System Safety:

A Science and Technology Primer

by

The New England Chapter

of the System Safety Society

April, 2002

Although care is taken to ensure the quality of this document, the publishers and other contributors and sponsors cannot be held responsible for its accuracy or for any errors, damages or injuries resulting from its use or misuse.

Table of Contents

Preface

This system safety primer has been developed to provide basic information to those who might be interested in pursuing a career in the field of system safety. It contains a brief history describing how the discipline came into being, and its historical importance.

This book offers the reader a synopsis of the various facets of the science, and how it has come to be recognized as an integral part of the production process for virtually every product and service that exists in today's world. No longer simply a method to reduce the occurrence of failure, or to prevent injury to personnel, system safety has emerged as a global imperative, necessary to facilitate technological advances, while simultaneously aiding in the preservation of our greatest natural resources — humans and our environment.

Welcome to system safety!

Dave Rice,
President,
New England Chapter of the
System Safety Society,
April 2002

What is System Safety?

by Niles T. Welch, CSP
ASWaterman Inc.

Introduction

As defined by MIL-STD-882, system safety is “the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.” Today, system safety is pushing at the constraints of its MIL-STD definition. To accurately define system safety, one must first determine the scope of the system in question. Is it composed of only one element (e.g., hardware or software), or will the system include the human factor as it applies to the design, operation, handling or maintenance of the system or its parts? It may be a simple device, or it could be a complicated series of devices and/or subsystems all functioning together in a specific environment. Defining what comprises the system is an essential first step in determining its system safety.

In many respects, system safety is a global concept. As shown in Figure 1 below, system safety has a direct impact on the environment. Its effects are more far-reaching than may be perceived. Figure 1 shows how system safety is traditionally defined. Consequently, it affects much more than just the systems under consideration. All hazard analyses must consider the environmental effects on personnel, the ecosystem and the equipment itself, in the quest for making, using and otherwise handling a system safely.

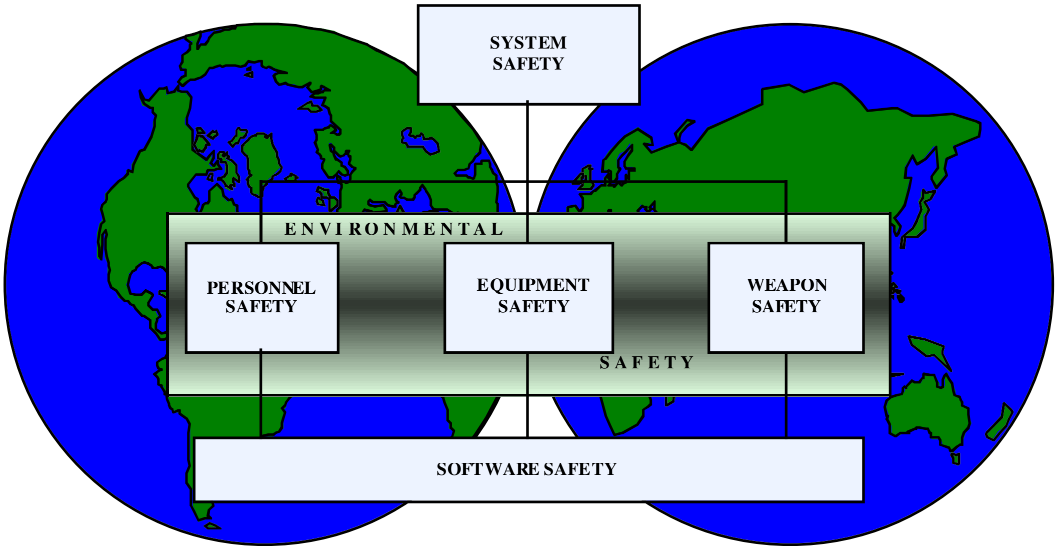


Figure 1.1 — System safety is a much broader concept than we may perceive.

In the broader sense, as illustrated in Figure 1.2, many aspects of system safety overlap to become a part of several different safety disciplines. For example, we as system safety practitioners can no longer consider chemical safety as separate and unrelated to system safety. Nor can the other items within the overlapping circles be segregated. System safety encompasses the whole of all its parts as the boundaries of the systems being analyzed expand. Safety professionals can no longer compartmentalize their own segment of system safety. All disciplines interact and are significant contributors to any, and perhaps all, other safety disciplines. Though we are skilled specialists, we alone cannot always determine what is right for ensuring overall safety. Non-system safety disciplines will also realize that their safety is part of the overall picture of system safety — once again, a global concept — where all safety disciplines are interrelated.

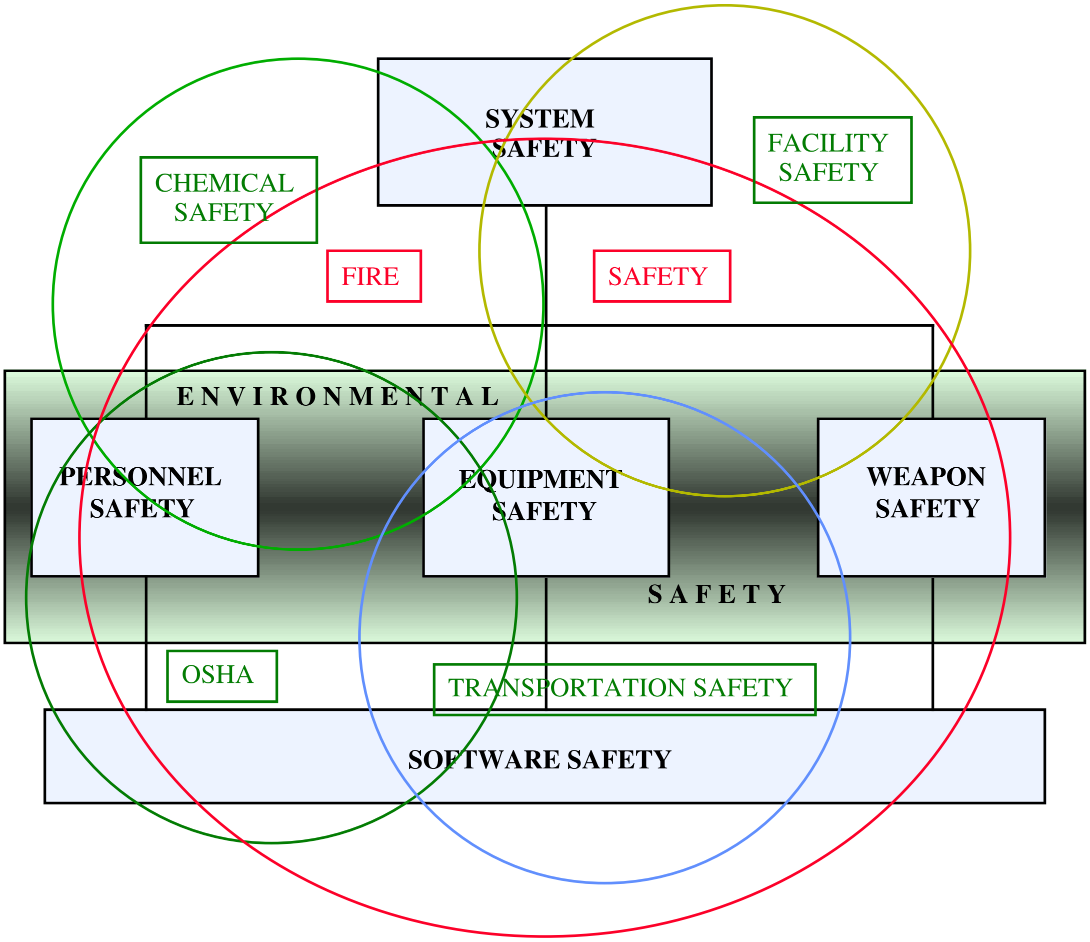


Figure 1.2 — All safety disciplines can be viewed as interrelated.

