# 1

# System Safety

An Overview

## Background

The idea or concept of *system safety* can be traced to the missile production industry in the late 1940s. It was further defined as a separate discipline by the late 1950s (Moriarty and Roland 1983) and early 1960s, used primarily by the missile, aviation, and aerospace communities. Prior to the 1940s, system designers and engineers relied predominantly on a trial-and-error method of achieving safe design. This approach was somewhat successful in an era when system complexity was relatively simple compared with those of subsequent development. For example, in the early days of the aviation industry, this process was often referred to as the *fly-fix-fly* approach to design problems (Moriarty and Roland 1983; Stephenson 1991) or, more accurately, *safety-by-accident*. Simply stated, an aircraft was designed based upon the existing or known technology. It was then flown until problems developed or, in the worst case, it crashed (Figure 1.1). If design errors were determined as the cause (as opposed to human, or "pilot" error), then the design problems would be fixed and the aircraft would fly again. Obviously, this method of after-the-fact design safety worked well when aircraft flew low and slow and were constructed of wood, wire, and cloth. However, as systems grew more complex and aircraft capabilities such as airspeed and maneuverability increased, so did the likelihood of devastating results from a failure of the system or one of its many subtle interfaces. This is clearly demonstrated in the early days of the aerospace era (the 1950s and 1960s). As the industry began to develop jet-powered aircraft and space and missile systems, it quickly became clear that engineers could no longer wait for problems to develop; they had to anticipate them and "fix" them before they occurred. To put it another way: the "fly-fix-fly" philosophy was no longer

*Basic Guide to System Safety*, Fourth Edition. Jeffrey W. Vincoli.

**Figure 1.1** The "fly-fix-fly" approach, or more accurately "safety-by-accident," focused on fixing design issues after an accident event rather than focusing on accident prevention through design (*Source:* United States Air Force / Wikimedia Commons / Public Domain).

feasible. Elements such as these became the catalyst for the development of *systems engineering*, out of which eventually grew the concept of *system safety*. The need to anticipate and fix problems before they occurred led to a new approach – a consideration of the design as a "system." This means that all aspects of the design of operation (e.g., machine, operator, and environment), must be considered in identifying potential hazards and establishing appropriate controls. Another important part of this "systems" approach to safety is the realization that resources for safety are limited and there must be some logical, reasoned way to apply resources to the most serious potential problems. Systems safety provides this capability. Figure 1.2 shows a simplification of the basic elements of the systems engineering process. It is noted that safety comprises only one part of this integrated engineering design approach (Larson and Hann 1990). Taken one step further, Figure 1.3 demonstrates how the systems approach associated with the initial element of the systems safety engineering process – the design aspect – can support the identification of hazards in the earliest phases of a project life cycle. Only after the accurate identification of hazards has been accomplished, can proper elimination or control measures be determined.

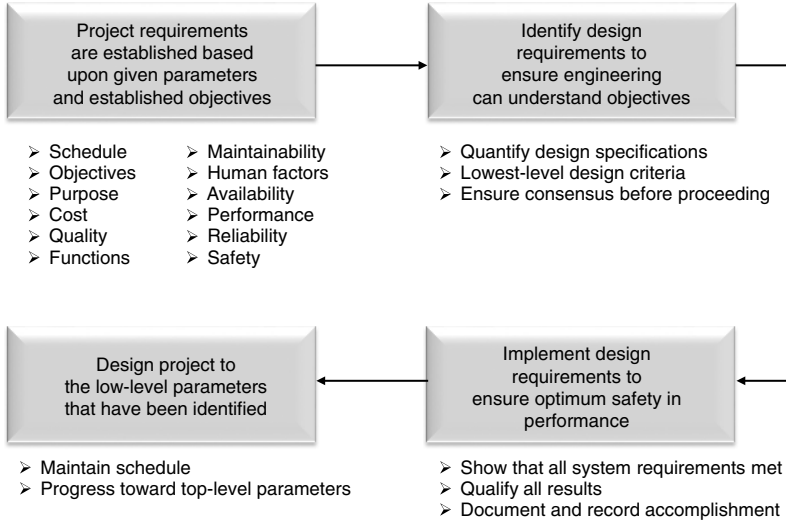


**Figure 1.2** The system safety engineering process (*Source:* Larson and Hann 1990/American Society of Safety Engineers).

