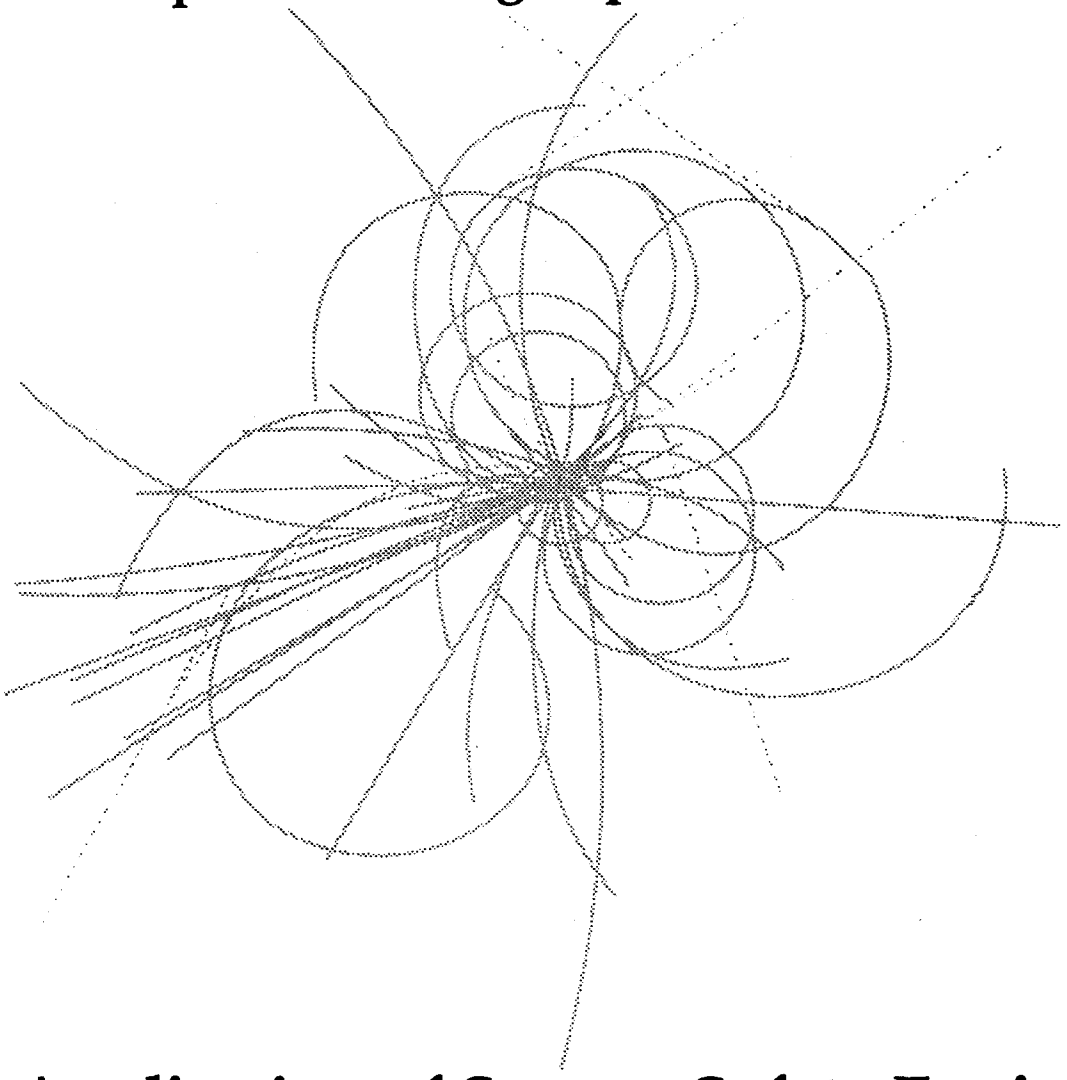
SSCL-396

SSCL-396

Superconducting Super Collider Laboratory



Application of System Safety Engineering Techniques for Hazard Prevention at the Superconducting Super Collider

B. L. Hendrix

March 1991

SSCL-396

APPLICATION OF SYSTEM SAFETY ENGINEERING TECHNIQUES FOR HAZARD PREVENTION AT THE SUPERCONDUCTING SUPER COLLIDER*

B. L. Hendrix

Project Managment
Superconducting Super Collider Laboratory†
2550 Beckleymeade Ave.
Dallas, TX 75237

March 1991

---

*Presented at the Third International Industrial Symposium on the Superconducting Super Collider, March 13-15, 1991.

†Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC02-89ER40486.

APPLICATION OF SYSTEM SAFETY ENGINEERING TECHNIQUES FOR HAZARD PREVENTION AT THE SUPERCONDUCTING SUPER COLLIDER

Barry L. Hendrix

Project Management Division
Superconducting Super Collider Laboratory*
2550 Beckleymeade Avenue
Dallas, Texas 75237

Abstract: A primary goal of the Superconducting Super Collider Laboratory (SSCL) is to establish an exemplary safety program. Achieving this goal requires leadership, planning, coordination, and technical know-how. To ensure that safety is an inherent part of the design, the Environment, Safety and Health Office employs a systems engineering discipline and process known as System Safety. The goal of System Safety—hazard prevention—is accomplished by analyzing systems to identify hazards and to evaluate design and procedural options and countermeasures to prevent, eliminate, mitigate, or control hazards and risks. Establishment of safety and human factors design criteria at the outset of the project prevents unsafe designs and safety violations, reduces risks, and helps in avoiding costly design changes later. This process requires a considerable amount of coordination with a variety of technical disciplines and safety professionals to integrate methods of hazard prevention, mitigation, and risk reduction throughout the system life-cycle.

INTRODUCTION

System Safety is an engineering management science that is being prudently implemented and practiced at the Superconducting Super Collider Laboratory (SSCL). System Safety is the arm of Project Management that works closely with the Environmental, Safety and Health Office on all safety planning and technical safety matters. System Safety is responsible for coordinating safety engineering efforts within each division at the SSCL. Other responsibilities within System Safety include Human Factor Engineering and Safety Risk Management. This paper provides an overview of the philosophy of System Safety and the proven safety engineering and management approaches that are used to influence safe design and operation of the SSC. Proven hazard analysis and risk assessment processes are presented.

*Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC02-89ER40486.

Definition and Purpose

The principal objective of a System Safety program is to ensure that safety, consistent with SSCL mission requirements, is designed into systems, subsystems, equipment, facilities, and their interfaces and operation. A *system* may comprise not only facilities and technical systems hardware, but also the software, interface controls, man-machine interface, operators, training, safety standards, guidelines and operating procedures. In accordance with System Safety philosophy, the formal textbook definition of *system* is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. (The elements of this composite entity are used together in the intended operational or support environment to perform a given task or to achieve a specific production, support, or mission requirement). From a System Safety perspective, the word *safety* means freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss destruction of equipment or property, or damage to the environment. *System Safety* can be defined as.the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life-cycle. Therefore, a *System Safety program* is the combined management and engineering tasks of planning, implementing, and establishing system-specific requirements to identify system hazards and impose design and management controls to prevent mishaps by eliminating hazards or reducing the associated risk to acceptable levels. For this to be effective, a systematic process is required to accomplish specific safety tasks.

The Process of System Safety

System Safety is not synonymous with Safety Systems, which is a safety design configuration. Instead, one should think of System Safety as the systematic safety process by which those safety systems are prudently and carefully planned and designed to meet their intended purpose. From a systems engineering perspective, System Safety is an effective process that streamlines the safety effort by focusing on essential tasks required to ensure adequate hazard mitigation and risk management. It is a flexible approach used throughout domestic and international industry and is in accord with the current philosophy of the SSC " to do whatever it takes to ensure systems are safe".

System Safety Engineering is the scientific and engineering approach to solving safety problems of a technical nature..The primary mission is hazard prevention. In order to prevent, eliminate, control, or mitigate specific hazards associated with design and operation, the hazard must first be clearly identified and evaluated for effects, severity, frequency of occurrence,.and associated risk. Department of Energy (DOE) and Department of Defense (DOD) experience has shown that risk reduction—through safety analyses and hazard prevention, elimination and control processes—is most effective when implemented early in the system life-cycle.