System Safety Definitions per MIL-STD-882:

Safety: Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

System safety: The application of engineering and management principles, criteria and techniques to achieve acceptable mishap 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 professional knowledge and skills in applying scientific and engineering principles, criteria and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

Safety-critical: A term applied to any condition, event, operation, process or item whose proper recognition, control, performance or tolerance is essential to safe system operation and support (e.g., safety-critical function, safety-critical path, or safety-critical component).

Fail-safe: A design feature to ensure that the system remains safe; or in the event of a failure, something that causes the system to revert to a state that will not cause a mishap.

Hazardous material: Any substance that causes safety, public health or environmental concerns requiring an elevated level of management effort, due to its chemical, physical or biological nature.

Health hazard assessment: The application of biomedical knowledge and principles to identify, eliminate or control health hazards associated with systems, in direct support of the life-cycle management of materiel items.

Life cycle: All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.

Mishap: An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Mishap risk: An expression of the possibility of a mishap and its impact, in terms of potential mishap severity and probability of occurrence.

Residual mishap risk: The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety specifications and guidelines.

Mishap probability: The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap.

Mishap probability levels: An arbitrary categorization that provides a qualitative measure of the most reasonable likelihood of occurrence of a mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies; or system, subsystem, or component failure or malfunction.

Mishap risk assessment: The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions.

Mishap risk categories: An arbitrary categorization of mishap risk assessment values often used to generate specific action, such as mandatory reporting of certain hazards to management for action, or formal acceptance of the associated mishap risk.

Mishap severity: An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard.

Mishap severity category: An arbitrary categorization that provides a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies; or system, subsystem, or component failure or malfunction.

When Do You Use System Safety Techniques?

System safety techniques should be used on any system that requires safety analyses.

Where is System Safety Used?

- Aerospace
- Automotive
- Aviation
- Computers & Software
- Business & Finance
- Biomedical
- Chemical
- Everywhere!

MIL-STD-882 – Its History and Importance

by David O'Keeffe
Raytheon Electronic Systems Company

System safety, as we know it today, was introduced in the 1940s. Gaining momentum and support during the 1950s, its value became firmly established during the Vietnam era. The system safety concept was not the brainchild of one person. It began as a grass roots movement within the engineering and safety communities to design and build safer equipment by applying lessons learned from accident investigations. In response to the general dissatisfaction with the "fly-fix-fly" approach to aircraft systems design, the early 1960s saw many new developments in system safety. In 1963, the Aerospace System Society was formed in Los Angeles, California. The University of Southern California's Aerospace Safety Division launched a Master's degree program in Aerospace Operations Management in 1964. Later, specific system safety graduate courses were developed. In 1965, the University of Washington began offering a short course in system safety analysis. System safety had become a recognized field of study.

In July 1969, MIL-STD-882 was published. This landmark document placed emphasis on system safety as a management science, and continued to expand the scope of system safety to apply to all military services within the Department of Defense (DoD). The full life-cycle approach to system safety was also introduced by MIL-STD-882, but this newest expansion in scope required a reworking of the system safety requirements. The result was a phase-oriented program that linked system safety requirements to the various stages of their development. This approach to system safety was a marked contrast to earlier guidelines, and the details provided to the practitioner were greatly expanded.

MIL-STD-882 was superseded in June of 1977 by MIL-STD-882A. The major contribution of MIL-STD-882A to system safety was its focus on the concept of risk acceptance as a criterion for developing system safety programs. Perhaps the most significant development to date, this milestone led to the inclusion of hazard probabilities, and established categories for frequency of occurrence to accommodate the long-standing hazard severity categories.

In March of 1984, MIL-STD-882B was published. It was a major reorganization of MIL-STD-882A, offering more detailed guidance in engineering and management requirements. However, as the standard evolved, these requirements were becoming more complex, provoking more discussion on tailoring the risk acceptance. Greater emphasis was placed on facilities and off-the-shelf acquisitions. In July of 1987, Notice 1 to MIL-STD-882B addressed software tasks and expanded their treatment as system safety elements.

MIL-STD-882C was released in January of 1993, integrating the hardware and software safety efforts that preceded it. A safety analysis would now include identifying the hardware and software tasks together within a system. Notice 1 to 882C was published in January of 1996 to revise the "data items descriptions" category for more universal application.

The mid-1990s saw the beginning of the acquisition reform movement. Together with the Military Specifications and Standards Reform (MSSR) movement, these actions spurred the creation of Standard Practice MIL-STD-882D, published in January of 2000. Under 882D, program managers would specify system performance requirements as before, but specific system details were now the responsibility of the system's designer. The use of military specifications was kept to a minimum, and only performance-oriented military documents were allowed. Commercial item descriptions and industry standards were now to be used for program details. The use of MIL-STD-882 was allowed to continue, provided it was converted to a performance-oriented military standard; and MIL-STD-882C was still used, but a waiver was generally required for it to be specified by a military program manager.

Today, the discipline of system safety is best described as an evolving science, consistently increasing its scope to meet an expanding number of system requirements. The underlying principles remain intact, while system safety concepts change and mature through increased knowledge and sparkling advances in technology. Still, MIL-STD-882 remains the standard for system safety, both within the military and in private industry.

System Safety Process Tasks

by Greg Huffmann
Raytheon Electronic Systems Company

These are the system safety tasks generally used to complete a system safety program:

- System Safety Program Plan
- Preliminary Hazard List
- Preliminary Hazard Analysis
- Subsystem Hazard Analysis
- System Hazard Analysis
- Operating and Support Hazard Analysis
- Hazard Tracking and Risk Resolution
- Safety Assessment Report
- Design Reviews

System Safety Program Plan

A System Safety Program Plan (SSPP) is a detailed description of the planned tasks and activities used when implementing the required system safety program. The SSPP includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort and points of integration with other program, engineering and management activities, and related systems. In its initial stages, it provides a basis of understanding for both the contractor and the Managing Activity, describing how the system safety program will be accomplished. Any SSPP changes requested by the contractor must be approved by the Managing Activity (i.e., the customer, as defined by MIL-STD-882).

Details of the plan will include the steps necessary to identify, evaluate and eliminate/control hazards, or to reduce the associated risks to a level acceptable to the Managing Activity, throughout the system's life cycle. The approved plan, amended to include specific as well as general provisions, becomes a blueprint between the contractor and Managing Activity for how the system safety program will be implemented to meet contractual requirements.

The purpose of the SSPP is to establish direction, and control monitoring and validation for the system under analysis. It defines the participants of the safety program and their responsibilities, which minimally include:

1) Defining safety requirements
2) Detailing safety analysis techniques
3) Outlining hazard risk and assessment criteria (hazard risk index)

An SSPP also describes safety analysis and testing methods. All personnel and equipment hazards that could possibly be encountered need to be identified. It will provide solutions for either elimination of the hazard, or mitigation to an acceptable level, with consideration given to time and cost parameters. The goal of the SSPP is to ensure that safety is an integral part of the system design. The plan details the System Safety Program’s organization, implementation procedures and compliance to standards, as well as its compliance to other system safety plans.