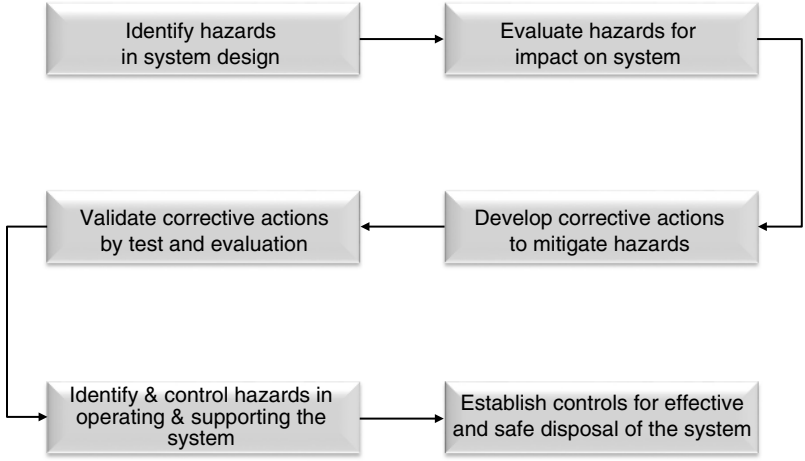


**Figure 1.3** The systems approach to the consideration of safety from the design phase through product disposal or project termination.

The dawn of the manned spaceflight program in the mid-1950s also contributed to the growing necessity for safer system design. Hence, the growing missile and space systems programs became a driving force in the development of system safety engineering. Those systems under

development in the 1950s and early 1960s required a new approach to controlling hazards such as those associated with weapon and space systems (e.g., explosive components and pyrotechnics, unstable propellant systems, and extremely sensitive electronics). The Minuteman Intercontinental Ballistic Missile (ICBM) was one of the first systems to have had a formal, disciplined, and defined system safety program (Moriarty and Roland 1983). In July of 1969, the U.S. Department of Defense (DOD) formalized system safety requirements by publishing MIL-STD-882 entitled "System Safety Program Requirements." This Standard has since undergone a number of revisions.

The U.S. National Aeronautics and Space Administration (NASA) soon recognized the need for system safety and has since made extensive system safety programs an integral part of space program activities. The early years of our nation's space launch programs are full of catastrophic and quite dramatic examples of failures. During those developing years, it was a known and quite often stated fact that *our missiles and rockets just don't work, they blow up*. The many successes since those days can be credited in large part to the successful implementation and utilization of a comprehensive system safety program. However, it should be noted that the Challenger disaster in January 1986 and the loss of the orbiter Columbia upon reentry in February of 2003 stand as historic reminders to us all that, no matter how exact and comprehensive a design or operating safety program is considered to be, the proper *management* of that system is still one of the most important elements of success. This fundamental principle is true in any industry or discipline.

Eventually, the programs pioneered by the military and NASA were adopted by industry in such areas as nuclear power, refining, mass transportation, chemicals, healthcare, and computer programming.

Today, the system safety process is still used extensively by the various military organizations within the DOD, as well as by many other federal agencies in the United States such as NASA, the Federal Aviation Administration, and the Department of Energy. In most cases, it is a required element of primary concern in the federal agency contract acquisition process.

