Chapter 1

System Safety and Hazard Analysis

1.1 INTRODUCTION

We live in a world comprised of systems. When viewed from an engineering perspective, most aspects of life involve systems. For example, houses are a type of system, automobiles are a type of system, and electrical power grids are another type of system. Commercial aircraft are systems that operate within a larger transportation system that in turn operate in a larger worldwide airspace system. Systems have become a necessity for modern living.

As a result of living in a system-centric world, we also live in a world comprised of hazards and risk. With systems and technology also comes exposure to hazards and potential mishaps. A hazard is a potential condition existing within a system, which when actuated becomes an actual mishap event resulting in damage, loss, injury, and/or deaths. Risk is the probability that a hazard occurs accompanied by the severity of the resulting outcome.

Hazard risk is a metric that predicts the likelihood and severity of a possible mishap. We live with risk, and make risk decisions, on a daily basis. For example, there is the hazard that a traffic light will fail, resulting in the mishap of another auto colliding with your auto. Automobiles, traffic, and traffic lights form a unique system that we use daily and accept the hazard risk potential because the risk is small. There is the danger that the gas furnace in our house will fail and explode, thereby resulting in the mishap of a burned house, or worse. This is another unique system, with known adverse side effects that we choose to live with because the mishap risk is small and the benefits are great. We live in a world comprised of many different systems with many different risks.

Our lives are intertwined within a web of different systems, each of which can affect our safety. Each of these systems has a unique design and a unique set of components. In addition, each of these systems contains inherent hazards that present unique mishap risks. We are

Hazard Analysis Techniques for System Safety, Second Edition. Clifton A Ericson, II.

always making a tradeoff between accepting the benefits of a system and the mishap risk they present. As we develop and build systems, we should be concerned about eliminating and reducing mishap risk. Some risks are so small that they can easily be accepted, while other risks are so large that they must be dealt with immediately. Risks are akin to the invisible radio signals that fill the air around us, in that some are loud and clear, some very faint, and some are distorted and unclear. Life, as well as safety, is a matter of knowing, understanding, and choosing the risk to accept.

System safety is the formal engineering discipline and process for identifying and controlling hazards, and the risk associated with these hazards. As systems become more complex and more hazardous, more effort is required to understand and manage system mishap risk. Hazard (and mishap) risk can be intentionally reduced and controlled to a small and acceptable level through the system safety process.

The key to system safety and effective risk management is the identification and mitigation of hazards. To successfully control hazards, it is necessary to understand hazards and know how to identify them. The purpose of this book is to better understand hazards and the tools and techniques for identifying them, in order that they can be effectively controlled during the development of a system. The system safety process is sometimes referred to as *design for safety* (DFS).

1.2 THE NEED FOR HAZARD ANALYSIS

Forensic engineering is the detailed investigation of a mishap after it has occurred, performed to determine the specific causes for the mishap in order that corrective action can be applied to prevent reoccurrences. System safety, on the other hand, is a form of preemptive forensic engineering, whereby potential mishaps are identified, evaluated, and controlled before they occur. Potential mishaps and their causal factors are anticipated and identified during the design stage, and then design safety features are incorporated into the design to control the occurrence of the potential mishaps – safety is intentionally designed in and mishaps are effectively designed out. This proactive approach to safety involves hazard analysis, risk assessment, risk mitigation through design, and testing to verify the design results. Potential mishaps are recognized and identified by the hazards that ultimately cause them. System safety is a proactive approach to affecting the future (i.e., preventing mishaps before they occur) by identifying hazards and then eliminating or controlling the risk they present.

Systems are intended to improve our way of life, yet they also contain the inherent capability to spawn many different hazards that present us with mishap risk. It is not that systems are intrinsically bad; it is that systems can go awry, and when they go awry they typically result in mishaps. System safety is about determining how systems can go bad and implementing design safety mitigations to eliminate, correct, or work around safety imperfections in the system.

