis is a qualitative reasoning approach best suited for reviews of mechanical and electrical hardware systems. The FMEA technique (1) considers how the failure modes of each system component can result in system performance problems and (2) ensures that appropriate safeguards against such problems are in place. The system is divided up into different units in the form of a block diagram. Figure 14.12 illustrates the functional block diagram on four components (U.S. Coast Guard, 2001, p. 9-5). Failure modes are identified for the various units. Conceivable causes, consequences, and the significance of failure are assessed for each failure mode. An investigation is made into how the failure can be detected. Recommendations for suitable control measures are made. To document the findings, the FMEA record sheet addresses the following: identification, failure mode, failure cause, failure effect, failure detection, possible action, and probability and/or criticality level. A quantitative version of FMEA is known as failure modes, effects, and criticality analysis (FMECA). Table 14.5 provides a vessel-based FMEA record sheet example from the U.S. Coast Guard (Walker, 2000). The terminology used is similar to that mentioned above.

14.3.5 Fault Hazard Analysis

The fault hazard analysis (FHA) method is a basic inductive method of analysis that is used to perform an evaluation that starts with the most specific form of the system and integrates individual examinations into the total system evaluation. The purpose of the FHA is to systematically examine a facility or system and to identify hazards and their effects. The FHA methodology, like the FMEA, is to examine the system, element by

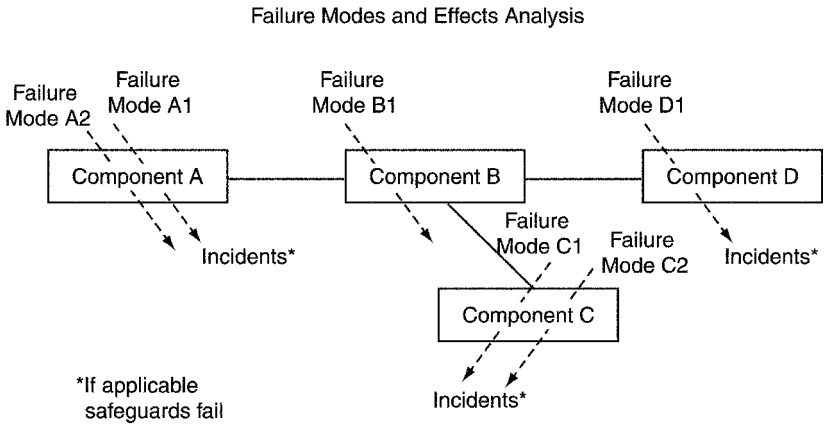


Figure 14.12 Failure modes and effects analysis.

TABLE 14.5 Example Failure Modes and Effects Analysis (FMEA)—Functional Failure-Based

Functional Failure	Loss Scenario (Effect)	Percent of All Reportable Marine Events	Dominant Causes	Applicable Inspection Activity	Inspection Effort	Criteria	Change in Risk
			Function: Providing Start Air for Engines				
No or insufficient volume of start air provided to engines	No engine start, which can lead to loss of propulsion and a disabled vessel	~25	Condensation in bottles (62%)	Blowdown bottles during inspection	<10 min	Do not have to do on variable pitch propellers	Current practice (high negative impact if not performed)
				Verify that regular blowdowns are scheduled and occurring (by record review)	<5 min	See above	Possibly high positive impact
	Could possibly lead to a grounding, collision, etc.			Communicate importance of blowdowns to crew	<5 min	See above	Current practice (high negative impact if not performed)

Disabled compressors (multiple compressors) (5%)	Operation verification (measure discharge pressure)	<10 min	See above	Current practice (high negative impact if not performed)
	Visual inspection for leaks, gauges functioning, obvious defects, etc.	<5 min	See above	Current practice (high negative impact if not performed)
	Communication with pilots about known problems during transit	<5 min	See above	Current practice (high negative impact if not performed)

element. Modes in which each element can fail are then identified. Finally, the effects to the system for each failure mode are determined, taken both singly and in combination with others (some variations classify effects according to their severity). The FHA method is very similar to a PHA and is a subset of the FMEA technique. Figure 14.13 provides an enhanced example of the FHA, which is very similar to the PHA. See Stephans and Talso (1997) for more information on FHAs.

14.3.6 System Hazard Analysis

The system hazard analysis (SHA) provides documentary evidence of safety analyses of the subsystem interfaces and system functional, physical, and zonal requirements. As the SSHA identifies the specific and unique hazards of the subsystem, the SHA identifies those hazards introduced to the system by the interfaces between subsystems, man–machine, and hardware–software. It assesses the entire system as a unit and the hazards and failure modes that could be introduced through system physical integration and system functional integration.

The SHA is accomplished in much the same way as the SSHA. That is, hazards and hazard causal factors are identified, hazard mitigation requirements communicated to the design engineers for implementation, and the implementation of the safety requirements are verified. However, several differences between the SSHA and SHA are evident. First, the SHA is accomplished during the acquisition life cycle where the hardware and software design architecture matures. Second, where the SSHA focused on subsystem-level hazards, the SHA refocuses on system-level hazards that were initially identified by the PHA. In most instances, the SHA activity will identify additional hazards and hazardous conditions because the analyst is assessing a more mature design than that which was assessed during the PHA activity. And third, the SHA activity will put primary emphasis on the physical and functional interfaces between subsystems, operational scenarios, and human interfaces. Figure 14.14 (Alberico et al., 1999) demonstrates the concept with a propulsion system. For further insight refer to Alberico et al. (1999) and Stephans and Talso (1997).

In the example illustrated in Figure 14.14, the fault tree approach is used to analyze a system-level hazard "Loss of Thrust Actuation." The hazard is depicted as the top event of the fault tree. The SHA activity analyzes all causes to the hazard, including the software branch that is a branch of the OR gate to the top-level event. This particular hazard has hardware causes (actuator control arm failure), human error causes (pilot commands shutdown of control unit), and software-induced errors causes.

Further, "Thrust Actuation" is a function of the propulsion system and administratively controlled by the propulsion Integrated Product Team (IPT) of contractor A. The computer hardware and software controlling the thrust actuators are also within the engineering boundaries of the same IPT. However, the software safety analyst has determined, in this case, that a fault condition in the computer operating system (OS) is the primary causal factor of this failure mode. This OS fault did not allow actuator sensor data to be read into sensor limit tables and allowed an *overwrite* to occur in the table. The actuator control algorithm was utilizing this sensor data. In turn, the actuator control computer software component functional architecture could not compensate for loss of credible sensor data that transitioned the system to the hazardous condition. In this example, the actuator and controlling software are designed by contractor A; the sensor suite and throughput data bus are designed by contractor B; and the computer OS is developed by contractor C.