Although it would not be possible to fully discuss the basic elements of system safety without comment and reference to its military/federal connections, the primary focus of this text shall be placed upon the advantages of utilizing system safety concepts and techniques as they apply to the general safety arena. In fact, the industrial workplace can be viewed as a natural extension of the past growth experience of the system safety discipline. Many of the safety rules, regulations, statutes, and basic safety

operating criteria practiced daily in the industry today are, for the most part, the direct result of a real or perceived need for such control doctrine. The requirement for safety controls (written or physical) developed either because a failure occurred, or someone with enough foresight anticipated a possible failure and implemented controls to avoid such an occurrence. Even though the former example is usually the case, the latter is also responsible for the development of countless safe operating requirements practiced in the industry today. Both, however, are also the basis upon which system safety engineers operate.

The first method, creating safety rules *after* a failure or accident, is likened to the *fly-fix-fly* approach discussed earlier. The second method, anticipating a potential failure and attempting to avoid it with control procedures, regulations, etc., is exactly what the system safety practitioner does when analyzing system design or an operating condition or method. However, when possible or practical, the system safety concept goes a step further and actually attempts to engineer the risk of hazard(s) out of the process. With the introduction of the system safety discipline, the *fly-fix-fly* approach to safe and reliable systems was transformed into the *identify, analyze, and eliminate* (Abendroth and Grass 1987) method of system safety assurance.

We have established the basic connection between the system safety discipline and its relationship to the general industry occupational safety practice. This conceptual relationship will be examined in more detail throughout this text.

## The Difference Between Industrial Safety and System Safety (Leveson 2005)

Industrial safety, or occupational safety, has historically focused primarily on controlling injuries to employees on the job. The industrial safety engineer usually is dealing with a fixed manufacturing design and hazards that have existed for a long time, many of which are accepted as necessary for operations. Traditionally, more emphasis is often placed on training employees to work within this environment rather than on removing the hazards.

To perform their charter, industrial safety engineers collect data during the operational life of the system and attempt to eliminate or control unacceptable hazards where possible or practical. When accidents occur, they are investigated and action is taken to reduce the likelihood of a recurrence – either by changing the plant or by changing employee work rules and

training. The hazards associated with high-energy or dangerous processes are usually controlled by either

- Disturbance control algorithms implemented by operators or an automated control system or
- Transferring the plant to a safe state using a separate protection system.

Safety reviews and compliance audits are conducted by industrial safety organizations within a company or, less frequently, by safety committees to ensure unsafe conditions in the workplace are corrected and employees are following the work rules specified in manuals, directives, and operating instructions. Lessons learned from accidents are incorporated into design standards, and much of the emphasis in the design of new plants and work rules is on implementing these standards. Often, the standards are enforced by the government through occupational safety and health legislation.

In contrast, system safety has been traditionally concerned primarily with new systems. The concept of "loss" is treated much more broadly as relevant losses may include

- Injury to nonemployees;
- Damage to equipment, property, or the environment;
- Loss of mission.

As has been previously established, instead of making changes as a result of operational experience with the system, system safety attempts to identify potential hazards before the system is designed, to define and incorporate safety design criteria, and to build safety into the design before the system becomes operational. Although standards are used in system safety, they usually are "process standards" rather than "product standards" as reliance on design or product standards is often inadequate for new types of systems, and more emphasis is placed on upfront analysis and designing for safety. There have been attempts to incorporate system safety techniques and approaches into traditional industrial safety programs, especially when new plants and processes are being built. Although system safety techniques are considered "overkill" for many industrial safety problems, larger organizations and increasingly dangerous processes have raised concern about injuries to people outside the workplace (e.g., pollution and exposures to chemical release) and have therefore made system safety approaches more relevant. Furthermore, with the increase in size and cost of plant equipment, changes and retrofits to increase safety are costly and may require discontinuing operations for a period of time. Similarly, it is interesting to note that system safety is increasingly considering issues that have been traditionally thought to be strictly industrial safety concerns.

In summary, industrial safety activities are designed to protect workers in an industrial environment with extensive standards imposed by federal codes or regulations to provide for a safe workplace. However, with few exceptions, these codes seldom apply to protection of the product being manufactured. With the increasingly more frequent use of robotics and artificial intelligence (AI) in the workplace environment and with long-lived engineering programs like space launch vehicles that have substantial and continuing complex engineering design activities, the traditional concerns of industrial safety and system safety have become more intertwined (Leveson 2005).