Murphy's law states that "if anything can go wrong, it will." This truism illustrates that the unexpected and undesired must be anticipated and controlled in order to prevent mishaps, and this can be achieved only through the system safety process. Hazards and risk often cannot be eliminated; however, hazards and risk can be anticipated and mitigated via safety design features, thereby preventing or reducing the likelihood of mishaps. If system safety is not applied, accidents and loss of life will not be prevented. System users are typically not aware of the actual risk they are exposed to, and without system safety this risk may be much higher than the users realize.

Hazard analysis is the basic key component of the system safety process. Therefore, it is necessary to fully understand the hazard theory and the hazard analysis process in order to develop safe systems.

1.3 SYSTEM SAFETY BACKGROUND

The primary guidance document for system safety is MIL-STD-882, System Safety Standard Practice. Version E was released on May 11, 2012. This standard has been in existence since 1969; its predecessor MIL-S-38130 was released in 1963.

MIL-STD-882 and its predecessor MIL-S-38130 are the genesis of system safety. The US military, along with US aerospace companies, saw the need for a holistic and proactive "systems" approach for the design, development, test, and manufacture of "safe" systems. Working together, these two groups developed the system safety methodology and discipline. MIL-S-38130 was originally released on September 30, 1963 and replaced by MIL-STD-882 on July 15, 1969. System safety was actually documented as a process prior to any formal documentation of the systems engineering discipline. System safety as a formal discipline was originally developed and promulgated by the military-industrial complex to prevent aircraft and missile mishaps that were costing lives, dollars, and equipment loss. As the effectiveness of the discipline was observed by other industries, it was adopted and applied to these industries and technology fields, such as commercial aircraft, nuclear power, chemical processing, rail transportation, the FAA, and NASA, to name a few.

The ideal objective of system safety is to develop a system free of hazards. However, absolute safety is not possible because complete freedom from all hazardous conditions is not always possible, particularly when dealing with complex inherently hazardous systems, such as weapon systems, nuclear power plants, commercial aircraft, etc.

Since it is generally not possible to eliminate all hazards, the realistic objective becomes that of developing a system with acceptable mishap risk. This is accomplished by identifying potential hazards, assessing their risks, and implementing corrective actions to eliminate or mitigate the identified hazards. This involves a systematic approach to the management of mishap risk. Safety is a basic part of the risk management process.

Hazards will always exist, but their risk can and must be made acceptable. Therefore, safety is a relative term that implies a level of risk that is measurable and acceptable. System safety is not an absolute quantity, but rather an optimized level of mishap risk management that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated and the level of risk accepted or rejected by an appropriate decision authority. Mishap risk management is the basic process of system safety engineering and management functions. System safety is a process of disciplines and controls employed from the initial system design concepts, through detailed design and testing to system disposal at the completion of its useful life (i.e. "cradle to grave" or "womb to tomb").

The fundamental objective of system safety is to identify, eliminate or control, and document system hazards. System safety encompasses all the ideals of mishap risk management and design for safety; it is a discipline for hazard identification and control to an acceptable level of risk. Safety is a system attribute that must be intentionally designed into a product.

From a historical perspective, it has been learned that a proactive preventive approach to safety during system design and development is much more cost-effective than trying to add safety to a system after the occurrence of an accident or mishap. System safety is an initial investment that saves future losses that could result from potential mishaps.

1.4 SYSTEM SAFETY OVERVIEW

System safety is effectively a design-for-safety process, discipline, and culture. DFS means that the design process utilizes the system safety process to intentionally design-in safety. This process anticipates potential safety problems (i.e., hazards) and eliminates them or reduces the risk they present. Safety risk is calculated from the identified hazards, and risk is eliminated or reduced by eliminating or mitigating the appropriate hazard causal factors. System safety, by necessity, considers function, criticality, risk, performance, and cost parameters of the system. Risk mitigation is achieved through a combination of design mechanisms, design features, warning devices, safety procedures, and safety training to counter the effect of hazard causal factors.

System safety involves a systems approach, which accounts for the distinctive name. System safety is the art and science of looking at all aspects and characteristics of a system as an integrated whole, rather than looking at individual components in isolation from the system. System safety is a holistic approach that considers the subject as an integrated sum-of-the-parts combination, rather than a piecemeal approach of looking at separate individual and solitary pieces of the system.