Safety issues need to be continuously identified, documented, tracked and resolved. This process of hazard analysis must persist throughout the life cycle of the plan. The SSPP dictates what type of closed-loop system (generally a database) to use to obtain information that will eliminate, or mitigate to an acceptable level, all identified hazards. This system will contain the hazards from your preliminary hazard list (as described elsewhere in this primer), the initial hazard risk index (HRI), the mitigation recommendation, the target HRI and the final HRI after mitigation.

The SSPP also defines the independent groups who must concur that the system is safe. For Navy weapons systems, these groups are the Weapons Safety Explosive System Review Board (WSESRB) and the Software System Safety Technical Review Panel (SSSTRP). The SSSTRP is a sub-board of the WSESRB and makes recommendations to the WSESRB regarding software safety issues. Another group that considers safety issues is the System Safety Working Group (SSWG). This group consists of representatives from the system and safety communities of the contractor, customer and any other organization that may be deemed appropriate for the project. A generic outline of the chapters for an SSPP, as taken from MIL-STD-882C, is shown below:

Section 1 ....Introduction
Section 2 ....System Description
Section 3 ....System Safety Program
Section 4 ....System Safety Milestones
Section 5 ....System Safety Requirements and Criteria
Section 6 ....Hazard Analyses
Section 7 ....System Safety Data
Section 8 ....System Safety Verification and Program Auditing
Section 9 ....Range Safety Considerations
Section 10 ......Environmental Considerations
Section 11 ......Demilitarization and Disposal
Section 12 ......Training
Appendix A....SSWG Charter

Preliminary Hazard List

A Preliminary Hazard List (PHL) defines the top-level hazards for the given system. Its purpose is to initially identify the most evident hazards that could occur in the system being built. These hazards are identified as anything that may be inherent to the concept and the associated mishap potential, or hazards specified by the Managing Activity. To formulate a PHL, historical data from similar systems is compared to that which is under review. Several sources for reference are provided in the list below. Note that this list is in no way all encompassing, but it is a solid starting point.

PHL Input:

1. Safety/system engineers from respective systems
1. Preliminary requirements and specifications
2. Generic hazards list
3. Similar Systems Hazard Analysis/lessons learned
4. Accident/Incident Reports

Typically, the PHL is developed through safety brainstorming during the initial SSWG session. At this meeting, the group should:

1. Consider all system and logistical aspects/phases
2. Identify possible energy sources and controls/containment
3. Identify mishaps resulting from inadvertent release of energy, or loss of energy control
4. Identify the worst-case hazard severity

After completing these brainstorming sessions, the safety engineer will compile a preliminary list of hazards.

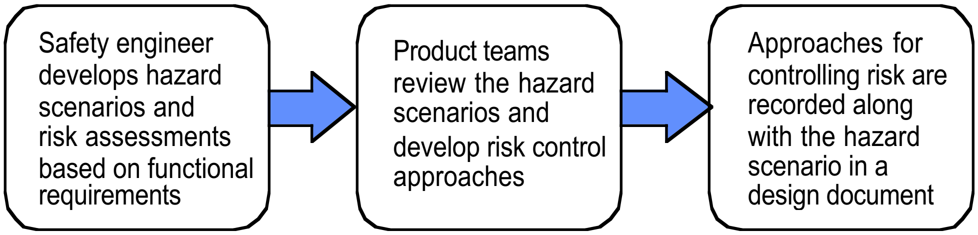
Preliminary Hazard Analysis

A Preliminary Hazard Analysis (PHA) is a high-level exercise intended to identify system-level safety issues during the earliest stages of development. The PHA is conducted during the initial requirements analysis phase of a project. The specific format of the analysis depends on the objective of the analyst, and the particular tools used to conduct the study.

The PHA focuses on system-level hazards that may be produced by the overall system. Its main objective is to identify system hazards as early as is practical, and either eliminate or control them to acceptable levels. Hazards are removed by selecting alternative technologies or materials. Risk is controlled via the system's technology by a reduction in the severity of harm and/or the probability of the hazard occurring.

A typical PHA hazard scenario includes a description of the hazard, the conditions that may cause it to escalate to a mishap, and the consequences that result when a mishap does occur. Hazard scenarios materialize early, usually after analysis of the functional requirements being proposed for the system under development. In a development team environment, a safety engineer or other responsible individual identifies the hazard scenarios, assesses the potential risk of the hazards, and presents the findings to the other members of the team. Based on input from the hazard analysis, the team develops general approaches for controlling the risk of each scenario. These approaches are commonly high-level in nature. For example, to control the exposure potential to high voltage operators, the hazard can be eliminated by selecting a different technology. Another alternative is to localize all of the high voltage equipment, and place it in interlocked enclosures. A third option uses ground fault interrupters and/or grounding and bonding schemes to minimize the consequences of exposure. Each approach will drive different system requirements and require appropriate trade studies to develop the optimum solution for the system in development.

The figure below illustrates the necessity for team understanding of hazard scenarios, and determining the general approaches for controlling the risk of identified hazards. Team understanding is accomplished by an initial discussion of the hazard scenario with key individuals from the appropriate product development teams. A general approach for addressing the hazard is suggested, and the product development team most likely to be affected is identified. The approach is documented and presented formally to the team for further discussion. The safety engineer or other responsible individual records the details and resulting decisions for controlling the hazard. The team assigns a member who is responsible to further research each of the hazard controls presented as a result of the team's decisions.


Safety engineer develops hazard scenarios and risk assessments based on functional requirements

Product teams review the hazard scenarios and develop risk control approaches

Approaches for controlling risk are recorded along with the hazard scenario in a design document

Developing General Controls for Hazard Risk.

In a multiple team environment, all teams are responsible for judging the credibility of each hazard scenario, and for determining which team will handle the problem. Cross-team issues are worked out between affected teams, or are deferred to management for review, and then delegated to the appropriate team members.

Subsystem Hazard Analysis

A Subsystem Hazard Analysis (SSHA) is performed to:

- Verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents
- Identify previously unknown hazards associated with the design of subsystems, including component failure modes, critical human error inputs, and hazards resulting from functional relationships between the components and equipment comprising each subsystem
- Recommend actions necessary to eliminate identified hazards, or control their associated risk to acceptable levels.

The processes used to conduct the SSHA identify the components and equipment that could result in a hazard, or whose design does not satisfy contractual safety requirements. Under scrutiny will be government-furnished equipment, non-developmental items and software. Factors to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. During the course of this analysis, the human element is considered a component that receives inputs and initiates outputs within a subsystem. The analysis includes determination of the following:

- Possible modes of failure that include reasonable human error, as well as single point and common mode failures, and the effects on safety when a failure occurs in subsystem components
- Potential contributions of hardware and software events (including those developed by other contractors/sources), faults and occurrences (e.g., improper timing) on the safety of the subsystem
- Satisfactory fulfillment of safety design criteria in the hardware, software and facilities specifications
- Hardware, software and facilities design requirements and corrective actions, such that they do not impair or decrease the safety of the subsystem, or introduce any new hazards or risks
- Detailed safety design requirements from top-level down through the design specifications for the subsystem (the Preliminary Hazard Analysis and Safety Requirements Criteria Analysis should also be included in the analysis to ensure that these requirements are met)
- Safety test plan and procedure recommendations to integrate into the hardware and software test programs
- Analysis of system-level hazards attributed to the subsystem, and the inclusion of adequate controls of the potential hazard in the design

