Office of the Under Secretary of Defense (Installations & Environment)/Safety & Occupational Health

DoD Guidance for System Safety Integration into Systems Engineering Process

September 2002

Defense Acquisition Deskbook Transitional Site
http://deskbooktransition.dau.mil

OSD ACQUISITION DESKBOOK
FINAL 7-31-02

SYSTEM SAFETY

DoD 5000.2-R, C.5.2.3.5.10.6

Guidance

This section provides useful guidelines to system acquisition personnel responsible for integrating safety and health requirements into the systems engineering process for an acquisition program. Safety and health considerations can be categorized into two areas: System Safety and Industrial Safety/Occupational Health. Currently, this section focuses on information pertaining to System Safety and will be expanded later to address other Safety and Occupational Health considerations.

System Safety Program Manager Guidance
System Safety Overview
System Safety Policies
System Safety Principles
System Safety Processes

- System Safety Management Plan
- System Safety Program Plan
- System Safety Working Group
- DoD Safety Centers
- Hazard Analyses
- Risk Methodology

COTS
PESHE
Resources

Definitions

System Safety Key Terms, See MIL STD 882C or MIL STD 882D

File Owner: Craig Schilder
Organization: ODUSD (IE)
Phone: (703) 604-1612
Email: craig.schilder@osd.mil
File Last Reviewed: July 2002

SPECIAL ADVICE FOR THE PROGRAM MANAGER

System Safety Program Manager Guidance

You, the Program Manager (PM), must be aware the process of designing safety into systems directly effects operational safety. The goal is to produce inherently safe systems with minimal operational safety requirements or restrictions. Naturally, contractors have an incentive to avoid serious, egregious hazards that may jeopardize the ultimate future of the program or cause them to incur liability for subsequent accidents. However, if the Government does not specifically integrate system safety requirements into the contractor's statement of work, then a contractor will not necessarily fund the resources and allocate work hours to perform system safety. This results in the potential for hazards to creep into the system's design, thereby, resulting in an unsafe system. If high-risk safety problems are allowed to be created or remain undetected until late in development and/or testing, the fixes can wreak havoc with budgets, schedules, and higher-level approvals.

It is your responsibility to demand a safe system from the contractor and to make safety a priority in system design. You acquire acceptably safe systems through these steps:

First, prevent the initial unnecessary hazards. You do this by communicating to the contractor that "designed in" safety is IMPERATIVE and IMPORTANT to you personally. Insist contractors design it in, not add it on, by ensuring there is funding and contractual requirements in the contractor's statement of work and proposal. Order the developer (contractor) to sensitize design engineers to be attentive to system hazards while creating the design, so they may minimize the number and severity of hazards initially residing in the system. Historically, this first step is proven to be a significant cost and problem avoidance technique--one occasionally overlooked by PM's.

Second, explicitly define the interactions between the Government and the contractor in executing system safety requirements. Identify the management and approval process for new and unresolved hazard risks. Use a system safety management plan (SSMP) to identify specific system safety program requirements. Use a technically qualified supporting safety staff to advise and assist you.

Third, manage residual hazards. You do this by assuring the proper level of management acceptance for residual hazard risks. For hazards that are to be "accepted," take care to assure that this risk acceptance occurs at the proper level of authority and is formally documented. Generally, the greater the risk, the higher the approval level is needed for acceptance (e.g., Service/Component Acquisition Executives for high risks and Program Executive Officers for serious risks). Higher levels of risk and acceptance must be justified to the acquisition decision-makers, not the Safety community.

Remember, the ultimate stakeholder with regard to residual safety and health risks for a system is the "end or operational user." The operators and maintainers accrue the most benefit from an effective system safety program executed during system development.

SPECIAL ADVICE FOR THE SYSTEM ENGINEER

System Safety Overview

Although the concept of system safety was first introduced to the engineering design community in the 1950s, the US Air Force Ballistic Missile Division (BMD) for the development of the MINUTEMAN Intercontinental Ballistic Missile (ICBM) used the first known full implementation of the system safety concept as an integral engineering design function. The BMD facilitated both the pace and direction of system safety efforts when they published in April 1960 the first system-wide safety specification, titled *BSD Exhibit 62-41*, *System Safety Engineering: Military Specification for the Development of Air Force Ballistic Missiles*. In the fall of 1962, the MINUTEMAN Program Director, in another system safety first, identified system safety as a contract deliverable item in accordance with BSD Exhibit 62-82.

After an inadvertent launch of a NIKE-AJAX missile in New Jersey in 1958, the Army Ad Hoc Committee investigating the incident recommended that "…safety control through independent review and a balanced technical check of missile systems be established to prevent compromise of safe design and operations…" and that "…the Army (Ordnance) Missile Command establish an authoritative safety organization to review missile weapons systems' design…" As such, this incident and the findings initiated the commencement of system safety within the Army missile community.

These early system safety efforts, including MIL-S-38130, *General Requirements for Safety Engineering of Systems and Associated Subsystems and Equipment*, in 1963, provided the basis for MIL-STD-882, *System Safety Program Requirements*, in July 1969, and the evolution of system safety as a formal, separate engineering discipline within the Department of Defense (DoD). System safety is considered a risk reduction approach for early identification, analysis, elimination, and/or control of hazards; as opposed to just ensuring compliance with various standards and regulations.

EVOLUTION of MIL-STD-882

- BSD Exhibit 62-41, April 1962
  Ballistic Missile Division
- MIL-S-38130, September 1963;
- MIL-S-38130A, 1966
  Aircraft, Space, and Electronics
- Aerospace System Safety Society Founded, 1963; Name Changed to System Safety Society, 1967
- MIL-STD-882, July 1969
  Management Emphasis and Industry Involvement
- MIL-STD-882A, June 1977
  Hazard Probabilities and Risk Acceptance Included
- MIL-STD-882B, March 1984
  Individual Safety Tasks Included
- MIL-STD-882C, January 1993
  Integrated Hardware and Software Tasks
- MIL-STD-882D, January 2000
  Acquisition Reform Changes

System safety engineering criteria and techniques are used to optimize safety for the development, test, production, transport, operation, training, maintenance, and disposal of a system. A collaboration of various organizations (Program Manager, System and Design Engineers, Logisticians, System Safety Engineers, End Users, Safety Centers, etc.) must work together to achieve the integration of system safety requirements into a program. Successful system safety engineering is achieved when Program Managers (PMs) ensure a matrix support structure between the system/design engineers and system safety engineers. The PM has the primary responsibility for ensuring system safety is integral to the systems engineering process and should identify a Government Lead System Safety Engineer early in the program to execute the PM's System Safety Management Program. This Lead System Safety Engineer is the primary safety point of contact for all aspects of the system.