Often, system safety is not fully appreciated for the contribution it can make to creating safe systems that present a minimal chance of deaths and serious injuries. System safety applies a planned and disciplined methodology for purposely designing safety into a system. A system can be made safe only when the system safety methodology is consistently and properly applied. Safety is more than eliminating hardware failure modes; it involves designing the safe system interaction of hardware, software, humans, procedures, and the environment, under all normal and adverse failure conditions. Safety must consider the entirety of the problem, not just a portion of the problem, that is, a systems perspective is required for full safety coverage. System safety anticipates potential problems and either eliminates them or reduces their risk potential, through the use of design safety mechanisms applied according to a safety order of precedence.

System safety is the process of managing the system, personnel, environmental, and health mishap risks encountered in the design development, test, production, use, and disposal of systems, subsystems, equipment, materials, and facilities.

A system safety program (SSP) is a formal approach to eliminate hazards through engineering, design, education, management policy, and supervisory control of conditions and practices. It ensures the accomplishment of the appropriate system safety management and engineering tasks. The formal system safety process has been primarily established by the US Department of Defense (DoD) and its military branches and promulgated by MIL-STD-882. However, the same process is also followed in private industry for the development of commercial products, such as commercial aircraft, rail transportation, nuclear power, and automobiles, to mention a few.

The goal of system safety is the protection of life, systems, equipment, and the environment. The basic objective is the elimination of hazards that can result in death, injury, system loss, and damage to the environment. When hazard elimination is not possible, the next objective is to reduce the risk of a mishap through design control measures. Reducing mishap risk is achieved by reducing the probability of the mishap and/or the severity of the mishap.

This objective can be attained at minimum cost when the SSP is implemented early in the conceptual phase and is continued throughout the system development and acquisition cycle. The overall complexity of today's systems, particularly weapon systems, is such that system

safety is required in order to consciously prevent mishaps and accidents. Added to complexity is the inherent danger of energetic materials, the effects of environments, and the complexities of operational requirements. In addition, consideration must be given to hardware failures, human error, software interfaces, including programming errors, and vagaries of the environment.

The following definitions from MIL-STD-882E help define the system safety concept:

System Safety The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life cycle.

System Safety Engineering An engineering discipline that employs specialized knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.

System Safety Management All plans and actions taken to identify hazards; assess and mitigate associated risks; and track, control, accept, and document risks encountered in the design, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and infrastructure.

The intent of system safety is mishap risk management through hazard identification and mitigation techniques. System safety engineering is an element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of those actions necessary to prevent or control hazards within the system. It draws upon professional knowledge and specialized skills in the mathematical and scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, evaluate, and document the safety of the system.

System safety management is an element of program management that ensures accomplishment of the correct mix of system safety tasks. This includes identification of system safety requirements; planning, organizing, and controlling those efforts that are directed toward achieving the safety goals; coordinating with other program elements; and analyzing, reviewing, and evaluating the program to ensure effective and timely realization of the system safety objectives.

The basic concept of system safety is that it is a formal process of intentionally designing-in safety by designing-out hazards or reducing the mishap risk of hazards. It is a proactive process performed throughout the system life cycle to save lives and resources by intentionally reducing the likelihood of mishaps to an insignificant level. The system life cycle is typically defined as the stages of concept, preliminary design, detailed design, test, manufacture, operation, and disposal (demilitarization). In order to be proactive, safety must begin when system development first begins at the conceptual stage.

The goal of system safety is to ensure the detection of hazards to the fullest extent possible, and provide for the introduction of protective measures early enough in system development to avoid design changes late in the program. A safe design is a prerequisite for safe operations. Things that can go wrong with systems are predictable, and something that is predictable is also preventable. As Murphy's law states "whatever can go wrong, will go wrong," the goal of system safety is to find out what can go wrong (before it does) and establish controls to prevent it or reduce the probability of occurrence. This is accomplished through hazard identification and mitigation.