If no specific analysis techniques are indicated, or if the contractor recommends that a technique other than those specified by the Managing Activity be used, the contractor will obtain Managing Activity approval prior to performing the analysis. Analysis types and techniques to consider for the SSHA are:

- MIL-STD-2036A Checklist
- MIL-HDBK-454 Checklist
- Fault Tree Analysis
- Failure Modes and Effects Analysis
- Event Tree Analysis
- Software Hazard Analysis
- Sneak Circuit Analysis
- Cause/Effect Analysis
- Safety Requirements Criteria Analysis
- Radiation Hazard Analysis

- Hazards of Electromagnetic Radiation to Ordnance (HERO) Analysis
- Hazards of Electromagnetic Radiation to Fuel (HERF) Analysis
- Hazards of Electromagnetic Radiation to Personnel (HERP) Analysis
- Single Point Failure Analysis
- Common Mode Failure Analysis
- Threat Hazard Assessment

When subsystem software is being developed under DoD-STD-2167 or -2168, or MIL-STD-1679 or other development documents, the contractor will obtain, use and monitor the output of each phase of the formal software development process to evaluate its contribution to the SSHA. Problems are reported to the Managing Activity in time to support the ongoing phase of the software development process.

System Hazard Analysis

A System Hazard Analysis (SHA) is performed to:

- Verify system compliance with safety requirements contained in system specifications, and other applicable documents
- Recognize previously unidentified hazards associated with the subsystem interfaces and system functional faults
- Assess the risks associated with the total system design including software, and more specifically, the subsystem interfaces
- Recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels

The processes used in conducting the SHA will include an analysis that demonstrates the subsystems' interrelationships for:

- Compliance with specified safety design criteria
- Possible independent, dependent and simultaneous hazardous events, including system failures, failures of safety devices, common cause failures and events, and system interactions that could create a hazard or result in an increase in mishap risk
- Degradation in the safety of a subsystem, or the total system, from the normal operation of another subsystem
- Design changes that affect subsystems
- Effects of reasonable human errors
- Determining the potential contribution of hardware and software events (including those which are developed by other contractors/sources, or Commercial-off-the-Shelf [COTS] hardware of software), faults and occurrences (e.g., improper timing), on the safety of the system
- Confirming that the safety design criteria in the hardware, software and facilities specifications have been satisfied

- Determining that the method of implementing the hardware, software, facilities design requirements and corrective actions have not impaired or degraded the safety of the system, or introduced any new hazards

If no specific analysis techniques are indicated, or if the contractor recommends a technique other than those specified by the Managing Activity, the contractor will obtain Managing Activity approval of the process prior to performing the analysis. Types and techniques to consider for the SHA are:

- Fault Tree Analysis
- Failure Modes and Effects Analysis
- Event Tree Analysis
- Radiation Hazard Analysis
- HERO/HERF/HERP Analysis
- Interface Analysis

When subsystem software is being developed under DoD-STD-2167 or -2168, or MIL-STD-1679 or other development documents, the contractor will obtain, use and monitor the output of each phase of the formal software development process to evaluate its contribution to the SHA. Problems are reported to the Managing Activity in time to support the ongoing phase of the software development process.

Operating and Support Hazard Analysis

The Operating and Support Hazard Analysis (O&SHA) evaluates the activities of operational and support procedures as they potentially introduce hazards or risks into the system. It also assesses the adequacy of the (subsequently) amended procedures used in these areas to eliminate, control or mitigate identified hazards or risks.

The processes used in conducting the O&SHA examine procedurally controlled activities. Hazards resulting from the introduction of operations/tasks performed by persons shall be identified and evaluated considering:

- The planned system configuration/state at each phase of activity
- The facility interfaces
- The planned environments (or ranges thereof)
- The supporting tools or other equipment specified for use, including software-controlled automatic test equipment
- Operational/task sequence, concurrent task effects and limitations
- Biotechnological factors, regulatory or contractually specified personnel safety and health requirements
- The potential for unplanned events, including hazards introduced by human error

The human element is considered a part of the total system, receiving inputs and initiating outputs during the performance of this analysis. The O&SHA will specify the safety requirements at risk and determine alternatives needed to eliminate or control identified hazards, or to reduce the associated risk to a level that is acceptable under either regulatory or contractually specified criteria. The analysis identifies:

- Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods
- Changes needed in functional or design requirements for system hardware/software, facilities and tooling or support/test equipment, to eliminate or control hazards or reduce associated risks
- Requirements for safety devices and equipment, including personnel safety and life support equipment
- Warnings, cautions and special emergency procedures (e.g., egress, rescue, escape, render-safe, explosive ordnance disposal, back-out, etc.), including those necessitated by failure of a software-controlled operation to produce the expected and required safe result or indication
- Requirements for packaging, handling, storage, transportation, maintenance and disposal of hazardous materials
- Requirements for safety training and personnel certification
- Effects of non-developmental hardware and software across the interface with other system components or subsystems
- Potentially hazardous system states under operator control

Analysis types and techniques to consider for the O&SHA are:

- Maintenance Hazard Analysis
- Operating Hazard Analysis
- Emergency Procedure Analysis
- Maintenance Requirement Card (MRC) Review
- Technical Manual Review
- Fault Hazard Analysis
- Human/Machine Interface (HMI) Studies
- Physical Safety Audit
- Hazard & Operability Analysis
- Health Hazard Assessment
- Environmental Safety & Health

The O&SHA documents system safety assessment of procedures involved in system production, deployment, installation, assembly, testing, operation, maintenance, servicing, transportation, storage, modification, demilitarization and disposal.

Hazard Tracking and Risk Resolution

A single closed-loop hazard tracking system will be established to document and track hazards and their controls, providing an auditable trail of hazard resolutions. A centralized file, computer database or hazard log must be maintained. The hazard log will contain:

- The name of the safety engineer who generated the hazard report
- Descriptions of each hazard, including an associated hazard risk index
- The system/subsystem involved
- Events/mission phases associated with the identified hazard
- Hazard effects on personnel, equipment, platform and environment
- Controls recommended to reduce the hazard to a level of risk acceptable to the Managing Activity
- Initial, target and final risk assessment
- Status of each hazard and its control
- Traceability of the process on each hazard log item from initial identification to resolution at a level acceptable to the Managing Activity
- Identification of residual risk
- Action person(s) and organizational elements
- Final disposition/verification
- The signature of the Managing Activity person accepting the risk, which affects closure of the hazard log

Safety Assessment Report

The Safety Assessment Report is a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system, prior to the next contract phase or at contract completion. The SAR identifies all safety features of the hardware, software and system design, and identifies procedural, hardware- and software-related hazards that may be present in the system being acquired, including specific procedural controls and precautions that should be followed. The safety assessment summarizes:

a. The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived, including the definition of acceptable risk as specified by the Managing Activity.

b. The results of analyses and tests performed to identify hazards inherent in the system, including:

(1) Those hazards that still have a residual risk, and the actions that have been taken to reduce the associated risk to a level contractually specified as acceptable.

(2) Results of tests conducted to validate safety criteria, requirements and analyses.

c. The results of the safety program efforts, including a list of all significant hazards along with specific safety recommendations or precautions required to ensure the safety of personnel, property or the environment; the list of hazards should be categorized as to whether they may appear under normal or abnormal operating conditions.

d. Any hazardous materials generated by or used in the system, including:

(1) Identification of material type, quantity, and potential hazards.
(2) Safety precautions and procedures necessary during use, packaging, handling, storage, transportation and disposal (e.g., explosive ordnance disposal); include all explosives hazard classifications.
(3) After a launch, safety-related activity of expendable launch vehicles and their payloads, including deployment, operation, reentry and recovery (if required) of launch vehicles/payloads which do not attain orbit (either planned or unplanned).