The Government Lead System Safety Engineer, often referred to as the Principal for Safety, is responsible for developing a system safety management approach for the acquisition program and documenting the approach in the Government's System Safety Management Plan (SSMP). The Government Lead System Safety Engineer is also responsible for ensuring the contractor has a specific System Safety Program Plan (SSPP) for development of the system. To successfully execute the overall system safety program for the acquisition program, the Government Lead System Safety Engineer establishes a System Safety Working Group (SSWG) comprised of Government and contractor representatives, who are responsible for implementing specific system safety program requirements as documented in the SSMP and SSPP. The Government Lead System Safety Engineer, as an integral member of Integrated Product Teams (IPTs) (such as the PM and System Engineering IPTs), elevates SSWG findings and recommendations to the IPT and PM. It is the combined decisiveness of the PM, IPT, and Government System Safety Engineer(s) that results in an effective system safety program and appropriate risk reduction measures to eliminate or minimize risks to human life during the development, test, production, transport, operation, training, maintenance, and disposal of the system.

There are several requirements for integrating system safety into the systems engineering process:

1. DoD 5000.2-R, Paragraph C5.2, requires a PM to implement a sound systems engineering approach, which shall permeate design, manufacturing, test and evaluation, and support of the system. Systems engineering principles shall influence the balance between performance, risk, cost, and schedule. Integral to the systems engineering process, especially with regard to performance and risk, is the recognition for the establishment of a system safety program. Working with system and safety engineers, the PM must identify and evaluate potential safety and health risks associated with the life cycle of a system, per DoD 5000.2-R, Paragraph C5.2.3.5.10.6.

2. DoDI 5000.2 explicitly states that safety is a part of total ownership cost. Implementation of an effective system safety management and risk reduction program can substantially control and/or reduce total ownership costs for a system. The ability to reduce during system development the potential for injuries, illnesses, or accidents and the attrition of systems due to serious accidents could result in extra funding available to the PM for application towards critical system development, faster system processes, improved communications and graphical/video imagery systems, etc.
3. Public and political scrutiny of DoD Programs continues to increase due to budgetary constraints and/or from serious accidents involving acquisition systems (i.e., developmental and operational testing or training accidents resulting in personnel death, serious injuries, and/or system damages). Congressional and Secretary of Defense interest focuses on the design of safe systems to protect personnel (operators, testers, and maintainers) from deaths, injuries, and illnesses. A "safe system sells well" with the public, whereas a system resulting in catastrophic to serious events/accidents will be heavily scrutinized by Congress and the Secretariats of Defense, especially with regard to mission and budget considerations. It is the Secretary of Defense's priority to reduce accidents and an overall DoD "zero" tolerance for personnel deaths and injuries resulting from the development, test, production, transport, operation, training, maintenance, and disposal of acquisition systems.

In addition to the above requirements, a recent National Safety Council Report, *DoD Executive Assessment of Safety and Occupational Health Management Systems,* submitted to the Honorable Donald H. Rumsfeld, Secretary of Defense, on 6 December 2001, concluded that safety is not sufficiently integrated into acquisition systems and often is not part of the milestone review decision process. This finding and the continued serious accidents with weapon systems re-emphasizes the criticality of integrating system safety requirements in all aspects of the systems engineering process and for conducting risk reduction assessments in all phases of the DoD acquisition system process.

Fortunately, the PM has available numerous resources to assist in the development and maintenance of a system safety management program. System safety practices and guidelines, as well as organizations, are available to facilitate a system safety program. Of primary importance is the recognition and use of MIL-STD-882 as a performance-based approach to system safety. Each DoD service component has also developed specific guidance and has established Safety Centers available to support acquisition system safety efforts. In addition, Office of the Deputy Undersecretary of Defense, Installations and Environment [(ODUSD (I&E)], Safety and Occupational Health Office, is mandated to provide overall policy and guidance regarding system safety and provides system safety input to OSD decision makers.

LinkClick.aspx

The PM has the final responsibility for implementing a system safety program and ensuring appropriate management level approval of uncorrected identified system hazard risks as part of the system safety process, especially during development and testing. For high to serious risks, the Component Acquisition Executive or Program Executive Office, respectively, is responsible for risk acceptance (e.g., whether to obtain the funding necessary to eliminate or minimize the hazard risk or to accept the degree of residual risks). The PM is the designated risk acceptance level for medium to low risks.

Upon transition of the system to the field, risk acceptance and management is then the responsibility of the “End or Operational User” of the system. Therefore, the user needs to participate in risk acceptance reviews, since they are the ultimate stakeholder with regard to residual safety and health risks. The operators and maintainers accrue the most benefit when the PM eliminates or reduces safety and health risks from having an effective system safety program. Reducing the potential for mishap hazard risks during system development helps to minimize system and operator attrition during deployment, improves user confidence, and ultimately allows for more funds to be allocated to performance enhancements, rather than safety corrective actions.

LinkClick.aspx

System Safety Policies

DoDD 5000.1, Paragraph 4.4.1, requires PMs to use a Total Systems Approach to manage their acquisition program, which includes "… full consideration to all aspects of system support, including logistics planning; manpower, personnel, and training; and human, environmental, safety, occupational health, accessibility, survivability, and security factors…" It is important for PMs to work closely with the requirements and user community to identify safety risks associated with their acquisition program early in the life cycle. DoDD 5000.1 requires the acquisition and requirements communities to maintain continuous and effective communication with each other and the operational user. DoDD 5000.1 further states, "The objective is to gain a sound understanding of the user's needs and to work with them to achieve a proper balance among cost, schedule, and performance considerations."

DoD 5000.2-R, Paragraph C5.2.3.5.10.6, defines the acquisition PM's responsibilities, synopsized as follows, with regard to safety and health:

- **Hazard Identification:** The PM shall identify and evaluate safety and health hazards, defining risk levels in terms of probability and severity. The systems/design and system safety engineering community use various hazard analyses to identify and define the degree of safety risks.
- **Risk Management:** The PM shall use DoD and industry standard practices for system safety and for managing risks encountered in the life cycle of the system, subsystem, equipment, and facilities. These risks include conditions that create significant loss of mission or system capability and death, injury, illness, disability, and/or reduced job performance of personnel who produce, test, operate, maintain, support, or dispose of the system.
- **Risk Acceptance:** The PM shall document each management decision regarding the risk associated with an identified hazard. Each hazard risk shall be accepted by the appropriate management level, based on the established degree of risk (i.e., "high risk" hazards require CAE acceptance). The fundamentals of an acceptable system safety program and risk acceptance methodology are described in MIL-STD-882.
- **Hazardous Materials Controls:** The Occupational Safety and Health Administration (OSHA) standards, which are applicable to all Federal employees, are also applicable to contractor employees working on DoD acquisition contracts or in DoD operations and workplaces. Contractor personnel exposure to hazardous equipment, processes, and materials (e.g., methyl ethyl ketone, beryllium, etc.) must be controlled to reduce the potential for injuries and illnesses.