Early identification and elimination or control of an unacceptable hazard or risk decreases the potential negative impact on the program and the likelihood of a costly retrofit. "After the fact" safety design changes due to negligence, oversight, and the like can be extremely expensive. Designing safety into a system can reduce the overall life-cycle cost and increase the system's reliability and availability. Therefore, it is the responsibility of management to ensure that a formal safety engineering or a System Safety Program is developed so that safety is designed "before the fact" into systems in a logical and efficient manner.

Responsibilities of Safety Professionals

Safety professionals are responsible for preventing injury to personnel and damage to equipment. To ensure safety, these professionals must have the authority to make safety decisions and to influence safe designs and operations. This requires planning and persistence.

One responsibility of all safety professionals is to ensure that engineering and safety standards are not compromised. According to current law, criminal sanctions can now be applied to individuals when willful violations of federal Occupational Health and Safety Administration (OSHA) standards result in a death of an employee. This means that safety professionals are obligated to do not only what is ethical and moral, but what is legally mandatory as well. The phrases " Best Management Practices" or "Most Stringent Guidelines" are not without meaning, but they are not always the right answer. There are practical and budgetary limits to what can be incorporated into a design. Therefore design tradeoff studies may be appropriate, and less stringent approaches may be applicable as long as safety is not compromised. Many design codes and standards may apply to a given project, but taken as a whole, they may yet leave some safety gaps. Codes and standards must be thoroughly evaluated by safety personnel before they are recommended to solve safety problems. In some cases the solution may lie outside the code. It is the responsibility of safety professionals to emphasize the design of systems to operate safely. But they should not blindly adhere to a safety design that yields no safety advantage. While safety professionals cannot violate applicable laws or overlook required minimum standards for safe designs, they should never stand behind a code or regulation without first thoroughly investigating and assessing its applicability.

The degree of safety achieved in a system depends directly on management's emphasis on safety during conceptual planning and design, construction, and operation. Management must see that mishap risk is understood and that risk reduction is always considered in the management review process. The consequences of personnel injury, equipment loss, system downtime, and environmental damage must be fully realized from a legal or liability perspective and from an ethical perspective. DOE and the SSCL are committed to the goal of building the safest system possible within the constraints of time, technology, and budget.

DOE Authorization

DOE Order 5481.1B Change 1, 5-19-87, Safety Analysis and Review System, clearly defines the purpose, policy, general requirements, and guidance for safety analysis, review, and assessment of DOE operations. Section 5, paragraph k of DOE 5481.1B references the use of MIL-STD-882B System Safety Program Requirements."which provides detailed information for organizing, developing, and implementing system safety programs tailored to individual program needs." As authorized by DOE 5481.1B, MIL-STD-882B can be tailored to a broad variety of applications and adapted as appropriate to various types of technologies and industries. It is currently used as a general guideline for implementing an effective System Safety Engineering program at the SSCL.

Organization

Although System Safety is a process, it is also a well-recognized engineering and technical safety management field. At the SSCL the System Safety Manager is assigned to the Project Office and is asked to provide technical interface assistance to the Assistant Director of Environmental, Safety and Health. System Safety, commonly referred to as Project Safety, interfaces closely with the line organization Operational Safety Officers, Safety Coordinators, and safety engineering staff of each division on all technical safety issues. System Safety reports administratively to the Manager of Systems Engineering.

Interfaces

System Safety provides integration assistance on all safety-related matters associated with SSCL design and operation. Provision of this service requires that safety tasks and interfaces be clearly identified. An effective safety program can be accomplished only with the full support and cooperation of upper management and by application of a broad variety of engineering, design, and support disciplines throughout the organization. In addition to direct support to Project Management, technical interface and frequent coordination with the Environmental, Safety and Health Office is required to ensure compliance with DOE orders and federal, state and local safety laws or standards. A close working relationship among System Safety and Systems Engineering Analysts and the support disciplines of Reliability, Maintainability, Availability, and Quality Assurance is required to ensure that the safety process is accomplished and implemented. Continuous interface with the safety officer, safety engineers, and other technical disciplines in all divisions is necessary to coordinate safety efforts and to ensure that the System Safety process of hazard prevention, elimination and control is working. This technical liaison will enhance the overall safety process and will help open channels of communication on safety issues. System Safety provides a technical and managerial interface with all divisions to ensure timely coordination of safety efforts associated with the highly complex and integrated task of developing the SSCL Safety System.