SYSTEM: Launch Car				SUBSYSTEM: Stabilization						Revision 1 as of 18 April 1993	
1 Number	2 Unit/ Item	3 System Event Phase	4 Brief HAZ Description	5 Effect on System	6 Severity	7 Probability	8 Index	9 Category	10 Recommended Control Requirement/Action	11 Effects of Recommended Action	
SB10X01	Stab Sys	Deploy	Mechanical energy of suppressed load	LSR lower while train is in motion resulting in rail car damage or derailment	I	D	8	X	Provide positive restraint of LSRs during transport	Reduces probability of occurrence I=12 (E - probability)	Design reviews and verification of incorporation into system design
SA10X02	HPU	Deploy	Chemical energy of hydraulic fluid	Spilled hydraulic fluid could result in a fire	I	D	8	X	Control leakage of fluid thru fittings of boundary failure. Select fire tolerant fluid	Reduces probability of occurrence I=15 (E - probability)	Open pending subsequent design reviews and verification of incorporation into system design
	SCU	Maint	Electrical Energy - Electrical Potential	Electrocution/shock to personnel from contact with energized system components	I	D	10	X	Design per MIL-STD-454, Req 1	Reduces probability of occurrence	Open pending subsequent design reviews and verification of incorporation into system design
			Electrical Energy	Erroneous signals from the SCU could result in improper leveling and MLC overturning during stabilization or erection operations	I	D	8	A	Provide two fault tolerance in the design	Reduces probability of occurrence	Open pending subsequent design reviews and verification of incorporation into system design

Figure 14.13 Fault hazard analysis example (reproduced with permission, Systems Safety Society, Stephans and Talso, 1997).

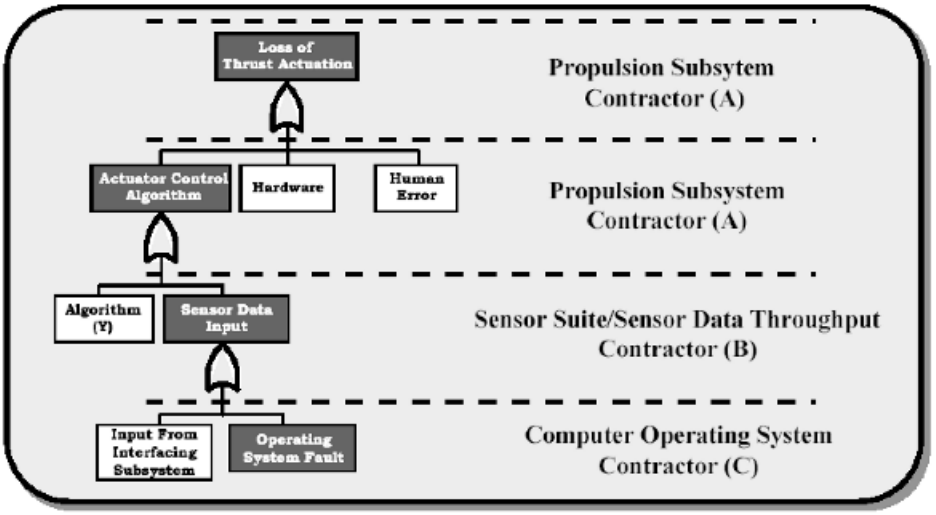


Figure 14.14 Example of a system and subsystem hazard analysis.

The safety analysis performed by contractor C is demonstrated in this example. If contractor C is contractually obligated to perform a safety analysis (and specifically a software safety analysis) on the computer OS, the ability to bridge (bottom-up analysis) from an OS software fault to a hazardous event in the propulsion system is extremely difficult. The analysis may identify the potential fault condition but not identify its system-level effects. The analysis methodology must rely on the "clients," of the software OS, or contractor A, to perform the top-down analysis for the determination of causal factors at the lowest level of granularity.

14.3.7 Subsystem Hazard Analysis

The hazard analysis performed on individual subsystems of the (total) system is the subsystem hazard analysis (SSHA). This analysis is "launched" from the individual hazard records of the PHA that were identified as a logically distinct portion of a subsystem. Although the PHA is the starting point of the SSHA, it must be only that—a starting point. The SSHA is a more in-depth analysis of the functional relationships between components and equipment (this also includes the software) of the subsystem. Areas of consideration in the analysis include performance, performance degradation, functional failures, timing errors, design errors, or inadvertent functioning.

14.3.8 Cause–Consequence Analysis

The cause–consequence analysis (CCA) combines the inductive reasoning features of ETA with deductive reasoning features of FTA. The result is a technique using six steps that relates specific accident consequences to their many possible causes. The first step selects an event or type of accident situation to be evaluated. The various accident paths are then constructed based on the chronological successes and failures of the appropriate safety

functions (systems, operator actions, etc.) that influence the course of the accident resulting from the event. The next step develops the accident paths resulting from the event through an ETA. Through the use of an FTA, the analyst develops the initiating event and the safety function failure event to determine their basic causes. The accident sequence is composed of a sequence of events, each of which is a top event for a fault tree that is part of the cause–consequence diagram. For an accident sequence to occur, all of the events in the sequence must occur. Evaluating the results of the CCA is a two-step process. First, the accident sequences are ranked based on their severity and importance to plant safety. Then, for each important accident sequence, the accident sequence minimal cut sets can be ranked to determine the most important basic causes. The final step in performing a CCA is to document the results of the study.

14.4 SYSTEM SAFETY PROCESS

The system safety process operates within the context of the systems acquisition process as illustrated in Figure 14.15. When the system is conceived, the designers take the operational environment, lessons learned from the past, technology, and the doctrine of how to achieve success, to determine the requirements for the system. As these requirements become the design, system safety engineers take these requirements, identify the hazards, and determine the safety requirements for the system. Testing that is conducted on the system also helps identify hazards. As the design of the system matures, safety engineers generate reports on the safety of the system to document the risk. The design and risk acceptance authorities use these reports to decide whether to accept the mishap risk and approve production of the design or allocate more resources for mishap risk reduction.

In order to determine the safety of a particular system, there are a number of important questions that need to be answered to define the system for which safety is a concern:

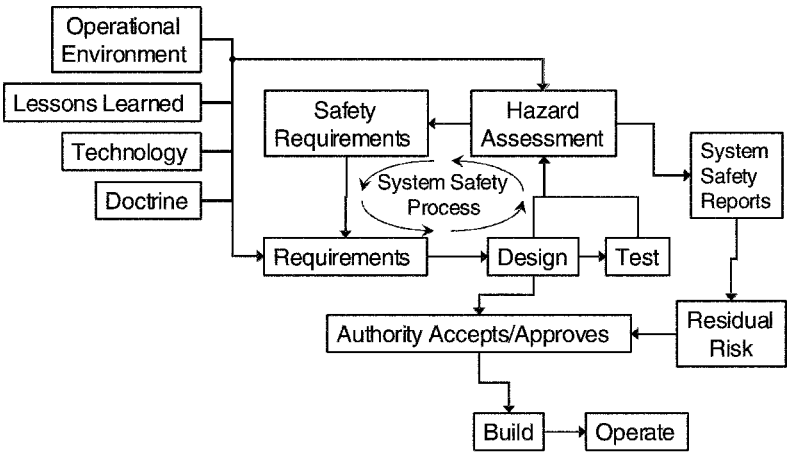


Figure 14.15 System safety process within the systems acquisition process.