Design Reviews

System safety engineers participate in the design reviews of all systems, subsystems, assemblies and components, as appropriate. The primary emphasis in the safety design reviews is on proactively designing-in safety features. During the conceptual phase, the main safety inputs to the design are the safety requirements to which the system design must adhere. As more design details become available, the safety design reviews determine what safety hazards exist or could exist under fault or abnormal conditions. For example, the presence of sneak circuits in an otherwise good design could cause hazards at unexpected times. Safety design reviews examine all possible scenarios and all conditions and environments, from the assembling of parts, to building subsystems, to testing systems, and finally to disposal of the equipment at the end of its useful life.

When done proactively, safety design reviews assist the designer in developing a safe system, and also ensure that the as-built system has all the required and necessary safety features installed and activated.

System Safety Task Scheduling

by Niles T. Welch, CSP
ASWaterman Inc.

The following list shows the chronological order of tasks in a system safety program. Note that some of these tasks may overlap.

- System Safety Program Plan
- Preliminary Hazard List
- Preliminary Hazard Analysis
- Health Hazard Assessment
- Safety Requirements/Criteria Analysis
- Subsystem Hazard Analysis
- System Hazard Analysis
- Operating and Support Hazard Analysis
- Safety Assessment
- Safety Review of ECPs, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver
- Safety Verification

Environmental Health and Safety Aspects

by David O’Keeffe
Raytheon Electronic Systems Company

As mentioned previously, the parameters defining system safety within the Department of Defense (DoD) changed dramatically upon the advent of acquisition reform and the publication of MIL-STD-882D. Traditionally, system safety focused on equipment and the real-time hazards it might present to the system or to personnel. In the beginning, system safety engineers paid little attention in their hazard analyses to potential effects (short and long term) on the environment, or on occupational health and safety. System safety engineering remained a distant cousin to environmental, safety and health (ESH) engineering. However, system safety always considered the effects of toxic or hazardous materials on personnel as part of the overall system safety analyses.

With the publication of DoD Directive 5000.2-R, system safety now includes consideration of environmental issues and compliance, hazardous materials management and pollution prevention. Today, a system safety engineer must be concerned with regulatory compliance issues, and must also have a working knowledge of federal and state statutes that govern environmental protection. These are the National Environmental Protection Act (NEPA) and the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA). Required as well, is a familiarity with international treaties designed to protect the environment, such as the International Convention for the Prevention of Pollution from Ships (MARPOL).

DoD 5000.2-R, “Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs,” is the top-level requirements document. It specifies that a Program Manager (PM) must institute a safety program that encompasses system safety and ESH disciplines. The pertinent sections of DoD 5000.2-R are:

> **5.2.10. — Environment, Safety, and Occupational Health (ESOH)**
>
> All programs, regardless of acquisition category and throughout their life cycle, shall comply with this section. The PM shall ensure a system design that can be tested, operated, maintained, repaired and disposed of in accordance with ESOH statutes, regulations and policies (collectively termed regulatory requirements), and the requirements of this section.
>
> The PM shall prepare a Programmatic ESOH Evaluation (PESHE) document early in the program life cycle (usually Milestone B*). The PESHE shall identify ESOH risks, contain a strategy for integrating ESOH considerations into the systems engineering process, delineate ESOH responsibilities and provide a method for tracking progress. The PM shall use the PESHE to identify and manage ESOH hazards, and to determine how to best meet ESOH regulatory requirements and DOD standards. The PM shall keep the PESHE updated over the system life cycle.
>
> The PM shall conduct ESOH analyses as described below. The PM shall provide details of these analyses, including supporting documentation, as part of the IPPD.**
>
> **5.2.10.1. — ESOH Compliance**

* Milestone B = Begin Development ** Integrated Product and Process Development

To minimize the cost and schedule risks over the system's life cycle that changing ESOH requirements and regulations represent, the PM shall regularly review ESOH regulatory requirements and evaluate their impact on the program's life-cycle cost, schedule and performance.

5.2.10.2. — National Environmental Policy Act (NEPA)

The PM is responsible for, and shall comply with, the NEPA (42 USC 4321-4370d90), the implementing regulations (40 CFR 1500-150891), and Executive Order (EO) 1211492, as applicable. The PM shall complete any analysis required under either NEPA or EO before the appropriate official may make a decision to proceed with a proposed action that may affect the human environment. The PM shall include an appropriate completion schedule for NEPA compliance in the acquisition strategy. The PM shall prepare NEPA and EO documentation in accordance with DoD Component implementation regulations and guidance. The Component Acquisition Executive (CAE) (or for joint programs, the CAE of the lead executive component) or designee, is the final approval authority for system-related NEPA and EO documentation. The PM shall forward a copy of final NEPA documentation to the Defense Technical Information Center for archiving.

90 Title 42, United States Code, Sections 4321-4370d, National Environmental Policy Act

91 Title 40, Code of Federal Regulations, Sections 1500-1508, "National Environmental Policy Act Regulations"

92 Executive Order (EO) 12114, Environmental Effects Abroad of Major Federal Actions

5.2.10.3. — Safety and Health

The Program Manager (PM) shall identify and evaluate safety and health hazards, define risk levels, and establish a program that manages the probability and severity of all hazards associated with development, use, and disposal of the system. The PM shall use and require contractors to use the industry and DoD standard practice for system safety, consistent with mission requirements. This standard practice manages risks encountered in the acquisition life cycle of systems, subsystems, equipment, and facilities. These risks include conditions that create significant risks 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.

The following policy applies to the acceptance of risk:

2. The PM shall formally document each management decision accepting the risk associated with an identified hazard.
3. "High Risk" hazards shall require CAE approval (lead executive component authority prevails for joint programs).
4. The acceptance of all risks involving explosives safety (see 5.2.10.6) shall require the appropriate risk acceptance authority to consult with the DoD Component's technical authority managing the explosives safety program.
5. "Serious Risk" hazards shall require Program Executive Officer approval.
6. "Medium Risk" hazards shall require PM approval.
7. The PM shall designate the approval authority for "Low Risk" hazards.

PL 91-59693 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.

93 Public Law 91-596, Occupational Safety and Health Act of 1970, as amended by Public Law 101-552, Section 3101, November 5, 1990

5.2.10.4. — Hazardous Materials Management

The PM shall establish a hazardous material management program consistent with eliminating and reducing the use of hazardous materials in processes and products (EO 1314894). The PM shall evaluate and manage the selection, use, and disposal of hazardous materials consistent with ESOH regulatory requirements and program cost, schedule and performance goals. Where the PM cannot avoid using a hazardous material, he or she shall develop and implement plans and procedures for identifying, minimizing use of, tracking, storing, handling, packaging, transporting, and disposing of such material.

94 EO 13148, Greening the Government through Leadership in Environmental Management

As alternate technology becomes available, the PM shall replace hazardous materials in the system through changes in the system design, manufacturing, and maintenance processes, where technically and economically practicable. To minimize costs, the PM shall, whenever possible, work with the contractor and other PMs to identify and test mutually acceptable alternatives. Defense Contract Management Agency shall coordinate this effort at contractor facilities under its cognizance. Where the Supervisor of Shipbuilding, Conversion and Repair, (SUPSHIP) provides contract management, the PM shall coordinate with SUPSHIP. The Contract Management Office, working in conjunction with the PM and IPT, shall help identify technical requirements, coordinate PM funding strategies, administer evaluation activities, and implement solutions.