In 2011, these circumstances led to the development of a new American National Standards Institute/American Society of Safety Engineers (ANSI/ASSE) Standard titled *Prevention Through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes* (ANSI/ASSE Z590.3-2011). This ANSI/ASSE Standard and its relationship to the objectives of this *Basic Guide to System Safety* will be discussed further in Chapter 4 and its utility in the prevention of accidents will be the focus of Chapter 16. It is noted that ASSE is now ASSP (American Society of Safety Professionals).

## System Safety and the Assessment of Risk

The idea, concept, or process of system safety has been defined in many ways, by a wide variety of scientific and technical professionals. However, since its inception, system safety has had the specific, driving purpose to eliminate system faults or failure risk and subsequent recognized accident and/or hazard potential through the design and implementation of engineering controls. Basically, system safety can be defined as

> *a sub-discipline of systems engineering that applies scientific, engineering and management principles to ensure adequate safety, the timely identification of hazard risk, and initiation of actions to prevent or control those hazards throughout the life cycle and within the constraints of operational effectiveness, time, and cost* (Stephenson 1991).

In the simplest of terms, system safety uses systems theory and systems engineering approaches to prevent foreseeable accident events and to minimize the result of unforeseen events. Losses in general (not just human death or injury) are considered and can include destruction of property, loss of mission, and/or harm to the environment (Leveson 2005). The term *safety*, as used here, is somewhat relative. Although "safety" has often been

traditionally defined in many sources as ... *freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property* (MIL-STD-882), it is generally recognized in the profession that this definition is somewhat unrealistic (Leveson 1986). This definition would indicate that *any* system containing some degree of risk is considered *unsafe*. Obviously, this is not practically logical since almost any system that produces some level of personal, social, technological, scientific, or industrial benefit contains an indispensable element of risk (Browning 1980). For example, safety razors or safety matches are not entirely *safe*, only *safer* than their alternatives. They present an acceptable level of risk while preserving the benefits of the less safe devices that they have replaced (Leveson 1986). A more vivid example of risk reduction and acceptance involves the sport of skydiving: Most sane skydivers would never jump out of an airplane without a parachute. The parachute provides a *control measure* intended to eliminate some level of risk. However, even with the parachute strapped in place, the jumper is still accepting the risk of parachute failure. System safety is concerned with the aspect of reducing the risk(s) associated with a hazard to its lowest acceptable level. In reality, no aircraft could fly, no automobile move, and no ship could be put out to sea if *all* hazards and *all* risks had to be completely eliminated first (Hammer 1972). Similarly, no drill press could be operated, forklift driven, petroleum refined, dinner cooked, microwave used, water boiled, etc., without some element of operating risk.

This problem is further complicated by the fact that attempts to eliminate risk result instead in the often unfortunate displacement of risk (Malasky 1982). For example, some preservatives approved by the U.S. Food and Drug Administration currently utilized in the food processing industry to prevent bacteria growth and spoilage are, themselves, a suspected cause of cancer (e.g., sodium nitrates). Likewise, there is a risk trade-off between the known benefits of improved medical diagnosis and treatment which result from the use of radiation (e.g., X-rays and radiation therapy), against the known risks of human exposure to radiation. Hence, safety is really more of a relative issue in that nothing is *completely* safe under *all* circumstances or *all* conditions. There is always some example in which a relatively safe material or piece of equipment can become hazardous. The very act of drinking water, if done to excess, can cause severe renal problems in most cases (Gloss and Wardel 1984).