- What are its boundaries?
- What are the people, machines, and processes that make up the system?
- What are the needs and objectives that the system must fulfill?
- How do the components of the system interact?
- What are the interfaces with other systems?
- What parts of the system can we control and redesign to make them safer and more effective in the desired functions of that system?

Regardless of the methods used to conduct risk analysis within the system safety process, organizations must have a system safety program and plan. (Refer to Fig. 14.1 as the general model for the following steps.)

Step 1. Develop System Safety Plan The first step of a system safety program is to develop a system safety program plan integrated with other program planning documents. OSHA addresses the components of a system safety program plan. Figure 14.16 shows how the elements of the system safety program are coordinated with other program efforts to ensure appropriate safety data is available at decision points in the program.

The preliminary hazard list (PHL) is developed at the beginning of the design and entered into the hazard tracking system (HTS). Following the preliminary design review, system safety starts a functional hazard analysis (FHA) to help determine what safety requirements need to be included in the requirements documentation. Systems safety further develops the FHA into an SSHA and SHA. The software hazard analysis and the safety assessment report are used at the critical design review to determine whether the design is ready for production. In conjunction with the critical design review, the residual risk will need to be accepted for each hazard that has not been eliminated. In addition, the safety data will be used to develop the test program. The data from the test program will be used to identify additional hazards and verify that mitigation measures are effective. Figure 14.16 also shows that meetings of the SSWG are scheduled to support program milestones and other requirements.

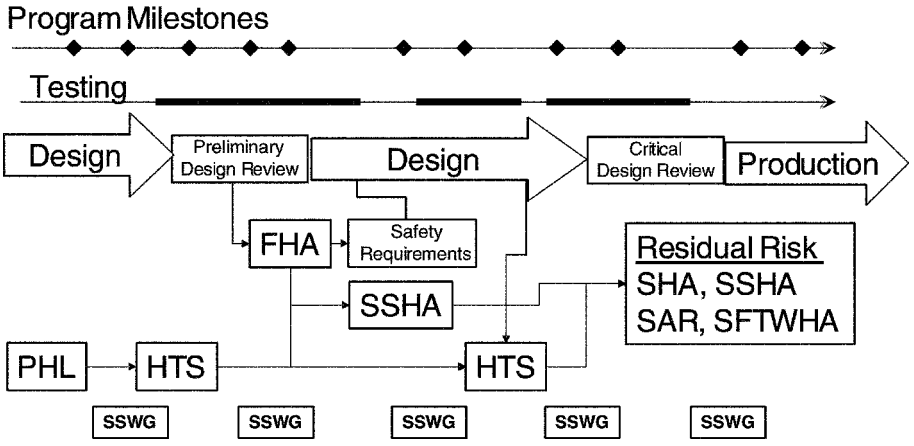


Figure 14.16 System safety program planning.

This all points out the importance of system safety understanding the program needs and writing the system safety plan to ensure that resources are allocated and personnel are assigned to support the program schedule. Some things that might go into the plan are the system safety program purpose, safety policies, responsibilities, hazard assessment plan, and system safety specific information on the product.

Table 14.6 shows the typical content items of the system safety plan. For example, critical items for the system safety plan are the policy, objectives, and risk management methodologies.

Policy The safety analysis should spell out the management's policies regarding system safety and include specifics as needed for the program. Some ideas for this include:

1. Proactively identify all hazards that could cause personal injury or equipment damage.

TABLE 14.6 Content of a System Safety Program Plan

References List organizational documents that govern safety program in general and system safety specifically. List applicable government documents as well as company directives. List industry standards that will be used to give guidance to system safety group and other teams in system safety methodologies and techniques that will be used.

Scope Delineate what plan applies to and what general areas of effort plan covers.

Policy Spell out in simple terms management's system safety policies pertaining to effort. Restate organizations policies regarding system safety and include specifics as needed for program.

Objectives State in clearest terms final objectives of system safety program

Task Objectives Here is where specific tasks for various members of system safety group and supporting teams are delineated. Make sure responsibilities are clearly delineated and that open communication between members occurs.

Risk Management Methodologies Describe how safety issues are handled and what the process is for identifying and entering hazards into tracking system. Describe how hazards will be classified. Identify when and how hazards will be closed (see Figure 14.17). Describe the process for residual risk acceptance and how acceptance will be documented. Identify items that should be included in hazard tracking system. Define severity levels.

Safety Integration with Other Disciplines Describe lines of communication and information exchange with other teams, working groups, and other supporting organizations.

Schedules Describe how system safety program events interact with overall program schedule. Include timing of reports and other deliverable products. This could be detailed appendix to plan.

System Safety Group Charter This can be an appendix to system safety plan or stand-alone document. Membership should be updated as necessary when there are major program reorganizations, the program passes a milestone, and significant personnel changes occur.

System Safety Document Examples This could include a sample risk analysis formats, hazard tracking formats, and risk acceptance documents.

Glossary of Abbreviations, Acronyms, and Terms Even though trained and experience system safety engineers and managers speak language of system safety, it is good idea to include a glossary to ensure all those who will work with system safety team fully grasp meaning of terms. For those who have not had experience or training in system safety, there is often confusion as to meaning of "risk," "hazards," etc. A good glossary of terms may help prevent confusion and help avoid rabbit trails in discussions on risk of particular hazard or when hazard is ready to close. It also helps to standardize terminology when numerous vendors are subcontracting on particular program.

2. Evaluate the risks associated with system hazards.
3. Eliminate or mitigate hazards to the lowest possible level consistent with operational requirements and resource constraints.
4. Ensure identified hazards and management controls are examined with respect to all applicable design standards and accepted design practices to include operational scenarios and environments.
5. Report residual hazards and associated risk to the appropriate risk decision authority.
6. Document all hazards and risk management decisions throughout the program life cycle.

Objectives The safety analyst should state the final objectives of the system safety program, such as:

1. All potential hazards associated with the program are identified and formally tracked for the life of the system and that risks associated with those hazards are properly managed and resolved.
2. No known residual hazard is accepted without formal documentation of associated risks. The appropriate authority shall make risk acceptance decisions.
3. System safety maintains a two-way interface with the HSI program and all design integrated product teams.
4. Historical safety data is included in the system safety program. Significant safety data are documented as "lessons learned" and will be entered in appropriate data banks and submitted as proposed changes to applicable design handbooks and specifications.
5. Safety measures consistent with system requirements, technical feasibility and cost are included in the system safety planning, development, production, and fielding.
6. Retrofit actions required to improve safety are minimized through the timely inclusion of safety features early in the life cycle of the program.
7. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains acceptable safety-related risk levels.
8. Maximum operational readiness and mission protection will be achieved through accident prevention.
9. Safety consideration is given to system design, production, fielding, and ease of disposal for all hazardous materials.

Risk Management Methodologies The safety analyst should describe such features as how safety issues are handled, how hazards will be classified, and how they will be closed. For example, hazard management tools such as shown in Figure 14.17 might be used in the hazard closure process. The flowchart describes such a process on a U.S Army system. It tracks the hazard process from the point a hazard is identified until the risk is accepted and the hazard closed by the program manager (PM) if the hazard is a low risk, by the program executive officer (PEO) if a medium risk, and the army acquisition executive if a high risk.

