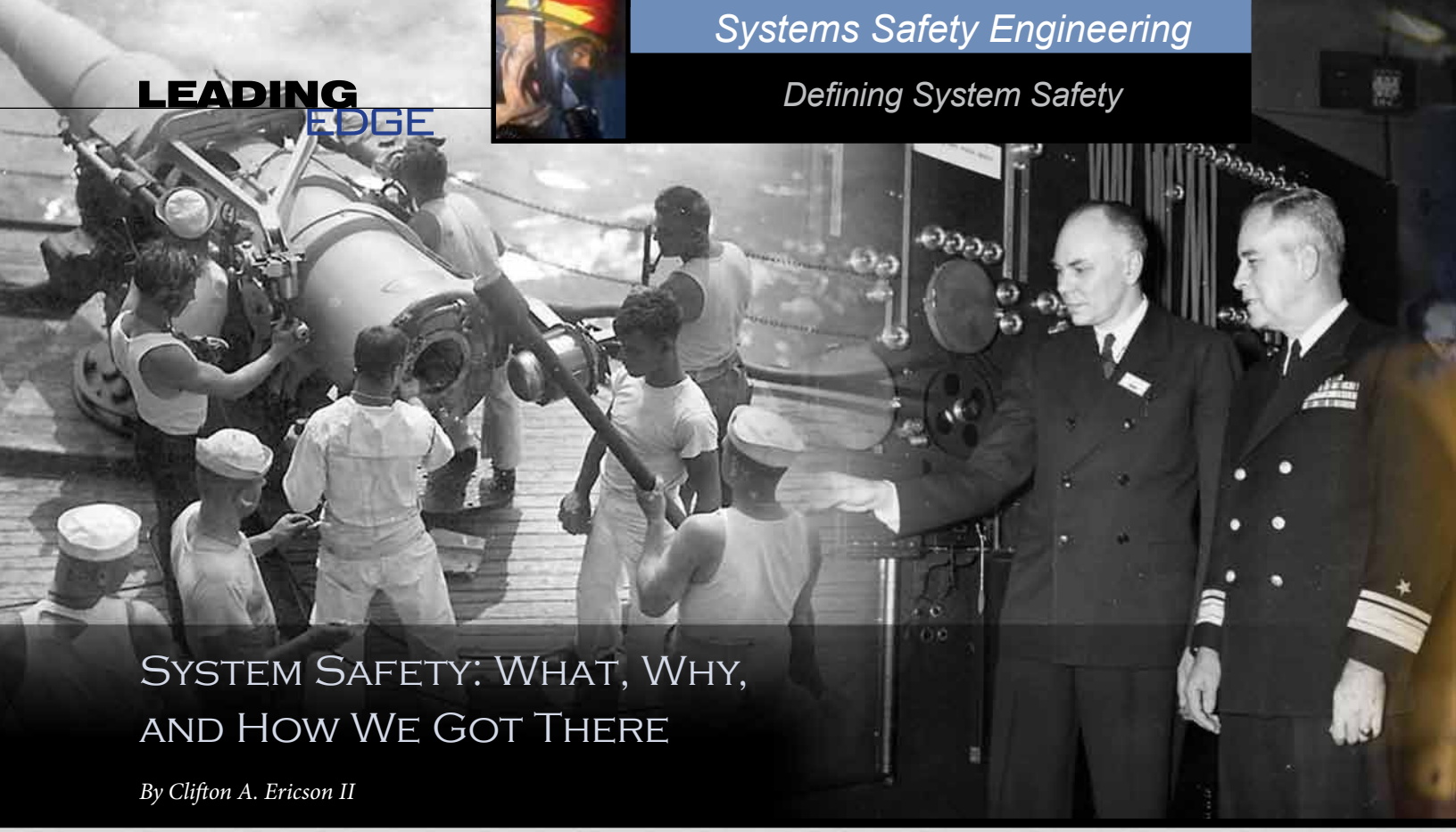


System Safety: What, Why, and How We Got There

By Clifton A. Ericson II

Introduction

To some degree, the endeavor for safety has always been around. Humans have a natural instinct for self preservation (i.e., safety), although some individuals seem to have a higher risk tolerance level than others. Prior to the advent of the system safety methodology, safety was achieved by accident—people did the best job they could, and if an accident occurred, they merely made a design change to prevent a future occurrence and tried again. However, as systems became larger and more techno-complex, knowing how to make a system safe was no longer a simple task. And, as the consequences of an accident became more drastic and more costly, it was no longer feasible to allow for safety by chance. System safety was a natural technological advancement, moving from the approach of haphazardly recovering from unexpected mishaps to deliberately anticipating and preventing mishaps. System safety is a design-for-safety concept; it is a deliberate, disciplined, and proactive approach for intentionally designing and building safety into a system from the very start of the system design. Overall, the objective of system safety is to prevent or significantly reduce the likelihood of potential mishaps in order to avoid injuries, deaths, damage, equipment loss, loss of trust, and lawsuits.

System safety as a formal discipline was originally developed and promulgated by the military-industrial complex to prevent mishaps that were costing lives, dollars, and equipment loss. As the effectiveness of the discipline was observed by other industries, it was adopted and applied to other industries and technology fields, such as commercial aircraft, nuclear power, chemical processing, rail transportation, medical, and agencies such as the Federal Aviation Administration (FAA) and the National Aeronautics and Space Administration (NASA).

What is Safety?

In order to understand ***system safety***, one must understand the related terms ***safe*** and ***safety***, which are closely intertwined; yet each term has different nuances such that they cannot be used interchangeably. In addition, the terms ***hazard***, ***mishap***, and ***risk*** must also be understood, as they are important components of system safety.

Safe is typically defined as freedom from danger or the risk of harm, secure from danger or loss. Safe is a state that is secure from the possibility of death, injury, or loss. A person is considered safe when there is little threat of harm. A system is considered safe when it presents low mishap risk (to users, bystanders, environment, etc.). Safe can be regarded as a state—a state of low mishap risk (i.e., low danger), a state where the threat of harm or danger is nonexistent or minimal.