SYSTEM SAFETY TASKS

The following tasks will be performed to ensure that System Safety can effectively influence the safety design of the SSCL.

- Implement a formal System Safety program
- Develop a System Safety and ES&H program plan
- Establish safety liaison with SSCL associates, contractors, vendors
- Review applicable safety policies, procedures, standards and guidelines
- Interface with ES&H and support safety mission
- Develop computerized hazard tracking and risk resolution database system
- Develop test and evaluation safety plan
- Develop System Safety progress summaries (submit to project management)
- Evaluate/recommend requirements for System Safety staff
- Develop preliminary hazard list of top-level safety concerns
- Conduct preliminary safety analysis/train engineers on safety analysis process
- Develop preliminary hazard analysis (PHA) reports (submit to DOE)
- Perform system/subsystem hazard analysis of technical systems design
- Conduct human engineering/human factors studies (as required)
- Perform operating & support hazard analysis of Safety System
- Assist ES&H in occupational health hazard assessments
- Develop safety verification guidelines

- Develop operational safety procedures
- Assist ES&H and divisions in developing and conducting safety training
- Perform assessments of Safety Systems and operations
- Perform safety design criteria compliance assessments
- Review engineering changes, deviation/waiver for safety
- Communicate, coordinate, elevate internal System Safety issues
- Assist safety consultants–university outreach program (as required).

Safety Design Criteria

DOE 6430.1A General Design Criteria is the primary document used to identify acceptable safety criteria for facilities. Technical systems and safety systems in many cases require specific engineering standards. During the development and operation of this project System Safety will assist engineers and engineering support personnel in defining acceptable design criteria for incorporation into requirements documents, specifications, and operating procedures. In some cases, this is being coordinated through the use of appointed safety committees that assess the applicability of various codes, regulations, and engineering standards. In many cases, specific safety design requirements are analyzed and prudent judgment is used to ensure that safety is inherent in the design. System Safety assists systems engineers and designers during the development of specifications. Close liaison with the SSCL Engineering Standards Department is also required.

Many design standards (e.g., ANSI, IEEE, ASME, and NFPA) that are used for a broad variety of facilities, equipment, and technical systems design have safety-related criteria that can be evaluated to determine applicability to the SSCL design. From a safety engineering perspective, many widely used and proven industrial codes and standards are acceptable design criteria, but some sections pertaining to DOE special facilities, such as nuclear or weapons plants, are not applicable to the specific technology of the SSCL. These should be evaluated on a case-by-case basis to determine whether to consider them as requirements or as flexible guidelines. Use of applicable DOE orders and specific commercial engineering standards and guidelines help reduce risks and help ensure that optimal engineering and safety design practices are followed.

Risk

The best safety design is one that has the least risk. The System Safety definition of *risk* is.the quantitative or qualitative expression of possible loss in terms of hazard severity and hazard probability that a hazard will cause harm and the consequences of that event. Safety design criteria are intended as acceptable standards to reduce risks to acceptable levels. Although there are other methods of mitigating hazards, such as training, protective equipment, warning devices, and operational safety procedures, they are seldom adequate substitutes for safe design. Whenever possible, within the constraints of technology, time and cost, severe hazards should be prevented, eliminated, or controlled through design. Inherently safe designs don't just happen—they are planned. If safety is not a primary consideration early in the design phase, it is usually a costly afterthought. Experience has proven that unsafe designs are unacceptable. Safety must be built into systems, not added as an afterthought. Residual Risk is that risk associated with significant hazards for which there are no control or mitigation measures.