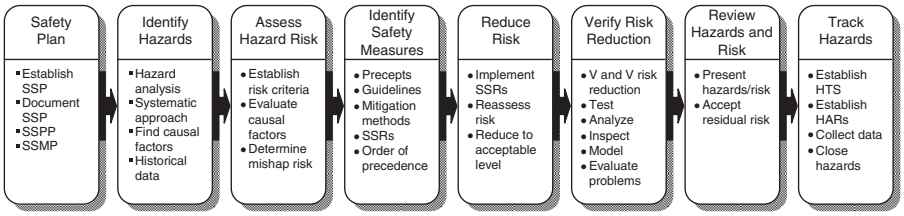

Figure 1.1 *Core system safety process.*

1.5 SYSTEM SAFETY PROCESS

MIL-STD-882 establishes the core system safety process in eight principal steps, which are shown in Figure 1.1.

The core system safety process involves establishing an SSP to implement the mishap risk management process. The SSP is formally documented in the system safety program plan (SSPP), which specifies all of the safety tasks that will be performed, including the specific hazard analyses, reports, etc. As hazards are identified, their risk will be assessed, and hazard mitigation methods will be established to mitigate the risk as determined necessary. Hazard mitigation methods are implemented into system design via system safety requirements (SSRs). All identified hazards are converted into hazard action records (HARs) and placed into a hazard tracking system (HTS). Hazards are continually tracked in the HTS until they can be closed.

It can be seen from the core system safety process that safety revolves around hazards. Hazard identification and elimination/mitigation is the key to this process. Therefore, it is critical that the system safety analyst understands hazards, hazard identification, and hazard mitigation.

The core system safety process can be reduced to the process shown in Figure 1.2. This is a mishap risk management process whereby safety is achieved through the identification of hazards, the assessment of hazard mishap risk, and the control of hazards presenting unacceptable risk. This is a closed loop process, whereby hazards are identified and tracked until acceptable closure action is implemented and verified. It should be performed in conjunction with actual system development, in order that the design can be influenced during the design process, rather than trying to enforce design changes after the system is developed.

System safety involves a life cycle approach, based on the idea that mishap and accident prevention measures must be initiated as early as possible in the life of a system and carried through to the end of its useful life. It is usually much cheaper and more effective to design

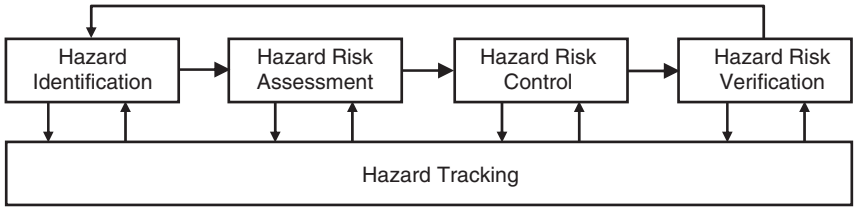

Figure 1.2 *Closed loop hazard control process.*

safety features into an item of equipment than it is to add the safety features when the item is in production or in the field. Also, experience indicates that some of the hazards in a newly designed system will escape detection, no matter how aggressive the safety program. Therefore, the safety program for a system must remain active throughout the life of the system to ensure that safety problems are recognized whenever they arise and that appropriate corrective action is taken.

The key to system safety is the management of hazards. To effectively manage hazards, one must understand hazard theory and the identification of hazards. The purpose of this book is to better understand hazards and the tools and techniques for identifying them. When hazards are identified and understood, they can then be properly eliminated or mitigated.

1.6 SYSTEM SAFETY STANDARDS

System safety is a process that is formally recognized internationally and used to develop safe systems in many countries throughout the world. MIL-STD-882 has long been the bedrock of system safety procedures and processes, and the discipline has grown and improved with each improvement in MIL-STD-882. Since the advent of MIL-STD-882, many other agencies, organizations, and standards groups have developed their own variation on the system safety process. These agencies have recognized that the system safety process is successful in making systems safe and they have tailored the methodology to reflect their particular industry.

