CHAPTER 1

The History of System Safety

Prior to the 1940s, safety was generally achieved by attempting to control obvious hazards in the initial design and then correcting other problems as they appeared after a product was in use or at least in a testing phase. In other words, designers relied, at least in part, on a trial-and-error methodology. In the aviation field, this process became known as the fly-fix-fly approach. An aircraft would be designed using the best knowledge available, flown until problems were detected (or it crashed), and then the problems would be corrected and the aircraft would be flown again. This method obviously worked best with low, slow aircraft.

This approach was not acceptable for certain programs—such as nuclear weapons and space travel—soon became apparent, at least to some. The consequences of accidents were too great. Trial-and-error and fly-fix-fly approaches were not adequate for systems that had to be first-time safe.

Thus, system safety was born or, more accurately, evolved. The history of system safety consists of

- Traditional trial-and-error or fly-fix-fly approach not adequate for aerospace and nuclear programs
- 1960s—MIL-STD-882 (DoD, NASA)
- 1970s—MORT (Department of Energy)
- 1980s—Other agencies
- 1990s—Risk-based process safety
- 2000s—Quest for intrinsic safety
- 2010s—Risk management integration
- 2020s—Improvements and international approach to risk maturing

The roots of the system safety effort extend back at least to the 1940s and 1950s. Accurately tracing the early transition from the traditional trial-and-error approach to safety to the first-time safe effort that lies at the heart of system safety is really impossible, but such a transition occurred as both aircraft and weapon systems became more complex and the consequences of accidents became less acceptable.

System Safety for the 21st Century, Second Edition. Richard A. Stephans.

Companion website: www.wiley.com/go/stephans/systemsafety2

THE 1960s—MIL-STD-882, DOD, AND NASA

Even though the need for a more in-depth, upstream safety effort was recognized relatively early in the aviation and nuclear weapons fields, not until the 1960s did system safety begin to evolve as a separate discipline. In the 1960s

- USAF publishes "System Safety Engineering for the Development of Air Force Ballistic Missiles" (1962)
- USAF publishes MIL-S-38130, "General Requirements for Safety Engineering of Systems and Associated Subsystems and Equipment" (1963)
- System Safety Society founded (1963)
- DoD adopts MIL-S-38130 as MIL-S-38l308A (1966)
- MIL-S-381308A revised and designated MIL-STD-882B, "System Safety Program Requirements" (1969)

Most agree that one of the first major formal system safety efforts involved the Minuteman intercontinental ballistic missile (ICBM) program. A series of pre-Minuteman design-related silo accidents probably provided at least part of the incentive (U.S. Air Force 1987).

Early system safety requirements were generated by the U.S. Air Force Ballistic System Division. Early air force documents provided the basis for MIL-STD-882 (July 1969), "System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for." This document (and revisions MIL-STD-882A and MIL-STD-882B) became, and remain, the bible for the Department of Defense (DoD) system safety effort (Moriarty and Roland 1983).

In addition to weapon systems, other early significant system safety efforts were associated with the aerospace industry, including civil and military aviation and the space program.

Even though the National Aeronautical and Space Administration (NASA) developed its own system safety program and requirements, the development closely paralleled the MIL-STD-882 approach and the DoD effort, primarily because the two agencies tend to share contractors, personnel, and, to a lesser degree, missions.

Also, through the early to mid-1960s, the System Safety Society emerged. This professional organization was founded in the Los Angeles area by Roger Lockwood. Organizational meetings were held in 1962 and 1963. The organization was chartered as the Aerospace System Safety Society in California in 1964. The name was changed to System Safety Society in 1967 (Medford 1973). In 1973, the System Safety Society was incorporated as "an international, nonprofit, organization dedicated to the safety of systems, products, and services" (System Safety Society 1989).

THE 1970s—THE MANAGEMENT OVERSIGHT AND RISK TREE

In the late 1960s, the Atomic Energy Commission (AEC), aware of system safety efforts in the DoD and NASA communities, made the decision to hire William G. Johnson, retired manager of the National Safety Council, to develop a system safety program for the AEC.

In the mid-1970s, AEC was reorganized into the Department of Energy (DOE). Even though the individual AEC programs and the AEC contractors had good (some better than others) safety programs in place, the programs and approaches varied widely. This lack of standardization or commonality made effective monitoring, evaluation, and control of safety efforts throughout the organization difficult, if not impossible.

Thus the goals of the AEC effort were to improve the overall safety effort by

Developing a new approach to system safety that incorporated the best features of existing system safety efforts
Providing a common approach to system safety and safety management to be used throughout the AEC and by AEC contractors

In 1973, revised management oversight and risk tree (MORT) manual was published by the AEC. Even though Johnson borrowed heavily from existing DoD and NASA programs, his MORT program bore little resemblance to programs based on MIL-STD-882 (Johnson 1973).

The work by Bill Johnson was expanded and supplemented throughout the 1970s by the System Safety Development Center (SSDC) in Idaho Falls, Idaho. The MORT program provides the direction for this second major branch of the system safety effort.