Hazard Analyses

The hazard analysis process is the backbone of System Safety and is used to identify hazards. A hazard cannot be eliminated or controlled unless it is first clearly identified. Truly effective safety systems and design safeguards cannot be conceptualized, effectively designed, or implemented early in a program planning stage unless system safety processes are employed. Methods for minimizing, mitigating, or controlling hazards either through design or through methods such as placarded warnings, cautions, notes, and safety training are possible only when the specific hazard and all of its effects are thoroughly analyzed and evaluated. For this reason the hazard analysis process must be employed as early in the system design stage as possible. Quantitative hazard analyses are somewhat similar to Reliability Failure Modes Effect and Analysis (FMECA). However, a hazard analysis takes the process a step further and assesses the safety implications, safety effects, hazard severity, and frequency of occurrence classifications and determines which criteria or actions are required to minimize identified hazards and risks. There are many types of hazard analyses including Preliminary Hazard Analysis, System/Subsystem Hazard Analysis, Operating and Support Hazard Analysis, Fault Hazard Analysis, Fault Tree Analysis, Software Hazard Analysis, and Consequences Analysis. Since the Preliminary Hazard Analysis is an initial step in influencing a safety program, it is the most common analysis.

Preliminary Hazard Analysis

The SSCL Project Management Plan (PMP) establishes the requirement for a Preliminary Hazard Analysis (PHA) Report, which is currently being developed. The PMP describes the PHA as.a" document (that) lists and discusses the procedures dealing with the hazards associated with the construction and testing of the SSC". MIL-STD-882B, which is endorsed by DOE 5481.1B, says the purpose of the PHA is to "identify safety critical areas, evaluate hazards, and identify the safety design criteria used".

The PHA is widely recognized as a proven safety approach used by the electronics industry, petrochemical industry, aircraft and aerospace companies, weapon system engineering firms and defense contractors, and various government agencies associated with complex systems. The PHA is an initial risk assessment of a concept or system. To be effective the PHA should begin during the concept exploration phases or earliest life-cycle phase of the program so that safety considerations are included in tradeoff studies and design alternatives. Based upon the best available data, including mishap data from similar systems, hazards associated with the proposed design or functions shall be evaluated for hazard mishap severity, hazard mishap probability, and operational constraint. The PHA also addresses safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the appropriate safety-managing agency. At a minimum, the PHA must consider the following for the identification and evaluation of hazards:

- Hazardous components (e.g., flammables, explosives, chemicals, toxic substances, hazardous construction materials, electrical, pressure systems, cryogenics, and all energy sources).
- Safety related interfaces (e.g., material compatibilities, electromagnetic interference, inadvertent activation or lack of control).
- Environmental constraints (e.g., drop, shock, vibration, temperature, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including electrical radiation).

- Operating, test, maintenance and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks analyses, task requirements, effects of factors such as equipment layout, lighting requirements, potential exposure to toxic materials and hazardous substances, effects of noise or radiation on human performance, emergency or environmental waste disposal, access and egress, operational safety procedures and safety training).
- Facilities and equipment (e.g., provisions for all phases of operations including daily operations, special operations, maintenance, testing and training).
- Safety related equipment, safeguards, and possible alternative approaches (e.g., interlocks, system redundancy/ back-up devices, hardware or software fail-safe design considerations, subsystem protection, fire detection and suppression systems, personal protective equipment, life support systems and equipment, alert devices, warning devices, detection equipment, ventilation, noise or radiation barriers, placarded warnings).

Hazard Classifications

During the hazards analysis process, risks are determined based upon hazard severity and probability. The following hazard classifications are adapted from MIL-STD-882B and are currently being used at the SSC to determine levels of risk:

Severity of Consequences

I (Catastrophic)—death, equipment loss > $500K, > 4 months downtime.

II (Critical)—severe injury, Loss $100–500K, > 2 weeks downtime.

III (Marginal)—minor injury, Loss $1–100K, 1 day to 2 weeks downtime.

IV (Negligible)—no injury, Loss < $1K, < 1 day downtime.

Probability of Mishap

A (Frequent)—likely to occur repeatedly during the life-cycle of system.

B (Occasional)—likely to occur several times in the life-cycle of system.

C (Occasional)—likely to occur sometime in life-cycle of system.

D (Remote)—not likely to occur in life-cycle of system, but possible.

E (Improbable)—probability of occurrence cannot be distinguished from zero.

F (Impossible)—physically impossible to occur.

Risk Zones

1 (High)—imperative to suppress to a lower level: IA, IB, IC, IIA, IIB are unacceptable (High) risk.

2 (Medium)—operation requires written, time-limited waiver by management: ID, IIC, IIIA, IIIB require mitigation action.

3 (Low)—operation permissible: IE, IF, IID, IIE, IIF, IIIC, IIID, IIIE, IIIF and IVA-F are acceptable.