Step 2. Identify Hazards The next step after developing the system safety plan is to identify the hazards. The system safety process follows the iterations of the system engineering process. As design requirements are identified in the conceptual phase and

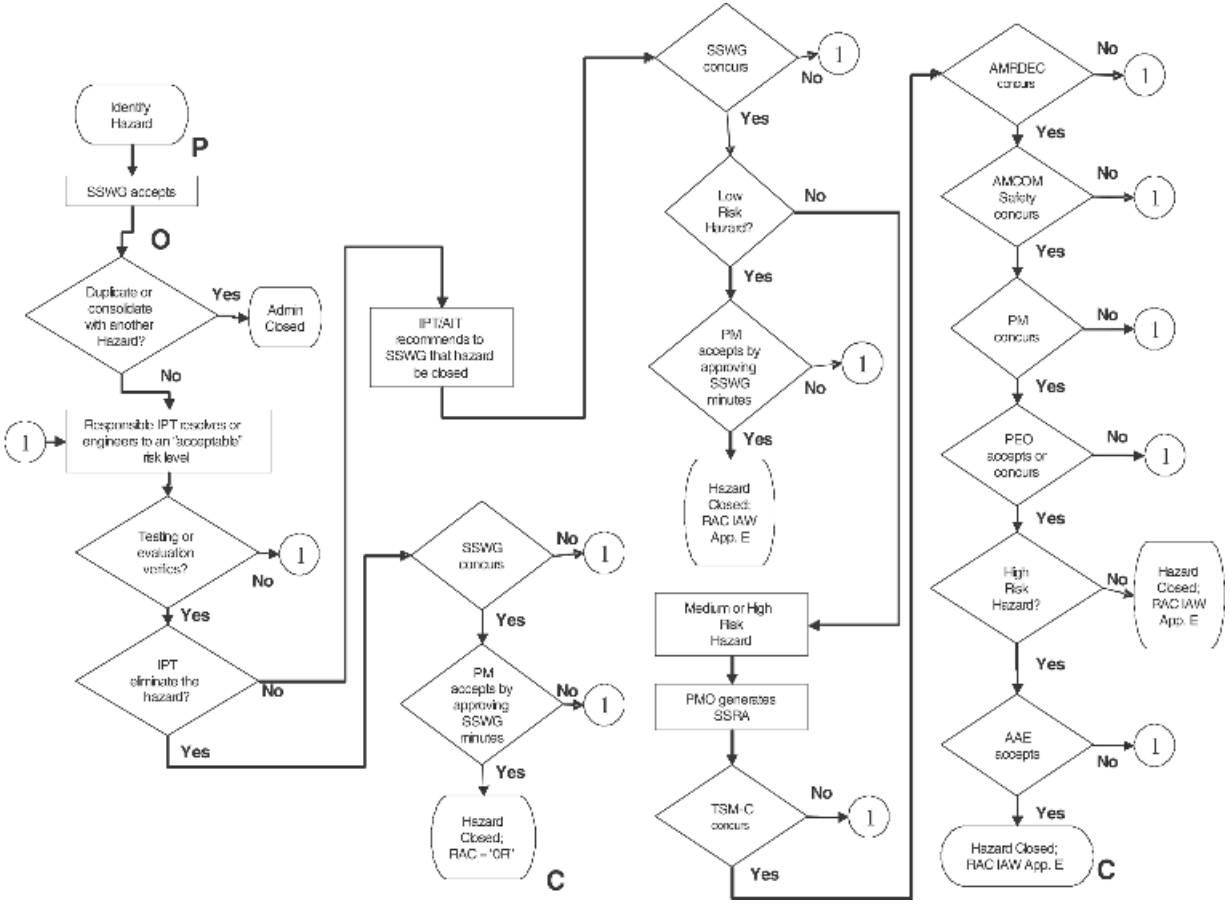


Figure 14.17 Flowchart of a hazard closure process.

continuing throughout the entire system life cycle, so are hazards. One fundamental concept understood by safety engineers is that all mishap risk is never fully identified. There are always some undiscovered conditions that can cause subsystems and components to interact in undesirable ways that create hazards. So never be surprised to find new hazards as the system design matures, is tested, and is fielded.

One of the best places to start looking for hazards is the legacy system for which the new system is comparable or replacing. For example, the DoD reviewed hazard lists from current fighter aircraft prior to initiating the joint strike fighter effort. The basic subsystems and components of a fighter aircraft are similar, and many of the interactions between the airframe, engines, flight controls, avionics, life support system, etc. produce the same hazards. Of course, these aircraft also introduce new concepts, technologies, and materials along with the introduction of new hazards.

Another method is a hazard checklist. While the checklist can never be all-inclusive, the framework provides a starting point to catch hazards that may have otherwise been overlooked.

Still another method of unearthing hazards is to perform analyses on the functions of the system to see what functions the overall system, subsystems, and components must do to operate properly. The analyst should start with a list of system functions. These may be derived from the work breakdown structure, brainstorming ideas, or requirements documents for the system. As an example, Figure 14.18 shows a diagram of the top-level functions for a military helicopter.

As each function is studied ask the following, "What harm could come if this system, subsystem, or component fails to function correctly?" "What would happen if this failure is not detected?" "How would it be different if it is detected?" All the functions depicted must be present for the helicopter to work effectively.

The functional hazard analysis process produces a very comprehensive listing of hazards. This method is effective because it is a top-down process of identifying hazards and mitigation measures based on what the system must do and not just on the current design of the hardware. The analysis supports assessments on component criticality and hazard severity. With data supplied by the reliability engineers, a determination on the probability of the hazard resulting in a mishap can then be made.

It is also very useful in analyzing the system software in order to determine that the software functions correctly and what would happen if it failed. Just like functional hazard analysis on hardware, this information helps software designers to better understand the system requirements and design in order to make a better product. A major difference between hardware and software is that the former is visible while the latter is not. This makes software system safety analysis especially difficult.

The functional hazard analysis needs to be updated any time a function is added, deleted, or changed or when another type of analysis reveals additional failure modes. As soon as design requirements are generated, the functional safety analysis should begin.

As a system matures, hundreds, even thousands, of hazards could be identified depending on the complexity of the system. A PHL would be created only in the very early stages with hazards undergoing a PHA when appropriate. The PHA, usually the first analysis, can be very valuable because it identifies and characterizes possible hazards early in the design phase when needed redesign is least costly. It identifies known hazards, such as explosives, radiation sources, pressure vessels or lines, toxic materials, and high voltage, and specifies where each will occur in the system and the method to be used to eliminate the hazard or control the associated risk.