Progress in the 1970s included

- NASA publishes NHB 1700.1 (V3), "System Safety" (1970)
- AEC publishes "MORT—The Management Oversight and Risk Tree" (1973)
- System Safety Development Center founded (1974)
- MORT training initiated for AEC, ERDA, and DOE (1975)
- MIL-STD-882A replaces MIL-STD-882 (1977)

THE 1980s—FACILITY SYSTEM SAFETY

Throughout the 1980s, three factors have driven system safety tools and techniques in areas other than the traditional aerospace, weapons, and nuclear fields.

First, the complexity and high cost of many nonflight, nonnuclear projects have dictated a more sophisticated upstream safety approach. Second, product liability litigation has provided added incentive to produce safe products, and, third, system safety experience has begun to demonstrate that upstream safety efforts lead to better design. System safety tools and techniques originally considered to be expensive but necessary add-ons have proven to be cost-effective planning and review tools.

Significant programs initiated or developed in the 1980s include the facility system safety efforts of the Naval Facilities Command and the U.S. Army Corps of Engineers and initiatives in the petrochemical industry.

- MIL-STD-882B replaces MIL-STD-882A (1984)
- NAVFAC sponsors system safety courses (1984)
- AIChE publishes "Guidelines for Hazard Evaluation Procedures" (HazOps) (1985)
- MIL-STD-882B updated by Notice 1 (1987)
- USACE-sponsored facility system safety workshops initiated (1988)

The need for a system safety effort for major military construction projects resulted in the development of draft guidelines and facility system safety workshops for the military safety and engineering communities. By the end of the decade, facility system safety training programs for government employees were established, and similar courses for contractors were available. Regulations outlining facility system safety efforts were pending, and facility system safety efforts were being required on selected military construction projects. In addition, NASA was initiating facility system safety efforts, especially for new space station support facilities.

In 1985, the American Institute of Chemical Engineers (AIChE) initiated a project to produce the "Guidelines for Hazard Evaluation Procedures." This document, prepared by Battelle, includes many system safety analysis tools. Even though frequently identified as hazard and operability (HazOp) programs, the methods being developed by the petrochemical industry to use preliminary hazard analyses, fault trees, failure modes, effects, and criticality analyses, as well as similar techniques to identify, analyze, and control risks systematically, look very much like system safety efforts tailored for the petrochemical industry.

THE 1990s—RISK-BASED PROCESS SYSTEM SAFETY

If the 1980s was designated as "facility safety," then the 1990s should be identified as "process safety." Prior to the 1990s, OSHA regulations were almost exclusively compliance-based. Very specific rules were promulgated, and inspections were made to ensure that the rules were followed. The OSHA process safety regulation (29 CFR 1910.119) required that the risk associated with a manufacturing or chemical processing site with listed substances be assessed and appropriate actions be taken to mitigate the results of an accident to protect the workers.

In addition, there was greater interface with quality assurance (QA) to include the management of change segment so important to safety. An analogy related to the safety aspect of change management is advice given when first driving a car. As long as you are in the same lane and stay there, you are fairly safe, but when you have to move lanes or make a turn, you must be particularly careful and watchful about what you are about to do. Much the same can be said about changes to hardware and software during design, development, and fielding. It also became more apparent that the "quality" of input materials was very important to desired output product as well as to the safety performance of the product. Product impurities could weaken a structure and result in an undesired chemical reaction with intermediate chemical ingredients.

Further, the QA audit function is directly related to safety. QA audits with an encompassing scope include facility and process safety as one of the elements reviewed.

Milestone Standards Issue Events

System safety-related events and guidance documentation evolution and emergence in the 1990s included: 882C in 93; the *System Safety Analysis Handbook* in 1993 (with a second edition in 1997). The handbook is currently sold in more than 35 countries; PSM in 1992; RMP in 1996; *Hazard Prevention* changed to the *Journal of System Safety* in 1999; European Machining Standard, European Norm (EN) 1050 in 1997 that requires risk analysis prior to mechanical or electrical controls; the System Safety Society increases the frequency of international conferences to annually; Center for Chemical Process Safety established; publication of the "System Safety and Risk Management—NIOSH Instructional Manual" by Dr. Rodney Simmons and Pat Clemens, both strong advocates of system safety and both very closely tied to the maturation of the Board of Certified Safety Professionals.

At the 1993 International System Safety Conference, the then Chief of Air Force Safety in his keynote presentation said that the two challenges for the 90s were in software system safety and in human factors. This was true then, and it is today, more than ten years later.

THE 2000s—QUEST FOR INTRINSIC SAFETY

As we progress into the new century, there are both opportunities and challenges. Opportunities present themselves in the form of (1) the potential of integrating system software safety with control engineering to more closely achieve a level of "intrinsic safety" and (2) the proliferation

of system safety as a discipline in other parts of the world. The challenges we face include the realization of security needs after the terrorist attack on the United States on September 11, 2000. Additional challenges and a future prediction are presented in Chapter 5.