Preliminary Hazard Analysis at the SSC

A Preliminary Hazard Analysis is currently being conducted at the SSC using the System Safety approach. Systems specialists, design engineers, and engineering support personnel assigned to each division are learning how to conduct hazard analyses of the designs for which they are responsible. With oversight from the SSC ES&H Office, the initial PHA was developed by the Project System Safety Office assisted by safety coordinators from the Accelerator, Magnet, Conventional Construction, and Physics Research divisions. In a coordinated effort, 29 engineers and technical personnel conducted first-order hazard analyses associated with over a dozen segments of the SSC design, including Magnet Test Lab (MTL), Magnet Development Lab (MDL), Accelerator Surface String Test (ASST), Injectors, Collider RF Systems, Electrical Systems, Cryogenic Systems, Quench Protection Systems, Conventional Construction, Facilities, and Laboratory Spaces. The PHA is a continuous process, and the document will be updated as new designs and technical requirements evolve. At the end of February 1991, an initial total of 164 hazards were identified and documented. Recommended actions and mitigation methods for each hazard are being planned. Mitigation actions to reduce risk to acceptable levels fall in the following categories:

- Incorporate new or retain current design features
- Develop operational safety procedures
- Conduct specialized safety training
- Develop safety policies
- Conduct inspections
- Comply with OSHA requirements
- Incorporate NFPA codes
- Impose restrictions
- Use protective equipment
- Perform tests
- Plan logistics
- Comply with applicable codes
- Incorporate safeguards
- Provide monitoring equipment
- Enforce policies
- Comply with laws, engineering standards, regulations, and safety rules.

Hazard Tracking

One of the most important areas of an effective System Safety program is documentation of hazards and of methods for resolving risk. A hazard tracking and risk resolution process helps ensure that unacceptable or highly undesirable hazards are documented, evaluated, tracked, and formally proposed to management for action. This systematic process is similar to safety action item identification and assignment of responsibility. An effective hazard tracking system is kept on a centralized database that is accurately updated each time hazard status is changed. A project the size of the SSCL will

have literally hundred of identified hazards, many of which must be individually tracked until the associated risks are minimized or reduced to an acceptable level. A paper file is not the most efficient or reliable method for hazard tracking. A computerized database log and track hazards and risks is currently being developed at the SSC.

Risk Assessments

Perhaps one of the most misunderstood areas of safety is risk assessment. Some professionals outside the safety field believe they are qualified to assess risks without all of the facts. A *Risk Assessment* is a comprehensive evaluation of the risk and its associated impact. Risk Assessments, sometimes called safety assessments, are performed as part of the hazard analysis process after hazards are systematically identified and hazardous effects are determined. Risk Assessments are thorough safety evaluations of hazard severity and probability, with a determination of acceptability or unacceptability based upon mitigation actions to reduce risks. Acceptability or unacceptability of a concept, scheme, design or operation is based upon facts such as the environment, conditions, scenarios, human factors, operation, user interface or inherent quality/reliability or safety procedure. Equipment or product integrity, the man-machine interface, potential for human error, types of equipment failures, safety design features, and other factors must be studied to determine risk. To simply determine that a hazard is potentially catastrophic or critical to humans or equipment is not enough. If there is a potential hazard, there must also be a determination of the probability and frequency of mishap occurrence. The methods for determining quantitative risks can be very complex, based as they are upon detailed knowledge of all of the facts and statistics linked to conditions and phases of operation. Often a conservative estimate or prediction, based upon a variety of factors, is the only reasonable way to assess risks. Sometimes research and development studies, computer models, simulations, statistics, reliability data, fault tree analyses, consequence analyses, or historical data associated with similar designs are the best methods for assessing risks. Some risks are reasonably simple to assess; others are very complex and difficult to assess. In the latter cases, extra time and resources may be required. The system/subsystem and all interfaces must be systematically analyzed based upon best available data. Risks are evaluated on the basis of hard facts rather than on an assumption or educated guess. Safety decisions must be justified