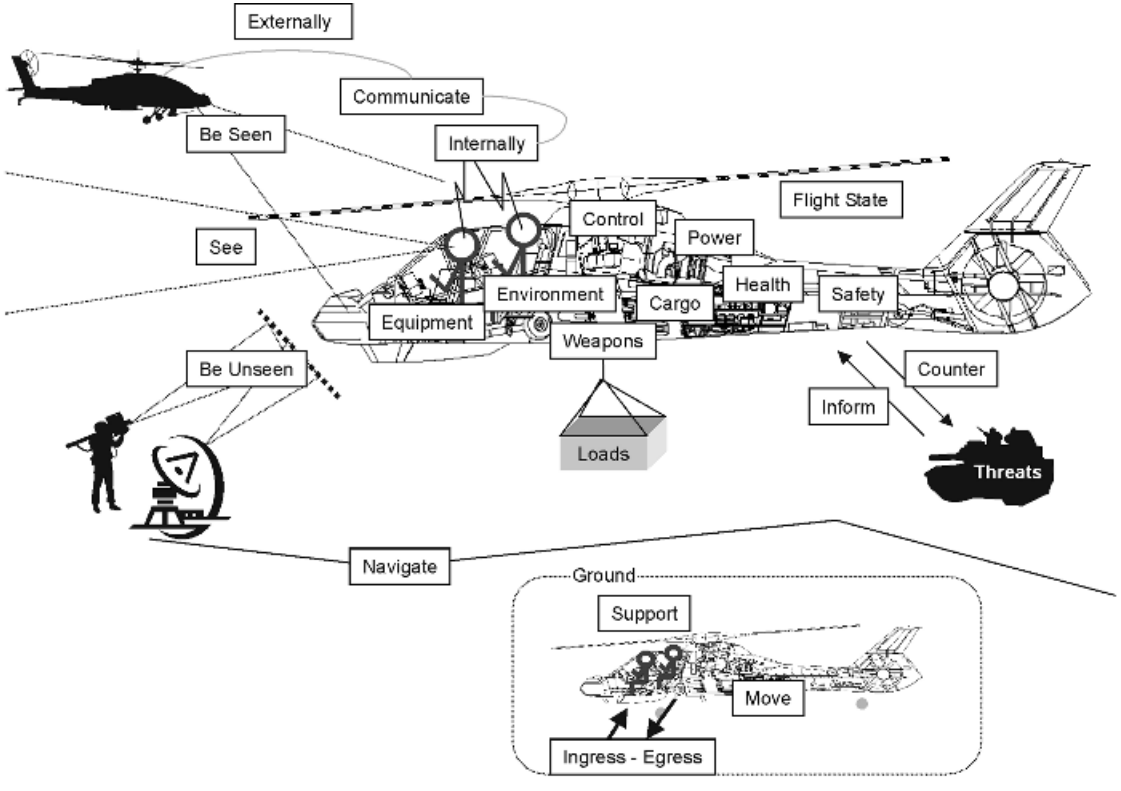


Figure 14.18 Functions of a military helicopter.

Finally, the analyst needs to ensure the hazard is thoroughly described in the hazard description. The narrative of the potential hazard contains three elements that express the threat: a source, a mechanism, and an outcome. A source is an event or a condition that serves to initiate the chain of events in the mishap. A mechanism is the means by which the source can bring about the harm. An outcome is the harm that will be suffered in the mishap. If a hazard cannot be described using a source, a mechanism, and an outcome, it likely is not a hazard. A complex hazard may have multiple sources, mechanisms, and outcomes and may require a diagram in addition to a narrative to fully describe the hazard.

Step 3. Assess Mishap Risk The third step in the system safety process is assessing the risk of the hazard in question. The most basic way to do this is to select a risk assessment code from the hazard matrix based on the hazard description and knowledge of the system. For example, what would be the risk of a military helicopter striking wires during flight? The severity would be "1," catastrophic, based on the description of catastrophic in Table 14.3. The worst credible outcome would be "Death or permanent total disability; system loss or mishap damage greater then or equal to $1,000,000."

But what is the probability? One way is to examine the mishap experience of a similar existing aircraft. The aircraft could be similar in mission and operating environment. Let's say the existing aircraft has a catastrophic mishap at a rate of 2.1 times 10^{-7} times per flight hour. That plots out to a "D, Remote" in Figure 14.6, since the probability falls in the range of 10^{-5} to 10^{-7} occurrences per flight hour. The resulting assessment based on design differences determines how much better or worse the new helicopter will perform. Perhaps the new helicopter will be able to see the wires better with sensors on board, or perhaps will have better or worse wire strike protection systems on board. Thus, the assessment provides decision makers with comparative information indicating whether the new system will be safe or not.

The final element in the accident analysis is cause–consequence analysis. This step evaluates the effect of the postulated accident on the workers, the public, and the environment. For some facilities, consequence analysis may also include health effects assessment, accident frequency estimates, or safety goal comparisons. Figure 14.19 is an example that highlights causes, preventive features, mitigation features, potential impact, and risk determination. For further information concerning qualitative consequence analysis, see U.S. Department of Energy (1997) for more information on workload analysis.

Step 4. Identify Mitigation Measures The fourth step in the system safety process is to identify those measures that will eliminate or mitigate a hazard. To accomplish this most effectively, system safety engineers use the "system safety order of precedence." Elimination of all hazards would be ideal, however, not practicable from a programmatic point of view and is often impossible. Figure 14.20 illustrates the concept that will be discussed in greater detail below as adapted from the *Software System Safety Handbook: A Technical & Managerial Team Approach* (Alberico et al., 1999).

First in the system safety order of precedence is to design for minimum hazard. Although not always possible, designing to eliminate hazards is preferable to procedures or training to avoid them. In every design there are options, some of which avoid or eliminate the potential for the hazard. If elimination of a hazard cannot be accomplished, the next step is to at least reduce the risk to an acceptable level. The acceptable risk for a hazard can be based on the performance of legacy systems. The acceptability of risk will be refined in

Causes:	Mixing of incompatible chemicals due to personnel error, container leakage, or improper maintenance of equipment
Preventive Features	
Design:	Ventilated storage cabinets and/or storage areas provided with sumps for spill containment
Administrative:	Segregation of non-compatible chemicals, regular inspection of containers and storage areas, instruction of personnel in proper handling techniques
Method of Detection:	Smoke and ionization detectors for fire conditions, personnel observation, appropriate alarms
Mitigation Features	
Design:	Fire suppression equipment (sprinklers, portable fire extinguishers), laboratory fume hoods, ventilation design
Administrative:	Employee training, safety procedures, automatic fire department response, emergency medical technicians available on site
Potential Impact:	Physical damage to affected area, potential water damage, potential injury to personnel from burns, explosions, or inhalation of toxic materials, partial shutdown of operations
Risk Determination:	
Probability Level:	Low
Consequence Level:	Medium
Risk Level:	Low

Figure 14.19 Example category 3 qualitative consequences analysis (uncontrolled chemical reaction).

an iterative review of the design to find an optimum balance of safety and other performance objectives.

The next activity in the order of precedence is to incorporate safety devices. If identified hazards cannot be eliminated or the associated risk adequately reduced through design selection, further risk reduction efforts are required by using fixed, automatic, or other protective safety design features or devices; for example, the addition of air bags and daytime running lights on vehicles.