Unfortunately, the question *How safe is safe enough?* has no simple answer. For example: It is not uncommon to hear the term *99.9% risk-free* used to signify high-assurance or low-risk assessments, especially in the advertising industry. In fact, it would be safe to say that this terminology is

somewhat over-used in our society. However, consider the following statistical facts (Larson and Hann 1990):

In the United States, 99.9% safe would mean

- one hour of unsafe drinking water per month;
- 20,000 children/per year suffering from seizures or convulsions due to faulty whooping cough vaccinations;
- 16,000 pieces of mail lost per hour;
- 500 incorrect surgical operations each week;
- 50 newborns dropped by doctors each day.

Clearly, a 99.9% assurance level is not really "safe enough" in today's society. If the percentage were increased by a factor of 10 to "99.99%," the following information indicates that even this level of risk is still unacceptable in certain instances. A 99.99% risk-free assurance level would mean

- 2000 incorrect drug prescriptions per year;
- 370,000 checks deducted from the wrong account per week;
- 3200 times per year, your heart would fail to beat;
- 5 children sustaining permanent brain damage per year because of faulty whooping cough vaccinations.

Obviously, the need to ensure optimum safety in a given system, industry, or process is absolutely essential. In fact, with certain critical functions of a system, there is no room for error or failure, as is evidenced in some of the above-listed examples. Thus, *safety* becomes a function of the situation in which it is measured (Leveson 1986).

Therefore, the question still remains as to the proper definition of *safety*. One possible improvement of the previously presented MIL-STD-882 definition might be that safety ... *is a measure of the degree of freedom from risk in any environment* (Leveson 1986). Hence, *safety* in a given system or process is not measured so much as is the level of *risk* associated with the operation of that system or process. This fundamental concept of acceptable risk is the very foundation upon which system safety has developed and is practiced today.

In the world of occupational safety, the ever-present requirement to achieve 100% compliance with written codes, rules, regulations, or established operating procedures is a challenge in and of itself. However, in the practice of system safety, it must be clearly understood that *design by code* is not a substitute for intelligent engineering and that codes only establish a *minimum* requirement which, in many systems or situations, must be exceeded to ensure adequate elimination or control of identified hazard(s). Therefore, 100% "compliance" usually means a system has met only the

*minimum* safety requirements. Looking at the subject of regulatory compliance in a different way, let us consider what it really means to be 100% compliant with the minimum requirements established by applicable codes and regulations. In the United States, for example, the Occupational Safety and Health Administration (OSHA) claims that occupational injuries and fatalities have decreased between 60% and 70% during the 50-year period of its existence between 1971 and 2021. While such a statistic is certainly laudable for obvious reasons, it also tells us that between 30% and 40% of workers in the United States are still suffering occupational injuries or fatalities. Clearly, compliance with the minimum requirements established by OSHA is not enough. Employers must do more. They must go beyond compliance, where required, to ensure optimum safety and health in the workplace.

The efforts associated with system safety attempt to exceed these minimum compliance standards and provide the highest level of safety (i.e., the lowest level of acceptable risk) achievable for a given system. In addition, it is important to mention at this point that system safety has often been used to demonstrate that some compliance requirements can be too excessive while providing insufficient risk reduction to justify the costs incurred. Costs, such as operating restrictions, system performance, operational schedules, downtime, and, of course, actual dollars, are all elements of a successful operation, which must be considered when determining the validity of implementing any new compliance controls. Proper utilization of system safety engineering has proven to be an excellent tool for evaluating the value of such controls with regard to actual savings and reduction of risk. For example: In general, the OSHA requires that machine guarding be employed to protect operators of machines from hazards created by the machining point of operation and/or other hazards associated with machine operation [Ref: OSHA 29 CFR §1910.212(a)(1)]. Both safety practitioners and machine operators are well aware that a machine can be effectively guarded to the point where it is no longer usable and, in actuality, borders on the ridiculous. Safety professionals will recall the famed "OSHA Cowboy" which was first drawn by J. N. Devin in 1972 and has circulated throughout the industry ever since. As shown in Figure 1.4, the OSHA Cowboy was a satirical view of OSHA compliance extremes. Essentially, the cartoon drawing demonstrated that the risks to the cowboy on horseback can be guarded and controlled to the point where even simple movement would be impossible.