MIL-STD-882 represents a standard and common approach for system safety requirements and risk management of potential hazards encountered during the development, test, production, transport, operation, training, maintenance, and disposal of the system. During acquisition reform, industry requested and upheld the need for continuing to use MIL-STD-882 in the systems engineering process for DoD acquisition programs. MIL-STD-882 is a readily accepted standard by DoD and industry for implementing a system safety program. Acquisition programs implemented under DoD 5000.2R will use MIL-STD-882D; whereas systems developed before acquisition reform may have system safety programs executed under the requirements of MIL-STD-882C.

System Safety Principles

System safety is based on the approach of studying the entire system under all possible operating conditions to identify potential hazards. System safety engineering is an integral element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of the actions necessary to eliminate/control hazards or reduce the associated risk to an acceptable level. It draws upon professional knowledge and specialized skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system. The degree of safety achieved in a system is directly dependent upon the emphasis applied by the Government and contractors during all phases of the life cycle.

System safety engineering is dedicated to "before the fact" elimination of hazards through the application of management and engineering principles. The fundamental objective is to optimize safety by identifying, eliminating or controlling, and documenting hazard risks throughout the system's life cycle. Design safety impacts operational safety and the goal is to produce an inherently safe system that will have minimal operational safety requirements or restrictions. Managing identified hazards through design and engineering processes is the most effective method. It is estimated 70% of the cost for developing and operating an acquisition system is determined early in the design process. Therefore, deliberations and recommendations of the SSWG communicated via the System Safety Engineer to the PM and Systems IPTs, early in the systems engineering process, can afford substantial benefits through the "design out" of potential safety and health hazards.

SAFETY/RISK REDUCTION PRECEDENCE

- **Design for minimum hazard risk**
- **Incorporate safety devices**
- **Provide warning devices**
- **Develop procedures and training**

Separating the potential hazard from personnel using safety devices (such as physical guards or barriers) is the next course of action, if design or engineering changes are not feasible. Warning devices are the next method for controlling remaining hazards. And finally, if all other methods have been exhausted, then procedures and training is used to control residual hazard risks.

To achieve this safety/risk reduction precedence, system safety must be integral with the acquisition program and must include close coordination with representatives of the acquisition, requirements, and operational communities to effectively identify and resolve hazard risks within the operational constraints and mission requirements of the system throughout its life cycle.

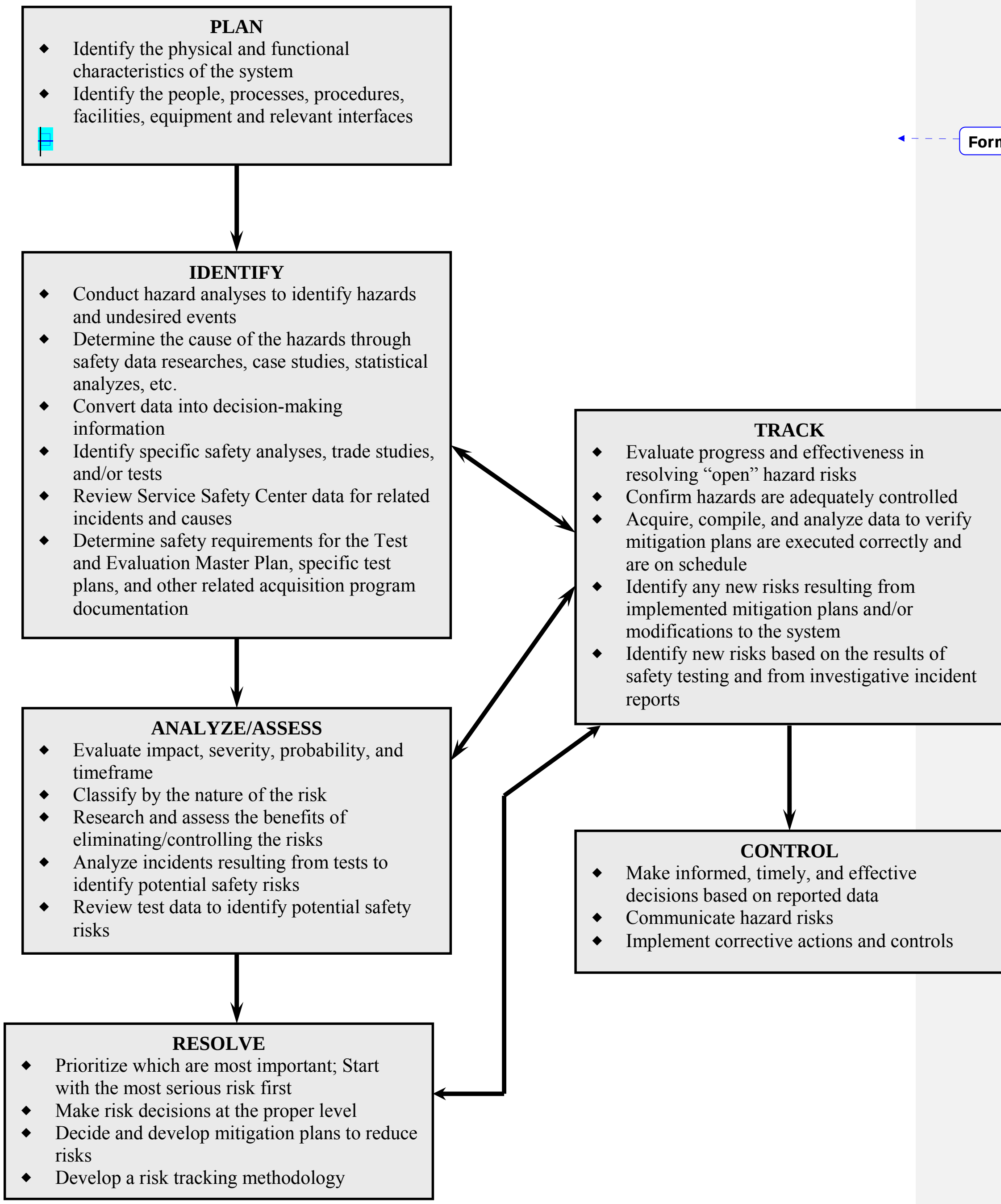
LinkClick.aspx

System Safety Processes

The PM can achieve a safe system through implementation and careful execution of a system safety program. The PM must continually monitor the system safety program to assure effective hazard control and proper acceptance of risk to avoid:

- Loss of life and/or serious injury to personnel;
- Serious damage to facilities and/or equipment resulting in large dollar loss;
- Failures with serious adverse impact on mission capability, mission operability, cost, schedule, or public opinion; and/or
- Detrimental harm to the environment and the surrounding community.