Risk Resolution

Once hazards and risks are determined, they must be closely tracked and resolved. An effective process to track hazards and to develop risk resolutions is needed. Recommended actions are based upon the risk assessment.. Safety professionals are responsible for determining the best method of preventing, eliminating, or controlling hazards within the constraints of cost and schedule. Tradeoffs may be required; in some cases "good enough" and "safe" may be appropriate. Specific recommendations for reducing risks must be clearly documented and approved by appropriate management. Options may include:

- Design changes to prevent hazards
- Safety features, interlocks, barriers
- Fail-safe devices
- Monitors, alarms, and control systems
- Redundant systems
- Emergency procedures and precautions

- Operational safety procedures
- Safety training
- Preventive maintenance, inspection ,and test
- Warning devices, placards
- Operating limitations, restrictions
- Other prudent mitigation methods.

As previously noted, once a risk has been determined to be borderline or unacceptable in accordance with established criteria, it must be resolved. Hazards and risks do not simply disappear, and sometimes they are hidden. A safety or reliability analyst may fail to identify a hazard or combination of hazardous conditions. A residual risk—a risk that has not been resolved—is usually unacceptable. During the hazard analysis process, hazards are identified and assessed, and actions are recommended to reduce unacceptable hazards to an acceptable level. Risks can sometimes be reduced by adding design features, safeguards, redundancies, back-up systems or safety devices. Such a course may not be economically feasible beyond the preliminary design stage. Therefore the timing of safety analyses and assessments is critical. Analyses and assessments must start early in the design process and continue until design is complete. Once the operational phase begins, safety does not stop. At that time emphasis shifts from the machine design to man-machine interfaces and human errors. If the human factor was not engineered into the safety design, such an omission will show up at this time. Because it is often not practical or possible to redesign the system, safety risks associated with human factor and human errors must be assessed and mitigation measures must be employed to reduce operational hazards and risks. These mitigation methods are usually in the form of training, operational safety procedure, operator limitations, operational restrictions, or less-than-optimum operations due to poor ergonomic or operator designs. Therefore, human factors must be an integral part of the safety hazard analysis and safety risk assessment process.

Safety Assessments

Safety Assessments are not paperwork exercises; they must be factual and accurate. Many assessment reports will be required on large projects or complex systems. A Final Safety Assessment is required at the SSC prior to system operation. Since it is important to identify all safety procedures of the hardware, software, and system design and to identify procedural hazards that may be present, the following areas need to be included in Safety Assessment Reports:

- Safety criteria and methodology used to classify and rank hazards.
- Analyses and tests performed to identify hazards inherent in the system.
- Those hazards that still have a residual risk and the actions that have been or will be taken to reduce those risks to acceptable levels.
- Results of the safety program effort, including a summary of all significant hazards along with specific recommendations, precautions, and mitigation methods required to ensure safety of personnel and property.
- A list of any hazardous materials generated by or used by the system. Identify material type, quantity, potential hazards, precautions, and safety procedures for use, storage, transportation and disposal. Also include copies of Material Safety Data Sheet (OSHA Form 20).

- Conclude with a signed statement that all risks have been resolved or controlled to acceptable levels. If there are any hazardous conditions or areas of risk that are unacceptable or questionable, these shall be clearly documented in the report and a deviation/waiver or variance shall be presented to the managing agency with sound justification and rationale for the lack of resolution of the hazard. As a general rule throughout industry, high risks must always be suppressed to a lower level. Any medium risk is subject to a written, time-limited waiver endorsed by management before operations are allowed.

SUMMARY

The ultimate goal of a comprehensive System Safety program is to minimize the potential for mishaps and thereby maximize operational effectiveness. Inherently safe designs and prudent safeguards and controls can help ensure systems availability and operational safety. To ensure that risks are minimized, many safety tasks must be performed. Safe systems must be planned. Systems must be designed with safety in mind. Shortcuts in safety and human engineering designs, invitations to disaster, must be avoided. Since human error is a contributing cause of the majority of mishaps, human factors must always be considered during design and during selection and evaluation of control and mitigation methods for severe hazards.

Hazard prevention, elimination, and control, and the four System Safety areas of hazard identification, risk assessment, hazard control, and risk management are all interrelated. System Safety hazard analyses and risk management processes, when coupled with Human Factors Engineering concepts, are proven methods and techniques that influence the design and operation of safe systems. Those methods and techniques are currently being implemented at the SSC.