If the hazard still presents a problem, warning (aural and visual) devices should be added to the system. Incorporate these devices to detect conditions related to the hazard to produce a warning signal for alerting personnel. Make sure the warning device(s) design minimizes incorrect reactions caused by nuisance warnings (false alarms). Work closely with human factors engineering to select visual, audible, or tactile warnings that are not ambiguous and cannot be confused with other warning mechanisms.

Finally, develop procedures and training. The reason procedures and training are listed last is that they rely on humans to provide the safety. People make errors in following procedures when distracted or bored. Training requires continuous monitoring on seldom-

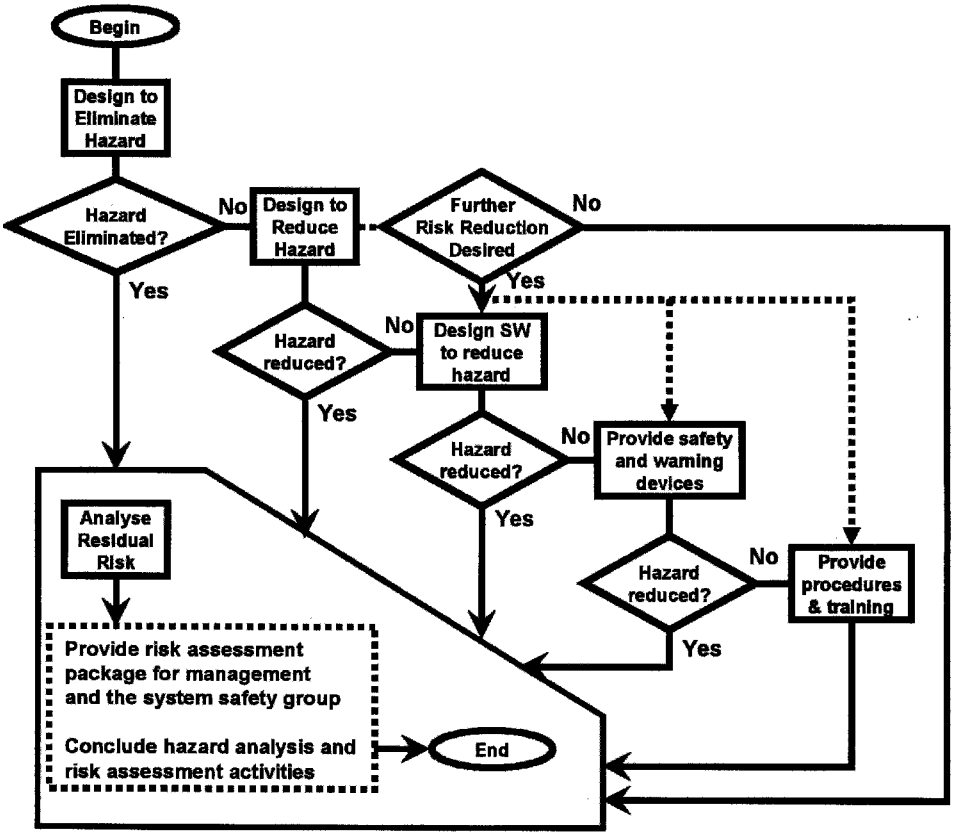


Figure 14.20 System safety order of precedence.

used procedures, like emergency responses, since the system is unable or it is undesirable to provide actual situations to reinforcement training.

It is very important for the safety engineer to work closely with the other engineers in this step of the system safety process. Look for opportunities to apply lessons learned from other systems and for ways to apply new methods and technologies.

Step 5. Verify Mitigation Effectiveness The next step in the process is to establish mechanisms to verify that mitigation measures are in place as designed and effectiveness is verified in actually eliminating or mitigating the hazard. This may involve reviewing drawings to see if proposed design changes were included, inspecting components, subsystems, and the system by observing fabrication and test activities, and by reviewing test reports. These verification mechanisms should be included as part of the hazard tracking system that will be discussed below. Remember that people do fail so verification mechanisms are important. Work closely with system engineering, configuration management, testing, and quality assurance to make sure effective safety-related design changes do make it into the final production configuration.

Step 6. Accept Residual Risk As design decisions are finalized, program management must also begin to formally accept the residual risk. Often these decisions will be

informally addressed prior to the formal acceptance of risk at design reviews and other decision meetings. Make sure the system safety plan clearly spells out how the process works and who must review the risk documentation before the final acceptance decision is made and signed off.

A decision maker may ask, "How do I know when to accept risk?" The best answer is depicted by the "bathtub curve." As depicted in Figure 14.21, the total cost of safety is the sum of the cost of mishaps and the cost of safety mitigation measures. As the resources are expended on safety, the cost of mishaps decreases and the cost of mitigation increases. There comes a point where the cost of one more dollar of mitigation results in just one dollar of mishap cost reduction. The next dollar that is spent will only save 99 cents. This is the optimum level of risk and that is where spending money on risk reduction efforts yields no additional system benefit. This concept can be applied to mitigation measures for a specific hazard or can be applied to all the hazards of the system.

Another question that a decision authority may ask is, "If I have a limited amount of resources to spend on safety, how can I best spend those resources?" The answer is to prioritize the mitigation measures being considered for the entire system based on which ones produce the most reduction in mishap cost for the dollar expended. Usually, those mitigation efforts that bring the system closest to optimum level of risk are where limited resources should be spent.

Often, the critical issue is determining the cost to human life, those injuries and deaths due to mishaps in risk assessment and risk acceptance. The short answer is to determine the costs in terms of replacing trained and experienced people plus any additional cost for worker's compensation and death benefits. For example, the DoD assigns a value to a military aircraft pilot of $1.1 million. There are obviously intangible costs to organizations for injuries and deaths. There are costs in terms of the suffering of families and co-workers. There is lost productivity and effectiveness due to poor morale. There are public relations impacts and legal requirements related to the provision of workers compensation benefits packages. There is time spent dealing with lawsuits and investigations. However, in practical terms, human life is worth what decision makers are willing to spend to protect it. Appropriate authorities must make judgments (whether or not based on quantified values) on how much to spend for risk mitigation to protect human lives. The role of the

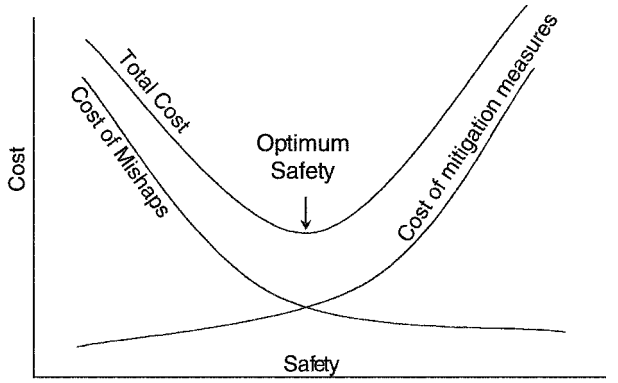


Figure 14.21 The safety "bathtub" curve. [Adapted with permission from Clemens (2002, Sheet 00-6).]

safety engineer is to provide the best information as to the residual risk in terms of dollars, injuries, and deaths over the system life cycle as well as the cost of proposed countermeasures.