The system safety process, depicted below, revolves around identification and elimination and/or control of hazards throughout the life cycle of the acquisition system, which is accomplished through the conduct of hazard analyses and testing.



Formatted: Bullets and Numbering

The degree of safety achieved depends directly on management emphasis. For that reason, the PM and the Government Lead System Safety Engineer, working within all system functional areas, must consider the following as integral in developing effective system safety processes:

- Safety, consistent with mission requirements, is designed into the system in a timely and cost-effective manner.
- All hazards are identified, evaluated, and eliminated; and the Milestone Decision Authority (MDA) accepts the residual risks associated throughout the system's life cycle. All MDA decisions regarding hazard risks are documented.
- Historical safety data, such as "lessons learned" and "case studies" from other systems, are considered and used in defining system safety criteria and objectives. This information serves as a baseline for conducting Preliminary Hazard Lists and Preliminary Hazard Analyses.
- Minimum risk is sought in accepting and using new designs, materials, production, and test techniques.
- Retrofit actions are minimized.
- Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MDA.
- Hazards identified after production are minimized consistent with program constraints.

The extent of system safety integration within the systems engineering process is directly related to the complexity of the system being procured. For example, a system that consists of a network of Commercial Off-The-Shelf (COTS) computer hardware might require only an assessment on the status of individual item electrical safety certifications and an analysis of the interfaces to demonstrate its safety. Conversely, a major weapon system such as a fighter aircraft (consisting of munitions, guidance systems, sophisticated computer software, lasers, fuel systems, and communications systems) would require individual analyses of each component for explosives, fire, laser, ground/shore, and software safety. System safety requirements for an acquisition program are tailored based on the system's characteristics, the required performance requirements, and the hazards inherent to the system.

LinkClick.aspx

System Safety Management Plan

The Government Lead System Safety Engineer will develop a System Safety Management Plan (SSMP) to document the Government's overall system safety management approach for the system. The Government's SSMP is one of the first steps for ensuring integration of system safety into an acquisition program and is typically prepared prior to awarding the system development contract. The SSMP must be reviewed and modified, as necessary, on a regular basis (such as at critical reviews and milestone decisions).

CONSIDERATIONS for the SSMP

- Define specific system safety program requirements and tasks
- Identify the organization and responsibilities of Government personnel involved in the system safety program
- Define the interfaces between the Government and contractor in executing system safety program requirements and risk resolution
- Identify the System Safety Working Group members
- Specify safety analysis and trade studies required and the associated timelines for performing the studies
- Develop the tailored risk assessment methodology and risk definitions for the acquisition program.

System Safety Program Plan

The Government PM and Lead System Safety Engineer are responsible for mandating the contractor develop a System Safety Program Plan (SSPP) for the acquisition program. The contractor's SSPP serves as the basic foundation for executing their system safety program. The SSPP defines the logical, systematic, and efficient approach for applying system safety principles to system development; thereby serving as the guiding document for the "what, when, how, where" aspects of the planned system safety program. The SSPP identifies the contractor's organizational resources and responsibilities for executing the system safety program, the specific system safety tasks and procedures, the risk assessment methodology and risk acceptance criteria, system safety products, and critical milestones. Often the SSPP is submitted either as part of the contractor's proposal to the Government or as one of the first safety deliverables of the contract. The SSPP should be periodically updated, such as at critical review points (such as each life cycle phase).

EXAMPLE OUTLINE for a SSPP

- Introduction
- System Safety Program Description
    - Contractor Organization
    - Contractor Responsibilities
    - System Safety Tasks
    - Milestones
- System Safety Requirements
    - Task Descriptions
    - Specific Hazard Analyses
    - System Safety Data
- Risk Assessment and Mitigation Methodology
    - Safety Verification Process

System Safety Working Group

The System Safety Working Group (SSWG) serves as an advisory panel to the PM. An effective SSWG is usually comprised of Government and contractor representatives from the various systems engineering functional areas and a representative of the user/operator. Critical to the SSWG is the Government Lead System Safety Engineer, who typically serves as the Chairperson, and the PM or their designated representative (such as the Class Desk Lead). SSWG meetings/reviews are held at a regular frequency (typically quarterly for a major acquisition program) and/or at key milestone reviews (e.g., concept design review, system design review, in-process reviews, etc.).

REPRESENTATIVE SSWG RESPONSIBILITIES

- Review acquisition documents, both Government and contractor, for safety and health implications
- Collect and evaluate "lessons learned" and "case studies" that may be relevant to the acquisition program
- Implement a risk assessment and acceptance methodology, as well as a hazard tracking database
- Review and track progress on system safety tasks
- Evaluate and monitor contractor system safety documentation
- Maintain the appropriate revisions to the SSPP
- Independently assess and verify the degree of risk for identified hazards
- Review and recommend best technical approach regarding resolution of safety and health hazard risks

The SSWG is integrated with various individual functional IPTs, reporting directly to the PM via the Government Lead System Safety Engineer. If the program is a Joint Service development program, it is even more critical that user representatives from all involved services participate as SSWG members. The user representatives bring to the table valuable insight into the actual operational environments of their commands from a safety perspective and provide channels through which timely user command feedback and buy-in may be obtained for cases where risk must be accepted.

The SSWG's is responsible for elevating system safety issues to the PM with recommendations for integration into the overall program risk management structure. The Component Acquisition Executive (CAE) is far more likely to look favorable on a request for acceptance of high risk, especially in Joint Service programs, if the CAE knows the users/operators have been participants in the system safety process and are fully on board.

DoD Safety Centers

Each DoD Service has established safety centers that collect accident data. These centers offer a wealth of expertise and experience available to assist the PM, Systems/Design Engineers, and System Safety Engineers in identifying historical and current safety and health hazard risk information on DoD systems. Do not hesitate to request safety center representation at SSWG meetings or assistance in assessing and resolving hazard risks.