As stated previously, system safety developed or evolved as a direct result of a need to ensure, to the greatest extent possible, reliability in the safe operation of a system or set of systems (especially when a given system is known to be hazardous in nature). While no system can be considered

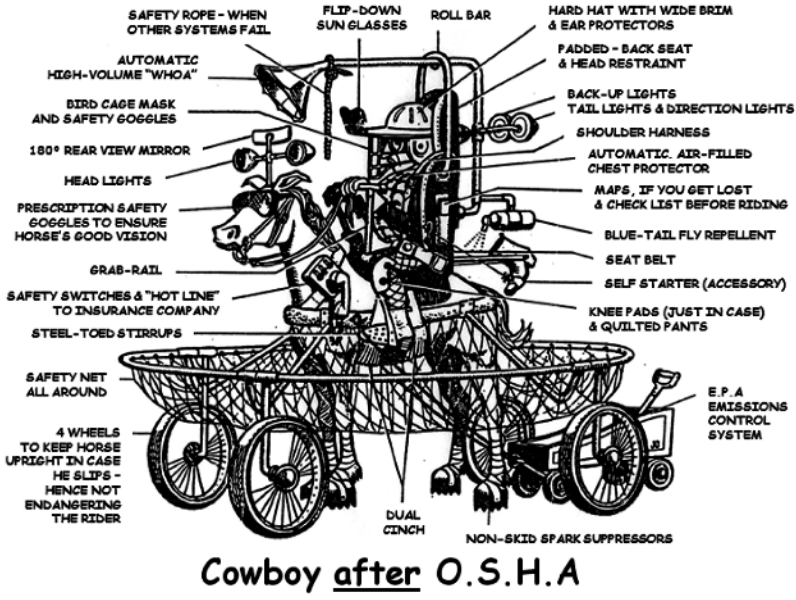


**Figure 1.4** The "OSHA Cowboy" as first depicted by J.N. Devin in 1972/John Wiley & Sons.

completely or 100% reliable, system safety is an attempt to get as close as practical to this goal. Over the years, numerous techniques and methods used to formally accomplish the system safety task have also evolved and have further expanded our capabilities to examine systems, identify hazards, eliminate or control them, and reduce risk to an acceptable level in the operation of that system. These analytical methods and/or techniques are known by many names such as, but certainly not limited to the following common system safety tools:

- Preliminary Hazard Analysis (PHA)
- System Hazard Analysis (SHA)
- Subsystem Hazard Analysis SSHA)
- Operating & Support Hazard Analysis (O&SHA)
- Failure Mode and Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Fault (or Functional) Hazard Analysis (FHA)
- Management Oversight and Risk Tree (MORT)
- Energy Trace and Barrier Analysis (ETBA)
- Sneak Circuit Analysis (SCA)
- Software Hazard Analysis (SWHA)

- Common Cause Failure Analysis (CCFA)
- Cause and Effect Analysis (CEA)
- Event Tree Analysis (ETA)
- Hazard and Operability Studies (HAZOP)
- Random Number Simulation Analysis (RNSA)
- Health Hazard Analysis (HHA)

The chapters in Part 2 of this text will provide a simplified explanation of the most commonly used of these techniques. The intention is to present a *basic foundation of understanding* with regard to the fundamental analytic methods associated with the system safety engineering discipline. It is important to note once again that it is not the purpose of this limited volume to provide a single-source technical reference on the complete scope of the system safety discipline. This approach, although feasible, is not practical or advisable when attempting to discuss only the basics of system safety development and its potential use in general industry. There are numerous scientific and engineering reference volumes available on this subject and further research is recommended for those who desire more complete and detailed instruction on the use of system safety techniques. In addition, many universities, training institutions, professional and trade organizations, and independent private consultants offer continuing educational courses on the subject of system safety engineering/analysis.