5.2.10.5. — Pollution Prevention

The PM shall identify and evaluate environmental and occupational health hazards and establish a pollution prevention program. The PM shall identify the impacts of the system on the environment during its life (including disposal), the types and amounts of pollution from all sources (air, water, noise, etc.) that will be released to the environment, actions needed to prevent or control the impacts, ESOH risks associated with using the new system, and other information needed to identify source reduction, alternative technologies, and recycling opportunities. The pollution prevention program shall serve to minimize system impacts on the environment and human health, as well as environmental compliance impacts on program TOC. A fundamental purpose of the pollution prevention program is to identify and quantify impacts, such as noise, as early as possible during system development, and to identify and implement actions needed to prevent or abate the impacts.

In developing contract documents such as work statements, specifications, and other product descriptions, PMs shall eliminate the use of virgin material requirements, as practicable. They shall consider using recovered materials and reusable products. They shall further consider life-cycle costs, recyclability, the use of environmentally preferable products, waste prevention (including toxicity reduction or elimination) and disposal, as appropriate. (FAR 11.00295 and EO 1310196)

95 Federal Acquisition Regulation, Part 11 -- Describing Agency Needs, Section 11.002, “Policy”

96 EO 13101, Greening The Government Through Waste Prevention, Recycling, and Federal Acquisition (Replaces EO 12995 and EO 12873)

5.2.10.6. — Explosives Safety

All acquisition programs that include or support munitions, explosives, or energetics shall comply with DoD explosives safety requirements. The PM shall establish an explosives safety program that ensures that munitions, explosives, and energetics are properly hazard classified, and safely developed, manufactured, tested, transported, handled, stored, maintained, demilitarized, and disposed. The PM shall evaluate and manage the use and selection of energetic materials and the design of munitions and explosive systems to reduce the possibility and the consequences of any munitions or explosives mishap and to optimize the trade-off of munitions reliability against unexploded ordnance liability.

MIL-STD-882D reinforces this merging of the disciplines when it states:

3. This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the *management of environmental, safety, and health mishap risks* encountered in the

development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described herein conforms to the acquisition procedures in DoD Regulation 5000.2-R and provides a consistent means of evaluating identified mishap risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by the system user or customer) to the appropriate authority, and compliant with federal laws and regulations, Executive Orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision. Residual mishap risk associated with an individual system must be reported to and be accepted by the appropriate authority as defined in DoD Regulation 5000.2-R.

A.4.1 General. System safety applies 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. It draws upon professional knowledge and specialized skills in the mathematical, physical and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the environmental, safety and health mishap risk associated with a system. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given. The program manager and the developer must apply this emphasis during all phases of the system’s life cycle. A safe design is a prerequisite for safe operations, with the goal being to produce an inherently safe product that will have the minimum safety-imposed operational restrictions.

A.4.1.1 System safety in environmental and health hazard management. DoD 5000.2-R has directed the integration of environmental, safety and health hazard management into the systems engineering process. While environmental and health hazard management are normally associated with the application of statutory direction and requirements, the management of mishap risk associated with actual environmental and health hazards is directly addressed by the system safety approach. Therefore, environmental and health hazards can be analyzed and managed with the same tools as any other hazard, whether they affect equipment, the environment, or personnel.

Hazard Analysis

by Peter Rosa
Raytheon Electronic Systems Company

A Hazard Analysis (HA) is most easily described as an assessment of the results of each safety analysis. Though its content varies depending on the analysis being undertaken, all HAs follow the same general format.

An HA begins with an introduction that describes the purpose of the analysis, the overall governing instructions (i.e., statement of work) and the scope of the analysis.

Next, the System Description contains summaries of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions (including specifications and review documentation) is supplied as such documentation becomes available. The capabilities, limitations and interdependence of these components are to be expressed in terms relevant to safety, whereas the system and components are addressed in relation to their mission and operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. A discussion of the software used is also included in the System Description.

The Data and Reference Documents section consists of summaries used to determine the safety aspects of design features.

Safety Requirement and Criteria describes how the program operates under various conditions. It includes definitions, system safety precedence, hazard severity categories and probabilities, and hazard risk index/assessment criteria. Also included in this section are safety hazard categories, program-specific undesired events, safety-critical hardware configuration items (HWCIs), and computer software configuration items (CSCIs), interfaces and signals.

Hazard Analysis results consist of a summation (or total listing) of the HA's findings. Included may be a summary table highlighting the hazardous event, corrective action, corrective action status, and initial and final hazard risk indexes for each event. Another table can be provided to show the hazard risk index summary. This table will categorize and plot "Unacceptable," "Undesirable," "Acceptable with MA Review," and "Acceptable Initial Risk" and "Final Hazard Risk" indexes.

The Conclusions section describes any unresolved safety issues that have arisen from the analyses performed, and can suggest possible solutions.

Finally, Detailed Hazard Reports are attached as an appendix and contain all the hazard information specified for the hazard-tracking database. To complete the Safety Assessment Report, all hazard reports should be closed and signed-off by the appropriate personnel (as detailed in Section 3.1: System Safety Program Plan).

Professional Safety Organizations

by Alan Southwick
Abbott Labs/MediSense Products

There are many safety organizations across the country and around the world. The common bond among them is their desire to promote increased knowledge and a sharing of ideas and technologies within and across their various disciplines.

The System Safety Society is dedicated to the safety of systems, products and services through the effective implementation of the system safety concept. The Society's objectives are:

- To advance the art and science of system safety
- To promote meaningful management and technological understanding of system safety
- To disseminate advances in knowledge to all interested groups and individuals
- To further the development of the professionals engaged in system safety
- To improve public understanding of the system safety discipline
- To improve the communication of system safety principles to all levels of management, within all disciplines

Other safety organizations include the American Society of Safety Engineers (ASSE), the Safety-critical Systems Club in the U.K., the National Safety Council, and the Human Factors and Ergonomics Society. Groups such as the American Society of Mechanical Engineers (ASME) and the American Institute of Aeronautics and Astronautics (AIAA) have recognized the importance of safety within their industries, and have incorporated a safety adjunct into their organizations.

Highlighted below are some of the principal safety organizations, along with their contact information.

System Safety Society
P.O. Box 70
Unionville, VA 22567-0070
Phone: 540-854-8630
Fax: 540-854-4561
http://www.system-safety.org

The System Safety Society was chartered in California and subsequently incorporated as a non-profit professional organization in the District of Columbia. The Society has enjoyed a steady growth in numbers, scope and influence over the years. The membership now extends to over twenty different countries and a variety of professional occupations. Numerous local chapters have been formed throughout the U.S. which provide an opportunity for direct participation by interested members.

Human Factors and Ergonomics Society
P.O. Box 1369
Santa Monica, CA 90406-1369
Phone: 310-394-1811
Fax: 310-394-2419
http://www.hfes.org

The Human Factors and Ergonomics Society's (HFES's) mission is to promote the discovery and exchange of knowledge concerning the characteristics of human beings that are applicable to the design of systems and devices of all kinds. The Society advocates systematic use of such knowledge to achieve compatibility in the design of interactive systems of people, machines and environments to ensure their effectiveness, safety and ease of performance.