LinkClick.aspx

Air Force Safety Center (http://safety.kirtland.af.mil):

- Develops, implements, executes, and evaluates Air Force aviation, ground, weapons, space and system mishap prevention, and nuclear surety programs to preserve combat readiness
- Conducts research to promote safety awareness and mishap prevention
- Oversees mishap investigations
- Evaluates corrective actions and ensures implementation
- Develops and directs safety and operational risk management education

Army Safety Center (http://safety.army.mil):

- Prevents the accidental loss of personnel and conserves materiel resources through safe air and ground
- Enhances combat readiness through proactive risk management to prevent accidents
- Assist commanders in integrating risk management into all the Army does
- Provides proactive assistance to command risk management and safety programs through assessments and educational tools
- Trains military and civilian safety professionals in the latest risk management techniques and integration skills
- Develops safety policies which promote safe practices and processes
- Conducts accident investigations

Marine Corps Safety (http://www.hqmc.usmc.mil/safety.nsf):

- Enhances Marine Corps readiness by educating and equipping Marines, Sailors, and Civilians to manage risks and reduce mishaps
- Implements an effective strategy for force protection
- Provides support in determining safety program policies and objectives
- Develops procedural guides and implementing directives

Naval Safety Center (http://www.safetycenter.navy.mil):

- Trains and motivates Sailors and Marines to prevent mishaps and save lives
- Evaluates emerging safety technology and processes in Government and private industry
- Solicits feedback from the Fleet and Naval Safety Center team
- Assesses mishap trends
- Provides safety policies, guidance, and assessments

LinkClick.aspx

Hazard Analyses

System safety hazard analyses are an integral part of the systems engineering function. These analyses are a systematic approach to identifying and resolving the potential safety and health hazard risks associated with the development, test, production, transport, operation, training, maintenance, and disposal of the system. Hazard analyses include an assessment of the system, subsystems, operations, processes, equipment, personnel, and materials in terms of severity of consequences and the probability of the hazard occurring. There are established Data Item Descriptions (DIDs) (refer to the ESOH Reference Library on the Acquisition Deskbook) specifying contractual requirements for these hazards analyses.

BASIC SYSTEM SAFETY HAZARD ANALYSES

- Preliminary Hazard List (PHL)
- Preliminary Hazard Analysis (PHA)
- System Hazard Analysis (SHA)
- Subsystem Hazard Analysis (SSHA)
- Operating and Support Hazard Analysis (O&SHA)
- Safety Assessment Report (SAR)
- Health Hazard Assessment (HHA)
- Software Safety Analysis (SSA)

Preliminary Hazard List

The Preliminary Hazard List (PHL) is typically a one-time assessment performed early in the acquisition process (i.e., concept and technology development) to identify the initial potential hazards with the system. The PHL serves as the baseline for focusing management emphasis in relation to overall effective risk management, developing design or performance criteria for the system to eliminate/control the hazards, and defining the extent of required hazards analyses necessary for the system safety program. As part of the PHL development, a review of safety experience on legacy and similar systems should be conducted regarding mishap/accident occurrences, safety lessons learned, existing hazard risks, operator/user concerns, etc.

Preliminary Hazard Analysis

A Preliminary Hazard Analysis (PHA) is an expansion of the PHL and documents the safety critical areas and initial assessment of the identified hazards in terms of probability and severity. In addition, the PHA identifies the required corrective actions to eliminate or control the hazard risks. The proposed design and function of the system is evaluated for additional hazards and risks, and to identify operational constraints.

Subsystem Hazard Analysis

A Subsystem Hazard Analysis (SSHA) is performed to verify previously unidentified hazards associated with the design of the subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between system components and equipment comprising each subsystem.

System Hazard Analysis

A System Hazard Analysis (SHA) is performed to identify hazards associated with the subsystem interfaces and system functional faults, and to assess the degree of risk associated with the total system design, including software. The SHA determines whether or not safety design criteria in the hardware, software, and system specifications have been met; and confirms that design or corrective actions do not impair or degrade the safety of the system.

Operating and Support Hazard Analysis

The Operating and Support Hazard Analysis (O&SHA) evaluates the potential for hazards and the degree of risk resulting from the implementation of operational and support procedures (e.g., maintenance, transport, disposal, etc.) performed by personnel supporting the system. The O&SHA considers the relation of the system to each phase of activity; facility interfaces; planned operating environments; support equipment; safety and occupational health regulatory requirements; and the potential for unplanned events, including hazards introduced by human errors.

Software Safety Analysis

Today's acquisition systems rely heavily on the use of automated and digital controls to achieve effective and efficient system operations and mission capabilities. Software anomalies, design flaws, or run-time errors within the safety-critical functions of a system introduce the potential of a hazardous condition that could result in death, personnel injury, and/or loss of the system. Examples of software incidents include inadvertent missile launches, flight control failures at supersonic transition, missile launch timing failures resulting in hang-fires, incorrect missile firings due to invalid set-up sequences, or complete loss of the system because of software driven hardware malfunctions. Consequently, Software Safety Analyses on the system and subsystems is extremely important to reduce the overall safety risk of software-controlled operations.

The PM and Government Lead System Safety Engineer should ensure the inclusion of Software Hazard Analyses as part of the overall system safety engineering process. Software Safety Analyses address both the software requirements for a system and the software codes and programs. The purpose of these analyses are to identify potential system hazards contributed to by the software or software environment and to examine the causal factors so as to eliminate or mitigate the hazard risks throughout the continued development of the software.

The application of this analysis is especially critical relative to the procurement and integration of COTS into both new and existing systems.

LinkClick.aspx

Health Hazard Assessment

The Health Hazard Assessment (HHA) focuses on the identification of potential health hazards and costs due to system component materials and evaluates potential alternative materials to reduce the associated risk to users/operators of the system. Specific health hazards and impacts assessed during a HHA include chemical, physical, biological, and/or ergonomic hazards, as well as other potential hazards that may be introduced by the development, test, production, transport, operation, training, maintenance, or disposal of the system. The degree of personnel exposure to a health hazard is an integral part of the evaluation process and is based on the potential routes, the cause, magnitude, frequency, and duration of exposure. The following is a representative example of health hazard categories evaluated during a HHA:

HHA CATEGORY	EXAMPLES
▪ Acoustic Energy: Potential energy existing in a pressure wave transmitted through the air may interact with the body to cause loss of hearing or internal organ damage	▪ Steady-state noise from engines ▪ Impulse noise from shoulder-fired weapons
▪ Biological Substances: Exposures to microorganisms, their toxins, and enzymes	▪ Sanitation concerns related to waste disposal
▪ Chemical Substances: Exposures to toxic liquids, mists, gases, vapors, fumes, or dusts	▪ Combustion products from weapon firing ▪ Engine exhaust products ▪ Degreasing solvents
▪ Oxygen Deficiency: Hazard may occur when atmospheric oxygen is displaced in a confined/enclosed space and falls below 21% by volume; Also used to describe the hazard associated with the lack of adequate ventilation in crew spaces	▪ Enclosed or confined spaces associated with shelters, storage tanks, and armored vehicles ▪ Lack of sufficient oxygen and pressure in aircraft cockpit cabins ▪ Carbon monoxide in armored tracked vehicles