Step 7. Track Hazards through Life Cycle The last step in the system safety process is to track the hazards throughout the life cycle of the system. In a complex system there will be thousands of hazards identified over time. The hazards will be published in documents such as the SHA, SSHA, operating and support hazard analysis (O&SHA), or the safety assessment report (SAR). As systems change due to changes in operating the system within a certain environment and planned product upgrades, previously identified hazards may resurface or new hazards may be introduced. Continuous risk reduction efforts will be required.

The best way to track hazards and risk reduction efforts is a computer database. By using such a database, reports can be easily generated to track the progress of risk reduction. Documents can be generated for risk acceptance. Mitigation measures can be tracked as well. Each hazard should have a record in the database. This record may be referred to as hazard tracking record (HTR), an SAR, or another name that fits the organization. The record fields should be described in the system safety plan and include those indicated in Table 14.7.

For example, the status of the hazard is important to record. A possible status could include:

- *Proposed* The hazard has not yet been accepted by the system safety group.
- *Open* The hazard was accepted by the system safety group with no corrective action plan in place.
- *Monitor* The hazard is accepted by the systems safety group with a corrective action plan in place.
- *Recommend Closure* The contractor determines that there will be no further elimination or mitigation of risk by design changes and proposes closure to the systems safety group.
- *Pending Closure* The systems safety group has concurred that the hazard should be closed and has forwarded the closure document to the risk acceptance authority.
- *Closed* The hazard has been eliminated or all corrective actions have been completed.
- *Verified* The appropriate decision authority has accepted any residual risk.
- *Administratively Closed* The hazard was determined by the system safety group as describing a hazard that is already identified in another hazard tracking record or it has been incorporated in the scope of another hazard tracking record.

If a hazard tracking system is thoughtfully designed, a variety of hazard reports and decision documents are available to the organization. The HTS can also be used to present information to the SSG and other teams directly from the database.

14.5 CONCLUSION

System safety focuses on providing the foundation for designing safe systems around human capabilities and limitations rather than reacting to unacceptable situations. By

TABLE 14.7 Example Hazards Tracking Database

Unique Number This number should, if at all possible, be based on system that helps users determine with what part of system hazard is associated. By convention, hazard is assigned to originating subsystem. However, this may be difficult to determine because often hazards are related to interface of two or three subsystems. To which subsystem will the hazard be assigned? This example highlights the need for system safety engineering to coordinate its activities with systems engineering and design teams.

Hazard Topic This is a short phrase used to quickly differentiate hazard from other hazards in hazard list.

Hazard Description A hazard description is brief narrative of potential mishap attributable to the hazard having three elements that express the threat: a source, a mechanism, and an outcome.

Status Tracking record should state where hazard is in process of analysis and risk acceptance. Possible status list of codes could include

- Proposed
- Open
- Monitor
- Recommend closure
- Closed and verified
- Administratively closed

Tailor the list of status codes to level of complexity dictated by system. This could range from two or three status codes to dozen or more.

Risk Assessment Code This is code assigned showing the worst credible consequence of hazard and its probability.

Subsystem, Component, and Part Number If hazard is associated with specific subsystem, component, or part, there should be a field to enter that data.

Severity Include reasoning used to assign severity of risk assessment code.

Probability Include rationale used to assign probability of risk assessment code.

Special Considerations Track whether hazard involves radioactive material, explosives, munitions, health hazard, or involves system requirement.

Risk Reduction Alternatives List here all reasonable alternatives for risk elimination or reduction. By listing all alternatives, creativity of design engineers to find even better alternative is enhanced.

Recommendations List here mitigation measures recommended by system safety engineer or system safety group. Individually track these recommendations as part of system safety management system.

Consequences of Risk Acceptance List here costs of risk acceptance if no further risk reduction is funded. This should include how many deaths and serious injuries may occur over life cycle of system. What are financial costs in terms of damage or other forms of loss such as data loss or environmental impact?

Dates of Status Changes Tracking dates provides understanding of hazard history at glance.

System Description Short description of subsystem or components involved with hazard helps users of hazard tracking system understand how hazard fits into the system.

Sources and References List design standards, safety standards, safety analyses, requirements documents, and other related documents and references related to hazard.

Actions Track actions taken and decisions made related to hazard individually in database within system safety management system. These should be dated to provide history of hazard.

understanding system safety concepts, principles, and elements, managers transform system requirements into operational systems through a comprehensive, iterative technical management process. It is an activity that must be done throughout the entire life cycle of the system, from "cradle to grave," and is a concurrent approach to both product and process development. If safety personnel are involved early in the design concept, they will be better able to identify hazards, avoid risk, and develop reliable countermeasures to those hazards that cannot be eliminated. The earlier system safety efforts are funded in a program, the more cost effective those dollars will be in reducing the mishap risk of the system. In order to aid decision authorities, a listing of 101 techniques and methods used by safety personnel throughout the entire life cycle was presented in the chapter. In particular, system safety engineering deals with the tools of the trade, the principles and methodology of analyzing the hazards of system components, subsystems, and interfaces. Whereas, system safety management deals with how the decisions are made based on the analysis done by the system safety engineers in order to eliminate or reduce the associated mishap risk. Through interaction between engineering and management, hopefully an acceptable level of risk can be achieved within the constraints of operational effectiveness, time, and cost. In order for system safety to be effective, the integrated product team must agree on a system safety plan that will identify hazards, assess mishap risk, identify elimination and mitigation measures, verify mitigation effectiveness by reducing risk, accept residual risk, and track hazards though the life cycle.

NOTES

1. For acquisition work within the DoD, DoD (2001) 5000.2-R, paragraph C5.2.3.5.10.1 indicates, "All programs, regardless of acquisition category and throughout their life cycle, shall comply with this [the Environment, Safety, and Occupational Health (ESOH)] section. The PM [program manager] shall ensure a system design that can be tested, operated, maintained, repaired, and disposed of in accordance with ESOH statutes, regulations, policies, and, as applicable, environmental treaties and agreements (collectively termed regulatory requirements) and the requirements of this section." As such, paragraph C5.2.3.5.10.6.3 identifies that "Pub. L. 91-596 (1990) (reference (dddd)) [Public Law 91-h;596, "Occupational Safety and Health Act of 1970," as amended by Public Law 101-552, Section 3101, November 5, 1990] makes Federal Occupational Safety and Health Act standards and regulations applicable to all federal (military or civilian) and contractor employees working on DoD acquisition contracts or in DoD operations and workplaces. In the case of military-unique equipment, systems, operations, or workplaces, Federal safety and health standards, in whole or in part, shall apply to the extent practicable."
2. FAA Order 8040.4 (U.S. Department of Transportation, 1998) requires that "The FAA shall use a formal, disciplined, and documented decision making process to address safety risks in relation to high-consequence decisions impacting the complete product life cycle. The critical information resulting from a safety risk management process can thereby be effectively communicated in an objective and unbiased manner to decision makers, and from decision makers to the public. All decision making authorities within the FAA shall maintain safety risk management expertise appropriate to their operations, and shall perform and document the safety risk management process prior to issuing the high-consequence decision. The choice of methodologies to support risk management efforts remains the responsibility of each program office."
3. NASA (2000) NPG 8715.3 states, "This NASA Safety Manual is the central Agency document containing procedures and guidelines that define the NASA Safety Program. This document serves as a general framework to structure the more specific and detailed requirements for Headquarters, Program, and Center Directors."