The American Society of Safety Engineers (ASSE)
1800 E. Oakton St.
Des Plaines, IL 60018
Phone: 847-699-2929 between 8:30 to 5:00 CST
Fax: 847-768-3434 24 hours
http://www.hfes.org

Founded in 1911, ASSE is the world's oldest and largest professional safety organization. Its 33,000 members manage, supervise and consult on safety, health and environmental issues in industry, insurance, government and education. ASSE has 12 divisions and 148 chapters in the U.S. and abroad.

Institute for Safety & Health Management
2004 Hatton Court
Columbia, MO 65203
Phone: 800-321-2910
Email: ishm@ishm.org
http://www.ishm.org

Through its certification program, the Institute for Safety and Health Management (ISHM) promotes the advancement of safety management through the application of management principles and the integration of safety into all levels and activities of management.
Safety is an integral part of the responsibilities of every function of line and staff management. ISHM identifies professionals who understand the role of safety in providing valuable support to organizations by preventing performance errors and controlling hazards that may result in loss-producing incidents, customarily called "accidents."

The organization's Certified Safety and Health Manager (CSHM) program recognizes the safety and health professionals who demonstrate knowledge of health and safety management skills and techniques through examination and experience. In addition to technical knowledge of safety and industrial hygiene, a successful safety and health manager must possess working knowledge of a broad range of business and financial principles, and an understanding of related issues such as hazard analyses, accident/incident investigations, safety audits/surveys, workers' compensation, product safety, environmental laws, quality and labor relations. The Certified Safety and Health Manager program is designed to provide recognition of those who can apply a broad range of health and safety management tools. For more information go to http://www.safetyhealthmanager.org/.

Society for Risk Analysis
1313 Dolley Madison Blvd.
Suite 402
McLean, VA 22101
703-790-1745
E-mail: sra@burkinc.com
http://www.sra.org

According to their Web site, the Society for Risk Analysis (SRA) provides an open forum for all those who are interested in risk analysis. Risk analysis is broadly defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk. The SRA's interests include risks to human health and the environment, both built and natural. They consider threats from physical, chemical and biological agents, and from a variety of human activities as well as natural events. They also analyze risks of concern to individuals, to public and private sector organizations, and to society at various geographic scales.

American Conference of Governmental Industrial Hygienists
1330 Kemper Meadow Drive
Cincinnati, OH 45240
Customer/Member Phone: 513-742-2020; Administrative Phone: 513-742-6163
Fax: 513-742-3355
http://www.acgih.org

The American Conference of Governmental Industrial Hygienists (ACGIH) is a member-based organization and community of professionals that advances worker health and safety through education and the development and dissemination of scientific and technical knowledge. Examples of this include our annual editions of the Threshold Limit Values (TLV) and Biological Exposure Indices (BEI), and work practice guides in ACGIH's Signature Series of Publications. For over 60 years, ACGIH has been respected for its dedication to the industrial hygiene and occupational health and safety industries.

Safety Publications

by Niles T. Welch
ASWaterman Inc.

Listed below are some of the safety journals and magazines published either online or in hard copy. This list is not complete, but represents a cross-section of materials available to the safety practitioner.

Journal of System Safety (System Safety Society)
http://www.system-safety.org

Professional Safety (American Society of Safety Engineers [ASSE])
http://www.asse.org

Human Factors and Ergonomics in Design (Human Factors and Ergonomics Society)
http://www.hfes.org

Occupational Health & Safety — The National Magazine for Safety, Ergonomic, and Occupational Safety
http://www.ohsonline.com

Management of Occupational Health, Safety and Environment (online journal)
http://www.ohse.co.uk

Rad Journal — The Radiation Safety and Processing Magazine
http://www.radjournal.com

Safety News
http://www.safetynews.com/news/news.html

Chemical Health and Safety (American Chemical Society Division of Chemical Health and Safety)
http://dchas.cehs.siu.edu

Flying Safety
http://www-afsc.saia.af.mil/magazine/htdocs/fsmfirst

Utility Safety
http://www.utilitysafety.com

SafetyLine (online)
http://www.safetyline.wa.gov.au/

National Safety Council Family Safety & Health
http://www.nsc.org/pubs/fsh

Industrial Safety and Hygiene News (online)
http://www.ishn.com/

Safety Systems (Safety-critical Systems Club, U.K.)
Newsletter published three times yearly

Becoming a Board Certified Safety Professional (CSP)

by Alan Southwick
Abbott Labs/MediSense Products

The following material was obtained from the Board of Certified Safety Professionals' (BCSP) Web site. For further information, please go to: http://www.bcsp.org.

Board of Certified Safety Professionals
208 Burwash Avenue
Savoy, Illinois 61874
Phone: 217-359-9263
Fax: 217-359-0055

AM I ELIGIBLE FOR THE CERTIFIED SAFETY PROFESSIONAL (CSP) CERTIFICATION?
Take this exam to find out if you may be eligible for the CSP certification. This test is for informational purposes only.

1. Do you have a college degree from an accredited* institution?

YES _____ NO ______

2. An Associate's degree in safety?

YES _____ NO ______

3. Bachelor's in any field?

YES _____ NO ______

4. Can you provide proof of your degree?

YES _____ NO ______

5. Is the primary function of your position safety?

YES _____ NO ______

6. Is the position at the professional level?

YES _____ NO ______

7. Is the primary responsibility the prevention of harm to people and the environment, rather than responding to harmful events?

YES _____ NO ______

8. Does the safety position require at least 900 working hours per year?

YES _____ NO ______

9. Does the position have breadth of duties?

YES _____ NO ______

* The Council on Higher Education Accreditation (http://www.chea.org) is the accrediting body referenced.

If you answered "YES" to all of the above questions, you may be eligible for the CSP examination. All eligibility is determined by the Board of Certified Safety Professionals after careful review of submitted applications. This short quiz does not certify your eligibility.
If you answered "NO" to any of the questions above, you may not be eligible for the CSP Certification. Contact a customer service associate at BCSP for further information.

Frequently Asked Questions

Q: How do I qualify for the Certified Safety Professional title?
A: Apply to the Board of Certified Safety Professionals;
Meet an academic requirement;
Meet a professional safety experience requirement;
Pass the Safety Fundamentals Examination;
Pass the Comprehensive Practice Examination.

Q: Where do I get the application?
A: The application is available free of charge at
http://www.bcsp.org/csphdbk/csp_handbook.htm.
You can also find an application form in the Application Guide available from BCSP.

Q: Do I need to have a college degree to be eligible?
A: Yes, a CSP candidate must meet one of the following minimum educational requirements:
An Associate's degree in Safety and Health, or a Bachelor's degree in any field.

Q: Can I use more than one undergraduate degree for credit?

A: A candidate can use only one undergraduate degree for the academic requirement. The degree yielding the highest value is used when there is more than one degree. Associate degrees earn one half the credit of a Bachelor's degree in the same field.

Q: Can I get credit for a graduate degree?
A: Yes, a Master's degree earns one fourth the credit allowed for a Bachelor's degree in the same field. A Doctoral degree earns one half the credit allowed for a Bachelor's degree in the same field. Graduate degrees count toward the experience requirement. A graduate degree does not waive acceptable proof to BCSP of having met the minimum degree requirement.

Q: Will a non-U.S. degree be considered for credit?
A: Yes. However, degrees from foreign colleges and universities are evaluated for U.S. equivalency, and BCSP requires proof that a degree was awarded.

Q: Do continuing education courses and certificate programs count toward the academic or experience requirement?
A: No, continuing education courses and certificate programs will not be considered for credit.

Q: How much safety experience must I have?
A: The CSP candidate must have at least four years of "acceptable professional safety experience."