LinkClick.aspx

HHA CATEGORY (CONTINUED)	EXAMPLES (CONTINUED)
▪ Radiation Energy: Ionizing Radiation – any form of radiation sufficiently energetic to cause ionization when interacting with living matter; and Non-Ionizing Radiation – emissions from the electromagnetic spectrum that has insufficient energy to produce ionization, such as lasers, ultraviolet, and radio frequency radiation sources	▪ Ionization – Radioactive chemicals used in light sources for optical sights and instrumented panels ▪ Non-Ionizing – Laser Rangefinders used in weapons systems; Microwaves used with radar and communication equipment
▪ Shock: Delivery of a mechanical impulse or impact to the body. Expressed as a rapid acceleration or deceleration	▪ Opening forces of a parachute harness ▪ Back kick of firing a handheld weapon
▪ Temperature Extremes: Human health effects associated with hot or cold temperatures	▪ Increase to the body's heat burden from wearing total encapsulating protective chemical garments ▪ Heat stress from insufficient ventilation to aircraft or armored vehicle crew spaces
▪ Trauma: Injury to the eyes or body from impact or strain	▪ Physical injury cause by blunt or sharp impacts. ▪ Musculoskeletal trauma caused by excessive lifting
▪ Vibration: Adverse health effects (e.g., back pain, hand-arm vibration syndrome (HAVS), carpel tunnel syndrome, etc.) caused by contact of a mechanically oscillating surface with the human body	▪ Riding in and/or driving/piloting armored vehicles or aircraft ▪ Power hand tools ▪ Heavy industrial equipment
▪ Human-Materiel Interface: Various injuries such as musculo-skeletal strain, disc hernia, carpel tunnel syndrome, etc. resulting from physical interaction with and/or mechanical energy of system components	▪ Repetitive ergonomic motion ▪ Manual material handling – lifting assemblies or subassemblies ▪ Acceleration, pressure, velocity, and force

LinkClick.aspx

Safety Assessment

The Safety Assessment is the culmination of all the hazard analyses performed for an acquisition system and reflects the comprehensive degree of risk being assumed prior to the test or operation of the system. The Safety Assessment identifies all the safety features and safety procedures for the hardware, software, and system design. This assessment is critical to the "Safety Releases" issued prior to the testing, training, or operation of the system. Especially within the DoD testing community, the Safety Assessment Report (SAR) is used to provide appropriate requirements and controls for the Safety Release. Integral to this safety assessment and the safety release process is the integration of specific and appropriate DoD Service Safety Review Boards and/or Safety Centers.

Likewise, the Operational Test and Evaluation (OT&E) (http://www.dote.osd.mil) is a critical component in the safety assessment of the system during tests (especially prior to full rate production and deployment). Directly funded by Congress, the OT&E serves as an independent safety evaluator (from the developer) on the suitability, reliability, and safety of system. The importance of the OT&E in the development of the system and in assessing overall safety is further substantiated in Section 139 of Title 10 United States Code, whereby, Section 232 *Communicating of Safety Concerns between Operational Testing and Evaluation Officials and Program Managers* states:

"The Director shall ensure that safety concerns developed during the operational test and evaluation of a weapon system under a major defense acquisition program are timely communicated to the program manager for consideration in the acquisition decision-making process."

LinkClick.aspx

Risk Methodology

The process of identifying and managing system safety risks is a proven approach. Of importance is for the PM to integrate the results of the system safety risk assessment process into the overarching risk assessment methodology used for managing their entire acquisition program. The PM evaluates the hazards and associated risks in the context of user requirements, potential mission capability, the operational environment, and program constraints. Several points must be kept in mind when resolving hazard risks:

- Risk management is a process of tradeoffs
- Risk is a fundamental reality
- Quantifying risk does not ensure safety
- Risk is a matter of perspective

The communication to all system developers and users, documentation, and tracking the identified hazard risks and decisions made is ultimately the responsibility of the PM. The benefits of risk management include a reduction in serious personnel injuries and fatalities, reduction in material and property damage, effective mission accomplishment, protection of program schedules, and control of costs.

Within the DoD community, risk identification and management is based on the various system safety hazard analyses conducted for a system. All identified hazards are defined in risk terms by evaluating the “severity” of potential mishaps associated with the hazard and the “probability” that the hazard could create a mishap. These categories are used to provide a qualitative or quantitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies or failures, and system/subsystem/component failures or malfunctions.

The mishap “severity” category provides a qualitative or quantitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system/subsystem/component failures or malfunctions. Example mishap “severity” categories based on MIL-STD-882D are depicted as follows:

LinkClick.aspx

DESCRIPTION	CATEGORY	SAFETY and HEALTH RESULT CRITERIA
CATASTROPHIC	I	Could result in death, permanent total disability, loss exceeding $1M
CRITICAL	II	Could result in permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1 Million major system or subsystem loss
MARGINAL	III	Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $20,000 but less than $200K
NEGLIGIBLE	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2,000 but less than $20,000

These mishap severity categories provide guidance to a wide variety of programs. Therefore, a mutual understanding between the PM, Government Lead System Safety Engineer, the system development team, and the contractor is usually required as to the meaning of the "severity" definitions.

The "probability" category provides a qualitative or quantitative measure on the likelihood of the condition or event occurring. The probability is defined as potential occurrences per unit of time, events, items, population, or activity. Example "probability" categories from MIL-STD-882D are depicted as follows:

LinkClick.aspx

DESCRIPTION*	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET or INVENTORY**
Frequent	A	Likely to occur often in the life of the item, with a probability of occurrence greater than 10^{-1} in that life	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life	Will occur frequently
Occasional	C	Likely to occur some time in the life of the item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

The combination of “severity” and “probability” establishes the overall risk for an identified hazard, which is used to prioritize resolution of hazards and the appropriate management decision authority on identified hazards. The use of a matrix with “severity” on one axis and “probability” on the other axis, with the use of numeric mishap hazard assessment values, is used to represent the risk associated with each hazard and to identify the level of management required for risk acceptance. The specific method for risk assessment is up to the PM and the associated risk definitions and risk acceptance matrix are tailored accordingly for the program. The overall risk assessment method and definitions should be included in the Environmental, Safety, and Occupational Health (ESOH) section of the Acquisition Strategy Support Plan. One representative risk management matrix, based on MIL-STD-882D, is as follows:

HAZARD PROBABILITY	HAZARD SEVERITY				
		I Catastrophic	II Critical	III Marginal	IV Negligible
	A Frequent	1 High	3 High	7 Serious	13 Medium
	B Probable	2 High	5 High	9 Serious	16 Medium
	C Occasional	4 High	6 Serious	11 Medium	18 Low
	D Remote	8 Serious	10 Medium	14 Medium	19 Low
	E Improbable	12 Medium	15 Medium	17 Medium	20 Low

Mishap risk assessment values from the above representative matrix are then grouped into mishap risk categories, which are used to generate a specific action and the mandatory reporting requirement for the action and formal acceptance of the associated risk. Realistically, some level of risk will be accepted for a system. The following table, tailored from MIL-STD-882D, reflects the management reporting and acceptance requirements based on the mishap risk category and risk assessment values:

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1-5	High	Service/Component Acquisition Executive
6-9	Serious	Program Executive Office
10-17	Medium	Program Manager
18-20	Low	Program Manager or As Directed

In addition to the above risk management approach traditionally used within DoD, other Federal agencies have developed additional analysis and risk assessment methodologies. The National Aeronautics and Space Administration (NASA), for example, has developed a series of comprehensive approaches (i.e., Probabilistic Risk Assessment (PRA) to identify hazard risks – *PRA Procedures Guide for NASA Managers and Practitioners*) and uses established software tools.