Key reference standards and guideline documents that help define the system safety process and methodology include the following:

1. MIL-STD-882E, System Safety Standard Practice, May 11, 2012.
2. ANSI/GEIA-STD-0010-2009, Standard Best Practices for System Safety Program Development and Execution, February 12, 2009.
3. NAVSEA SWO20-AH-SAF-010, Weapon System Safety Guidelines Handbook, February 1, 2006.
4. *System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management*, Federal Aviation Administration (FAA), December 30, 2000.
5. NPR 8715.3, NASA General Safety Program Requirements, March 12, 2008.
6. *Air Force System Safety Handbook*, July 2000.
7. MIL-HDBK-764, System Safety Engineering Design Guide for Army Materiel, January 12, 1990.
8. SAE/ARP-4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, Aerospace Recommended Practice, 1996.
9. SAE/ARP-4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.

1.7 SYSTEM SAFETY PRINCIPLES

The following are a set of system safety principles; note that they all relate to hazards, hazard identification, and hazard mitigation, demonstrating the importance of hazard analysis:

Principle 1 Hazards, mishaps, and risk are a reality of life; they are typically the by-product of man-made systems.

Principle 2 Hazards are the *thing* that create risk and lead to mishaps. This thing, or entity, is a unique built-in design element that can be identified and controlled through design.

Principle 3 Systems can, and will, fail in various different key modes that often initiate or contribute to system hazards.

Principle 4 Safety is a resultant systems property, which changes with system design changes. This property is intentionally improved with design-for-safety activities.

Principle 5 Hazard risk is the metric that provides a measure of the safety property.

Principle 6 Risk should always be known; unnecessary or unacceptable safety risk should never be accepted.

Principle 7 System safety is the process for identifying and controlling hazards, mishaps, and risk. Safety is achieved through the hazard identification and hazard mitigation process.

Principle 8 Hazards are identified, and risk determined, from hazard analysis.

Principle 9 Safety is best achieved through a dedicated system safety program based on hazard analysis and risk control.

Principle 10 Safety is not free, but it costs less than the direct, indirect, and hidden costs associated with mishaps.

Principle 11 An absence of mishaps does not necessarily equate to a safe system. There could be hidden hazards that have not yet occurred; this is why hazard analysis should always be performed.

Principle 12 Safety must be earned; it does not happen by accident. This requires a system safety program based on hazard analysis and hazard mitigation.

1.8 KEY TERMS

For purposes of clarity and understanding, some key safety terms used throughout this book are defined as follows:

Safety-Significant	A term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related.
Safety-Related (SR)	A term applied to a condition, function, event, operation, process, or item whose mishap severity consequence is either Marginal or Negligible (see HRI criteria).
Safety-Critical (SC)	A term applied to a condition, function, event, operation, process, or item whose mishap severity consequence is either Catastrophic or Critical (see HRI criteria). SC is a term indicating a high consequence or high risk safety concern.
Safety-Critical Item (SCI)	SCI is a designation given to any item that has been identified as being safety-critical or part of a safety-critical function. Safety-critical items can be any system level of hardware, software or human tasks involving an event, operation, process, or procedure

	that is safety-critical. SCIs can be (but are not limited to) functions, requirements, paths, tasks, procedures, components or component tolerances.
Safety-Critical Function (SCF)	A term applied to any function involved in a hazard whose mishap severity consequence is either Catastrophic or Critical (see HRI criteria).

1.9 SUMMARY

This chapter discussed the basic concept of system safety. The following are the basic principles that help summarize the discussion in this chapter:

1. The goal of system safety is to save lives and preserve resources by preventing mishaps.
2. Mishaps can be predicted and controlled through the system safety process.
3. The focus of system safety is on hazards, mishaps, and mishap risk.
4. Hazard analysis is essential because hazards are the key to preventing or mitigating hazards.
5. System safety should be consistent with mission requirements, cost, and schedule.
6. System safety covers all system life cycle phases, from "cradle to grave."
7. System safety must be planned, proactive, integrated, comprehensive, and system oriented.
8. The system safety process contains eight core steps, all based on hazard analysis:
   a. Plan
   b. Hazard identification
   c. Risk assessment
   d. Identify hazard mitigation methods
   e. Reduce risk with mitigation methods
   f. Verify risk reduction
   g. Accept residual risk
   h. Track hazards through system lifecycle