Q: What is "acceptable professional safety experience"?
A: To be considered, each job position must meet all of the following criteria:

Professional safety must be its primary function (i.e., at least 50% of the position's duties must be safety).

The position's primary responsibility must prevent harm to people and the environment, rather than respond to harmful events.

The position must require at least 900 working hours in a year.

The position must be at the professional level.[**]

The position must have breadth of duties.[**]

[**] Please refer to http://www.bcsp.org/csphdbk/hdbk_c2.htm, "The Experience Requirement," for further explanation and additional information.

Q: How is credit determined?
A: Points are assigned to academic degrees and also to experience, with an ABET-accredited Bachelor's Safety degree receiving the highest point total of 48. Professional safety experience earns one point per month of acceptable safety experience. Graduate degrees count toward experience.

Q: How many points are required to take the examination?
A: 48 points are required for the Safety Fundamentals Examination.

96 points are required for the Comprehensive Examination.

Q: How is the total calculated?
A: Academic points + experience points = total eligibility points awarded.
Detailed information on the application process may be found at
http://www.bcsp.org/csphdbk/csp_handbook.htm.
All information may be downloaded at no cost.

Planning a Career in System Safety

by Ronald Bartos
Raytheon Electronic Systems Company

It's probably a safe bet to say that a majority of professionals in system safety did not begin their careers with the intention of being in this field. Most start out in another discipline; yet for one reason or another, they gravitate toward the field of system safety. However, if you know at the onset of your career that you want to become a system safety professional, you will be able to chart a logical and progressive career course to achieve your goal sooner. Whether your path is by design or by chance, many aspects of your career will become the foundation needed to build your reputation as a system safety professional.

A college education is the first requirement. There are universities that offer Bachelor's and post-baccalaureate degrees in safety and system safety. Depending on the type of system safety career you want to pursue, choose whether to receive a Bachelor of Arts (B.A.) or a Bachelor of Science (B.S.) degree. A B.A. is more appropriate for the management or behavioral aspects of system safety, whereas a B.S. degree is appropriate for the scientific and/or engineering arenas.

Firms looking for system safety professionals require a B.S. degree in a technical or scientific area such as engineering, chemistry or physics. It is helpful for candidates with a B.A. degree to demonstrate an understanding of these subjects as well. The key to the making of a system safety engineer is the acquired knowledge and proficiency to comprehend, define and solve complex problems.

Develop familiarity and experience in several systems areas. Knowledge of systems involving mechanics, physics, electrical technology, materiels, biology, chemistry and software will give you a desirable and diversified background. Volunteer for advancements that require you to expand your knowledge. Lessons learned from one area of expertise are often readily transferable to another. Strive to understand how systems are controlled, and learn how subsystems interact. Be conversant in several engineering disciplines. It pays to know a little bit in a lot of areas to avoid getting locked into one industry sector. A broad educational and experience base makes you more flexible in the job market, and can insulate you from layoffs and reorganizations. Having earned an M.S. or Ph.D. is a decided advantage when being considered for a promotion, or applying for a new position.

Once you have garnered a few years of experience in your chosen discipline, consider obtaining certification as a system safety professional The Certified Safety Professional (CSP) designation is a distinction that lends professional credibility to you and your organization, and will be recognized by potential clients in all engineering fields.

Here are some strategies to help your career development as a system safety professional:

- Communicate: initiate dialog with managers and coworkers at all levels. Develop and practice communication skills, both oral and written. Learn the art of negotiation and persuasion.

- Set goals: prepare a detailed career development timeline for the next ten years, outlining the direction you would like to take, and the goals you hope to achieve. Give it to your manager.
- Be sociable: attend meetings and luncheons; develop a rapport with your coworkers. Volunteer to be on a task force or committee. Join safety societies and actively participate. Network to find out what other system safety professionals are doing, and how you can help each other succeed. Get a mentor; and later in your career, be a mentor.
- Stay current in your field: take continuing education courses and seminars, go to conferences, participate in courses offered by your company. Learn new skills: develop your abilities with a new computer application.
- Get published: demonstrate your knowledge and achievements by writing about a project at work. Publish articles in *Journal of System Safety*, and present a paper at the annual International System Safety Conference.
- Be self-motivated: think of yourself as self-employed and take the responsibility of managing your own career. Use your time effectively. Assess your skills and identify areas of improvement that will advance your position and career.

Everyone’s system safety career takes different twists and turns. With the proper education, experience and use of the strategies listed above, you can achieve success and fulfillment in the system safety career of your choice.

Source:
Anderson, Sandy. “Maintaining Your Career Momentum,” *Leaders Online.* Volume One, Issue Two, December 2000.

System Safety Training

by David Rice
Raytheon Electronic Systems Company

Continuing education and an ongoing awareness of industry-wide technical advancements are vital if the system safety practitioner is to effectively achieve and maintain professional excellence. Through basic and advanced degree studies, as well as periodic “refresher” training, the safety professional first attains, then maintains, technical proficiency. Within the System Safety Society (SSS), the Operating Vice President for Education is responsible for publicizing the safety-related curricula and training offered by educational institutions and other organizations.

The American Society of Safety Engineers (ASSE, www.asse.org) maintains a listing of colleges and universities with safety-related offerings, complete with the names of contact persons, addresses, telephone numbers and the types of degrees offered. In addition, the Accreditation Board for Engineering and Technology (ABET, www.abet.org) is responsible for the accreditation of specialized educational programs in engineering, engineering technology and related fields.

System safety topics are typically taught in seminar or abbreviated-course format. The University of Washington offers a nine-day System Safety Management course as part of its Engineering Professionals program. The course provides a review of system safety management principles and engineering techniques. The university also offers a 10-day System Safety Reliability Analysis course that introduces methods of identifying risk and controlling hazards in complex systems. Some private organizations also provide training that prepares safety personnel for the various certification examinations offered by the Board of Certified Safety Professionals (BCSP, www.bcsp.com). Training usually includes seminars, home study and computer-based training for the Associate Safety Professional (ASP), Certified Safety Professional (CSP), Occupational Health and Safety Technologist (OHST), and Construction Health and Safety Technician (CHST) examinations.

Industry-related journals and safety conferences provide another valuable source of continuing education. *Journal of System Safety* (www.system-safety.org/JSS/JSS.html) is published quarterly by the SSS. The journal provides technical information and news of topical interest to safety professionals. The annual International System Safety Conference (ISSC) is a week-long event featuring the latest in safety products, services, technologies and software for system safety practitioners. Attendees are offered a generous cross-section of information, trends and future forecasts as they become better informed about system safety as a worldwide discipline. Other annual conferences include the European-based Safety-critical Systems Symposium and the U.S. Navy’s Weapons System Safety Symposium.

Conclusion

by Ann S. Waterman
ASWaterman Inc.

It is said that the only thing certain is change. As technology evolves, so does our need to keep tabs on it, and to ensure that our need for advancements in technology is always tempered by our need for safety. As system safety practitioners, that places an awesome responsibility in our hands. But it is one that we welcome and value tremendously.

In assembling this book, we hope to lay the groundwork for many of its readers to consider a career in system safety. We will continue to update and expand its pages, just as we expand our system safety knowledge and practice every day. In the meantime, we are eager to answer your questions and provide any guidance that you need. Please feel free to contact the New England Chapter of the System Safety Society in care of David Rice (David_E_Rice@raytheon.com or 401-842-5535), or visit our Web page at http://www.aswaterman.com/ss2.

We hope to see you here again soon.