The PRA is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effective, improved safety and performance. The PRA is a decision support tool to help managers and engineers find design and operation weaknesses in complex systems and to systematically and efficiently prioritize safety improvements. The PRA considers not only the low probability and high severity mishap scenarios, but also scenarios involving

LinkClick.aspx

strings of high-probability and low-severity, nearly benign, mishaps; which contrary to common perception are oftentimes more detrimental to safety than the former scenarios).

Software applications used by NASA support root cause analyses to solve identified problems/risks. The tools provide a standard operating procedure for users, guiding them through a step-by-step series of questions to achieve a solution. The tools serve as a basic foundation for designing prevention and control into processes.

ROOT CAUSE ANALYSIS

- Gather and order all relevant data about the problem/risk
- Identify the internal causes that have generated or allowed the problem/risk
- Identify all preventive controls for the problem/risk
- Analyze for decision-makers the comparative benefits and cost-effectiveness of all available prevention options

Root cause analyses, therefore, provide a means to depict and logically validate the cause and effect relationships in the entire causal system, so the person with the responsibility for making a decision has a means of validating the data upon which their decision is to be based.

LinkClick.aspx

Commercial Off-The-Shelf

Use of commercial items offers a PM significant opportunities for affordability, faster insertion of new technology, and/or greater reliability and availability of the system. Integration of Commercial Off-The-Shelf (COTS) items into a system can cause unexpected safety hazards. Not all commercially available items are necessarily developed to the same safety standards applied in the DoD acquisition process. With integration of COTS items, there is an increased potential for hardware or software failures that can result in system failures/losses and personnel deaths/injuries. For example, use of a COTS aircraft system could result in problems with flight controls, emergency response, communications, engine power levels, and fueling.

REPRESENTATIVE HAZARDS TYPICAL to INTEGRATION of COTS ITEMS

- Excessive Noise
- Toxic Fumes, Dusts, Mists, etc.
- High Energy Sources
- Temperature Extremes
- Fire or Explosion
- Radiation
- Weight Lifting Constraints

In addition, there is usually a lack of safety and other related documentation on the COTS item to assist the System Safety Engineer in assessing the potential hazards or factors contributing to potential undesirable safety risks. The environment in which the COTS item will be used must also be considered when evaluating potential safety hazards (i.e., many commercial electronics are not designed to operate in the rain and mud). As with the development of the overall acquisition system, the PM must address system safety and software engineering considerations with the procurement, integration, test, and sustainment of COTS items.

PMs must understand that, often, use of COTS items is cheaper only because standard development costs have not been applied and that, when some of those costs are applied, COTS items may not be the best alternative. The development position is that hazards must be identified and risks assessed to be acceptable regardless of how the component/function is developed. The decision to use COTS items does not negate system safety requirements and the costs for obtaining the hazard analysis/risk assessment data must be factored in to the overall cost for the COTS item.

LinkClick.aspx

Programmatic Environmental, Safety, and Health Evaluation (PESHE)

Per DoD 5000.2-R, Paragraph 5.2.3.5.10.2, the PM must prepare a Programmatic Environmental, Safety, and Health Evaluation (PESHE) document, which identifies system safety and occupational health risks to the operators and maintainers of the system, how hazard risks are managed, and how regulatory requirements are being met throughout the system's life cycle phases. Integral to this PESHE is a synopsis and concise discussion on the system safety efforts, per the SSMP and/or SSPP, and the current issues. The risk assessment methodology and risk definitions tailored for the acquisition program should be included in the PESHE, as well as in the ESOH section of the Program's Acquisition Strategy (AS) Support Plan. This ensures the planned risk assessment approach is accepted when the AS is approved. The PESHE document is the means for communicating to the PM and acquisition executives the highest, serious safety and health risks associated with the development, test, production, transport, operation, training, maintenance, and disposal of the system. The overall PESHE process and document offers the System Safety Engineers a mechanism to demonstrate how the SSWG is proceeding with achieving the system safety requirements defined in the SSMP and/or SSPP.

REPRESENTATIVE SYSTEM SAFETY AREAS ADDRESSED IN THE PESHE DOCUMENT

- Methods for Integration of System Safety into the Systems Engineering Process
- Risk Assessment and Reduction/Tracking Methodology
- System Safety Resources (i.e., DoD Services' Safety Centers) Used to Implement the System Safety Management Program
- Identification of High and Open Safety Hazards/Risk Areas
- Critical Issues Demanding Immediate PM/ Upper Management Attention

LinkClick.aspx

Resources:

Navy

ORGANIZATION	ADDRESS	WEB PAGE
Navy Safety Center	375 A Street Norfolk, VA 23511	http://safetycenter.navy.mil/
Navy & Marine Corps Accident (Mishap) Data Repository	375 A Street Norfolk, VA 23511	http://safetycenter.navy.mil/
Marine Corps Safety Center	Commandant of the Marine Corps (SD) HQ, US Marine Corps 2 Navy Annex Washington, DC 20380-1775	http://www.hqmc.usmc.mil/safety.nsf/
CNO Safety & Occupational Health Office	Chief of Naval Operations, N-454 Crystal Plaza #5 Room 636 2211 South Clark Place Arlington, VA 22202-3735	http://www.navosh.net
Naval Air Systems Command (NAVAIR) System Safety	NAVAIR System Safety Engineering Code 4.1.10 Bldg. 2185, Room 2121 Patuxent River, MD	
Office Environmental Protection & Occupational Safety and Health	Commander Naval Sea Systems Command (NAVSEASYSCOM) 1333 Isaac Hull Ave SE Washington Navy Yard, DC 20376	http://www.navsea.navy.mil/sea00tWWW/

Navy (Continued):

