

Part I

The System Safety Program

In the practice of occupational safety and health in industry today, the primary concern of any responsible organization is the identification and elimination of hazards that threaten the life or health of employees, as well as those that could cause damage to facilities, property, equipment, products, and/or the environment. When such risk of hazard cannot be totally eliminated, as is often the case, it becomes a fundamental function of the safety professional to provide recommendations to control those hazards in an effort to reduce the associated risk to the lowest acceptable levels.

It is the intention of this *Basic Guide to System Safety* to demonstrate the effectiveness of the system safety process in identifying and eliminating hazards and in recommending risk reduction techniques and methods for controlling residual hazard risk.

Part I introduces the reader to the system safety process, how it evolved, how it can be managed, and how it relates to the current practice of the industrial safety and health profession. In fact, on completion of Part I, the reader shall have developed a clear understanding of this relationship and, quite possibly, have developed an interest in the further pursuit of the system safety profession. As noted in the Preface, the information provided here is introductory in scope, intended to merely acquaint the reader with the system safety approach to hazard analysis and hazard risk reduction.

1

System Safety: An Overview

1.1 BACKGROUND

The idea or concept of *system safety* can be traced to the missile production industry of 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 aviation industry, this process was often referred to as the “fly–fix–fly” approach to design problems (Moriarty and Roland 1983; Stephenson 1991). Simply stated, aircraft design was based on existing or known technology. The aircraft was then flown until problems developed or, in the worst case, it crashed. 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. Elements such as these became the catalyst for the development of *systems engineering*, out of which eventually grew the concept of *system safety*. Figure 1.1 shows a simplification of the basic elements

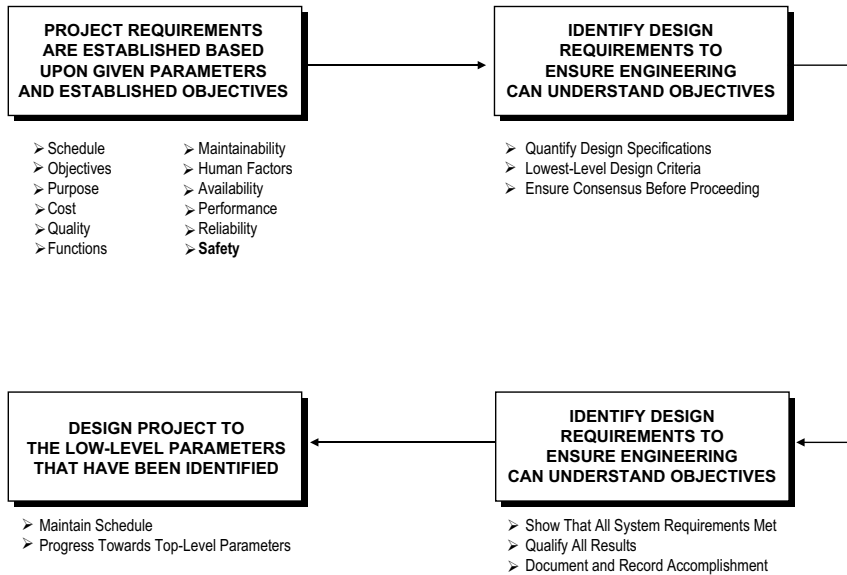


Figure 1.1 The system safety engineering process [source: Larson and Hann (1990)].

of the systems engineering process. It is noted that safety represents only one part of this integrated engineering design approach (Larson and Hann 1990).

The dawn of the manned spaceflight program in the mid-1950s also contributed to the growing necessity for safer system design. Hence, the budding 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 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 failure. During those early 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 on reentry in February 2003 stand as constant 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 applies in any industry or discipline.

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

Today, the system safety process is still used extensively by the various military organizations within the Department of Defense, as well as by many other federal agencies 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 is on 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 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. Although the former example is usually the case, the latter is also responsible for the development of countless safe operating requirements practiced in industry today. Both, however, are also the basis on 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, and other measures, 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.

1.2 SYSTEM SAFETY AND 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 design and implementation of engineering controls. Basically, according to Stephenson (1991), 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.

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 practical logic, for 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 hazard of risk to its lowest acceptable levels. In reality, no aircraft could fly, no automobile could move, and no ship could be put out to sea if *all* hazards and *all* risk had to be completely eliminated first (Hammer 1972). Similarly, no drill press could be operated, forklift driven, petroleum refined, dinner cooked, microwave oven used, water boiled, and so on 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 approved (by the U.S. Food and Drug Administration) preservatives 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 tradeoff between the known benefits of improved medical diagnosis and treatment that result from the use of radiation (e.g., X rays, 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 overused in our society. However, consider the following statistical facts (Larson and Hann 1990):

In the United States today, 99.9% safe would mean

- 1 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 physicians 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 would indicate that 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 examples listed above. 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 as 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 on 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 principles is a challenge in and of itself. However, in the practice of system safety, it must be clearly understood that “design by code” is no substitute for intelligent engineering and that codes establish only a minimum requirement that, in

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 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 and 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
- Random-number simulation analysis (RNSA)

The chapters in Part II of this text 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 that 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 and analysis.