REFERENCES

Air Force System Safety Handbook. (2000, July). Kirtland Air Force Base, NM: Air Force Safety Agency. Available: http://safety.Kirtland.af.mil/AFSC/ROBMS/Training/ssm-hndbk.pdf.

Alberico, D., Bozarth, J., Brown, M., Gill, J., Mattern, S., and McKinlay VI, A. (1999, December). *Software System Safety Handbook: A Technical & Managerial Team Approach*. Dahlgren, VA: Joint Services Computer Resources Management Group. Available: http://www.egginc.com/dahlgren/files/ssshandbook.pdf

Clemens, P. L. (2002). *System Safety Scrapbook* 9th ed. Tulahoma, TN: Jacobs Sverdrup. Available: http://www.sverdrup.com/safety/scrapbook.pdf.

Clemens, P. L., and Simmons, R. J. (1998). *System Safety and Risk Management*, NIOSH Publication 96-37768. Cincinnati, OH: National Institute for Occupational Safety and Health. Available: http://www.sverdrup.com/safety/riskmgt/riskmgt.shtml (retrieved July 16, 2002).

Dietz, T. R., Frey, S., and Rosa, E. (2002). Risk, Technology and Society. In R. E. Dunlap and W. Michelson (Eds.), *Handbook of Environmental Sociology* (pp. 562–629). Westport, CT: Greenwood.

Federal Aviation Administration. (2000, December). *System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management*. Washington DC: Department of Transportation. Available: http://www.asy.faa.gov/Risk/ (retrieved July 14, 2002).

Goetsch, D. L. (2002). *Occupational Safety and Health for Technologists, Engineers, and Managers*, 4th ed. Upper Saddle River, NJ: Prentice-Hall.

Kohn, J. P., Friend, M. A., and Winterberger, C. A. (1996). *Fundamentals of Occupational Safety and Health*. Rockville, MD: Government Institutes.

Li, T. S. (1999, December). *Principles of Risk Management*. Hong Kong: Hong Kong University of Science and Technology. Available: http://www.ab.ust.hk/sepo/esst/Riskmgt-notes.pdf (retrieved June 26, 2002).

Malasky, S. W. (1982). *System Safety: Technology and Application.* New York: Garland STMP.

National Aeronautics and Space Administration. (2000 January). *NASA Safety Manual*, NPG 8715.3. Washington, DC: National Aeronautics and Space Administration.

National Aeronautics and Space Administration. (2002, June 26). *NASA Guidebook for Safety Critical Software—Analysis and Development*, NASA-GB-1740.13-96. Available: http://swg.jpl.nasa.gov/resources.

National Safety Council. (2002, June). *About the Council*. Available: http://www.nsc.org/insidensc.htm.

Occupational Safety and Health Administration. *Overview of Occupational Safety and Health/Industrial Hygiene*. Available: http://www.osha-slc.gov/SLTC/smallbusiness/sec5.html.

Roland, H. E., and Moriarty, B. (1990). *System Safety Engineering and Management*, 2nd ed. New York: Wiley Interscience.

Stephans, R. A., and Talso, W. W. (Eds.). (1997). *System Safety Analysis Handbook*, 2nd ed. Albuquerque, MN: System Safety Society.

U.S. Army. (1990, June). *System Safety Management Guide*, Pamphlet 385-16. Washington, DC: Department of the Army.

U.S. Coast Guard. (2001). *Risk-Based Decision-Making Guidelines*, 2nd ed. Washington, DC: U.S. Coast Guard. Available: http://www.uscg.mil/hq/g-m/risk/e-guidelines/html/index.htm.

U.S. Department of Defense. (DOD) (1993). *System Safety Program Requirements*, MIL-STD 882C. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense. (DOD) (2000, February). *Standard Practice for System Safety*, MIL-STD 882D. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense. (DOD) (2001, June). *Mandatory Procedures For Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*, DOD 5000.2-R. Washington, DC: U.S. Department of Defense.

U.S. Department of Energy (DOE). (1997, September). *Hazard Categorization and Accident Analysis Techniques for compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, DOE-STD-1027-92, Change Notice 1. Washington, DC: U.S. Department of Energy.

U.S. Department of Transportation (DOT). (1998, June). *Safety Risk Management*, FAA Order 8040.4. Washington, DC: U.S. Department of Transportation.

Walker, D. A. (2000, May). *Field Demonstration Workshop on Performance-Based Inspection of Vessels Entering The St. Lawrence Seaway (Establishing Specific Inspection Plans)*, LR-101-11.3-1B-94. Washington DC: U.S. Coast Guard. Available: http://www.uscg.mil/hq/g-m/risk/e-guidelines/html/vol4/Volume4/Tool-spec_Rec/Failure%20Modes%20and%20Effects%20Analysis%20(FMEA)/FMEA.Htm.

RELATED READINGS

Bahr, N. J. (1997). *System Safety Engineering and Risk Assessment: A Practical Approach*. Philadelphia, PA: Taylor and Francis.

Brauer, R. L. (1994). *Safety and Health for Engineers*. New York: Wiley.

Briscoe, G. J. (1997, June). *Risk Management Guide*, SSDC-11. Idaho Falls, ID: EG&G Idaho.

Clark, R., Benner, L., and White, L. M. (1987, March). *Risk Assessment Techniques Manual*. Oklahoma City, OK: Transportation Safety Institute.

Grose, V. L. (1987). *Managing Risk: Systematic Loss Prevention for Executives*, Arlington , VA: Omega Systems Group.

Kije, L. T. (1963). *Residual Risk*. Rusee.

Layton, D. M. (1989). *Systems Safety Including DOD Standards*, Weber Systems.

Leveson, N. G. (1995). *SAFEWARE: System Safety and Computers, a Guide to Preventing Accidents and Losses Caused by Technology*. Reading, MA: Addison-Wesley.

Rodgers, W. P. (1971). *Introduction to System Safety Engineering*, New York: Wiley.

Saaty, T. L. (1996). *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, 2nd ed. Pittsburgh, PA: RWS Publications.

Society of Automotive Engineers (SAE). (1996a). *Certification Considerations for Highly Integrated or Complex Aircraft Systems*, Aerospace Recommended Practice 4754. Warrendale, PA: SAE.

Society of Automotive Engineers (SAE). (1996b). *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, Aerospace Recommended Practice 4761. Warrendale, PA: SAE.

Stephenson, J. (1991). *System Safety 2000, a Practical Guide for Planning, Managing, and Conducting System Safety Programs*, New York Van Nostrand Reinhold.

Tarrants, W. E. (1980). *The Measurement of Safety Performance*, New York Garland STPM.

Vincoli, J. W. (1993). *Basic Guide to System Safety*, New York Van Nostrand Reinhold.