ORGANIZATION	ADDRESS	WEB PAGE
Combat System Safety & Engineering Division (G70) System Safety Engineering Branch (G71) Software System Safety Review Board – Technical Review Panel	Commander Dahlgren Division Naval Surface Warfare Center Dahlgren, VA 22448-5100	Combat System Safety & Engineering Division (G70) http://www.nswc.navy.mil/safety/g70.htm System Safety Engineering Branch (G71): http://www.nswc.navy.mil/safety/g71.htm This Branch Includes: ◆ Software System Safety Review Board (SSSRB) – Technical Review Panel ◆ Weapon System Explosives Safety Review Board (WSESRB) ◆ US Navy and US Marine Corps Laser Safety
Weapon System Explosives Safety Review Board (WSESRB)	Naval Ordnance Safety and Security Activity (NOSSA) N31 23 Strauss Avenue Farragut Hall Bldg. D-323 Indian Head, MD 20640-555	http://nossa.ih.navy.mil/

LinkClick.aspx

Army:

ORGANIZATION	ADDRESS	WEB PAGE
Army Safety Center	Ft. Rucker, AL	http://safety.army.mil
Health Hazard Assessments, US Army Center for Health Promotion and Preventive Medicine	ATTN; MCHB-TS-OHH 5158 Blackhawk Rd Aberdeen Proving Ground, MD 21010-5422	http://chppm-www.apgea.army.mil/hha/
Army Materiel Command	ATTN: AMCSF 5001 Eisenhower Ave Alexandria, VA 22333-0001	http://www.amc.army.mil/amc/sf/staff.html
Army Aviation and Mission Command	ATTN: AMSAM-SF Redstone Arsenal, AL	http://www.redstone.army.mil/safety/safepoc.html
TRADOC Safety, Occupational Health, and Fire Safety	US Army Training and Doctrine Command Ft. Monroe, VA 23651-5000	http://www.tradoc.army.mil/safe/
Army Tank-Automotive and Armaments Command	ATTN: AMSTA-CZ-SF Warren, MI 48397-5000 ATTN: AMSTA-AR-QAW-S Picatinny Arsenal, NJ 07806-5000	http://www.tacom.army.mil/
Army Communication-Electronics Command	ATTN: AMSEL-SF Bldg. 2539 Laboratory Rd. Charles Wood Area Ft. Monmouth, NJ 07703-5000	http://www.monmouth.army.mil/cecom/safety/system/index1.htm
Army Simulation Training and Instrumentation Command	ATTN: AMSTI-EO 12350 Research Parkway Orlando, FL 32826	http://www.stricom.army.mil/STRICOM/SAFETY/sys_safe.jsp http://www.stricom.army.mil/STRICOM/SAFETY/
Army Soldier and Biological Chemical Command	ATTN: AMSSB-RA 5183 Blackhawk Rd Aberdeen Proving Ground, MD 21010-5424	http://www.sbccom.army.mil/

LinkClick.aspx

Army (Continued):

ORGANIZATION	ADDRESS	WEB PAGE
Army Fuze Safety Review Board	Army Fuze Management Office Picatinny Arsenal, NJ 07806-5000	http://w4.pica.army.mil/
Army Soldier and Biological Chemical Command – Natick	ATTN: AMSSB-OSE (N) Kansas Street Natick, MA 01760-5550	http://www.natick.army.mil/soldier/index.htm
Army Space and Missile Defense Command	ATTN: SMCS-TC-WS P.O. Box 1500 Huntsville, AL 35807-3801	http://www.smdc.army.mil/Safety.html
Army Developmental Test Command	ATTN: CSTE-DTC-IM-S 314 Longs Corner Road Aberdeen Proving Ground, MD 21005-5055	http://www.atc.army.mil/
Army Test and Evaluation Command	ATTN: CSTE-ILE-S 4501 Ford Avenue Alexandria, VA 22302-1458	http://www.dtc.army.mil/welcome.html

LinkClick.aspx

Air Force:

ORGANIZATION	ADDRESS	WEB PAGE
Air Force Safety Center	HQ AFSC/SE 9700 G Avenue SE Kirtland Air Force Base, New Mexico 87177-5670	http://www-afsc.saia.af.mil/
Air Force Accident/Mishap Data Repository	HQ AFSC/SE 9700 G Avenue SE Kirtland Air Force Base, New Mexico 87177-5670	https://sas.kirtland.af.mil/
AF Materiel Command	HQ AFMC-SE Wright Paterson AFB, 45433	https://www.afmc-mil.wpafb.af.mil/HQ-AFMC/SE/Systems/index.htm
Munitions	AAC/SES Eglin Air Force Base, FL 32542-5000	
Space Systems	HQ Space & Missile Systems Center Directorate of Systems Acquisition Acquisition Health & Safety SMC/AXZS 2420 Vela Way, Suite 1467 El Segundo, CA 90245	http://ax.losangeles.af.mil/axz/

LinkClick.aspx

Other Federal/Government Agencies:

ORGANIZATION	ADDRESS	WEB PAGE
DoD Explosive Safety Board (DDESB)	2461 Eisenhower Ave Alexandria, VA 223311-0600	http://www.ddesb.pentagon.mil/ddesb
Office of Safety and Mission Assurance	Code Q NASA Headquarters Washington, DC	http://www.hq.nasa.gov/office/codeq/
United Space Alliance	Boeing/Lockheed Martin Joint Venture to Conduct Space Flight Operations for NASA Houston, TX	http://www.unitedspacealliance.com/about/safety.html http://www.unitedspacealliance.com/ http://rootcause.com/
Federal Aviation Administration, Office of System Safety	800 Independence Avenue, SW Room 810 Washington, DC 20591	http://www.asy.faa.gov/
Department of Transportation	400 Seventh St. SW Washington, DC 20590	http://www.dot.gov/ http://www.dot.gov/safety.html
National Transportation Safety Board	490 L'Enfant Plaza SW Washington, DC 20594	http://www.ntsb.gov
National Highway Traffic Safety Administration	400 7th St. SW Washington, DC 20590	http://www.nhtsa.dot.gov/nhtsa/

LinkClick.aspx

Other Federal/Government Agencies (Continued):

ORGANIZATION	ADDRESS	WEB PAGE
Directorate of Health & Safety	US Coast Guard Commandant (G-WK) 2100 Second St. SW Washington, DC 20593-0001	Directorate of Health & Safety (G-WK): http://www.uscg.mil/hq/g-w/g-wk/wk.htm Aviation Safety Division (G-WKS-1): http://www.uscg.mil/hq/g-w/g-wk/g-wks/g-wks-1/wks1.htm
IH Human Factors Research & Technology HIS System Safety Research Branch	NASA Ames Research Center Information Sciences & Technology Directorate Moffett Field, CA 94035	http://human-factors.arc.nasa.gov/ http://human-factors.arc.nasa.gov/ihs/index.html
Government Electronic Industries Association System Safety Committee, G-48		http://www.geia.org/sstc/G48/
System Safety Society	PO Box 70, Unionville, VA 22567-0070	http://www.system-safety.org/