We define intrinsic safety as safety designed and built into a system. Yes, this is an overlap with system safety. The two concepts are converging. Intrinsic safety is certainly a noble goal and one that should be continually pursued.

The proliferation of information on the Internet can be overwhelming. It is important to know how to move around the Internet using search engines, generic sites, and links. The Internet can provide much useful information in a relatively short period of time.

Milestone Standards Issue Events

MIL-STD-882D (10 FEB 2000); ANSI B11.TR3 (2000) which promulgated guidance related to safety through design; EN1050 (97) for risk assessment prior to the installation of new machinery; the U.S. Department of Energy's 10 CFR 830 in 2001, effective in 2003 for nuclear safety management.

A new issue of Military Standard 882 in the year 2000 provided for a modified approach to system safety achievement. The Standard was renamed as a "Standard Practice for System Safety, and its implementation is further discussed in Chapter 3 "Current Approaches to System Safety." Suffice to say here, the standard allows for flexibility in implementation while preserving basic system safety requirements.

THE 2010s—RISK MANAGEMENT INTEGRATION

E-Version of 882. The current version of 882 continues to provide a standard, generic method for the identification, classification, and mitigation of hazards. It clarifies terminology and defines task descriptions to improve management practices. While the previous version removes task descriptions, this version reinstates them.

Risk Management Formalization. Internationally, with a new ISO and within the United States, it has been done via the Government Accountability Office (GAO). Chapter 10 has more details about the integration of risk management.

Boeing Disasters. Two Boeing 737 MAX passenger aircraft crashes took place with a similar cause and more than 300 fatalities. While all the corrective actions have yet to be completed and seen to be implemented as of this book edition, the status is discussed in the next section.

THE 2020s – IMPROVEMENTS AND INTERNATIONAL APPROACH TO RISK MATURING

While there are many improvements toward the enhancement to the reduction of risk and hazards, there have been steps back to include war in Europe and the international pandemic that started in China. It is still early in the decade and it's been a wild one. As this text goes to publication, we are seeing reductions in the scourge of disease, but we are still in the clutches of COVID. The end is in sight and there is the distinct possibility that the COVID will continue and be flu-like for years to come. More to the point, we still face continuation from a major Boeing 737 MAX disaster of the past that has and will continue into require after actions.

After 20 months, a number of global regulators have joined with the FAA in lifting 727 MAX suspension orders. The detailed software correction now operates in unusual flight conditions and relies on added sensors. Boeing has agreed to pay $2.5B in fines and that does not include the lawsuits associated with the 346 deaths.

Milestone Standards Issue Events

MIL-STD-882 continues to be the primary guidance for the system safety field. With a current upgrade in process there is a high probability that it will be somewhat influenced by external events and thinking. With war in Europe, there has been added focus on defense and rearming.

As detailed in Chapter 10, the latest version of ISO 13000 addresses enterprise risk management and it has been emulated in part by out General Accountability Office it their 17-63 regulation. Chapter 10 continues to describe the risk management application in a half dozen government agencies. Good practices associated with enterprise culture from GAO 17-63 are particularly important.

Further recent updates to ANSI Z10 the National Standard for Management Systems in Occupational Safety and Health now prescribes feedback and a more pro-active approach rather than being reactive.

REVIEW QUESTIONS

1. Explain the fly-fix-fly approach to developing safe products.
2. What made the fly-fix-fly approach unacceptable? What were the first types of programs to seek something better than the fly-fix-fly approach?
3. How did MIL-STD-882 evolve? Where did it originate and who uses it now?
4. How did the MORT approach to system safety develop? Who developed it and who uses it?
5. Identify the three primary factors that drove the expansion of system safety during the 1980s.
6. Name three areas in which system safety efforts were initiated or developed during the 1980s.
7. Discuss why, although it is appropriate to transition to risk-based safety, it is not possible or appropriate to entirely do away with safety compliance.
8. Name two quality assurance program elements and explain their interface with system safety.
9. Name and explain why two locations outside the United States are becoming "centers" for safety standards development.
10. Although the Internet existed for a decade prior to the year 2000, why is it so much more popular today?

BIBLIOGRAPHY

Johnson, W. G. 1973. *MORT, The Management Oversight and Risk Tree*. Washington, DC: U.S. Atomic Energy Commission.

Medford, F. 1973. History of the system safety society (SSS). *Hazard Prevention* 9(5):38–40.

Moriarty, B., and Roland, H. E. 1983. *System Safety Engineering and Management*. New York: John Wiley & Sons.

U.S. Air Force. 1987. *SDP 127–1: System Safety Handbook for the Acquisition Manager*. Los Angeles: HQ Space Division/SE.

U.S. Department of Defense. 2012. MIL-STD-882E: Department of Defense. *Department of Defense Standard Practice System Safety*. Washington, DC: Department of Defense.