Safety is typically defined as the condition of being protected against physical harm or loss. Safety as defined in MIL-STD-882D, *Standard Practice for System Safety*, is

> …freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Since 100% freedom is not possible, safety is effectively "freedom from conditions of unacceptable mishap risk." Safety is the ***condition*** of being protected against physical harm or loss (i.e., mishap). The term ***safety*** is often used in various casual ways, which can sometimes be confusing. For example, "the designers are working on aircraft safety" implies that the designers are establishing the conditions for a safe state in the aircraft design. Another example—"aircraft safety is developing a redundant design"—implies a branch of safety (i.e., aircraft safety) that is endeavoring to develop safe system conditions.

It should be noted that safety itself is not a device (as some dictionaries state); it's a state of being safe or an activity working towards creating a safe state. A ***safety device*** is a special device or mechanism used to create safe conditions or a safe design.

The definitions for the terms ***safe*** and ***safety*** hinge around the terms ***hazard***, ***mishap***, and ***risk***, which are closely entwined together. A ***mishap*** is an event that has occurred and has resulted in an outcome with undesired consequences. In system safety, the terms ***mishap*** and ***accident*** are synonymous. In order to make a system safe, the potential for mishaps must be reduced or eliminated. Risk is the measure of a potential future mishap event expressed in terms of probability and consequence. Safety is measured by mishap risk, which is the probability of the potential mishap occurring, multiplied by the potential severity of the losses expected to be experienced when the mishap occurs. Hazards are the precursor to mishaps, and thus potential mishaps are identified and evaluated via hazard identification and hazard risk assessment. Mishap risk provides a predictive measure that system safety uses to rate the safety significance of a hazard and the amount of improvement provided

by hazard mitigation. In summary, mishap risk is a safety metric that characterizes the level of danger presented by a system design via the potential mishap risk presented by system hazards.

What is System Safety?

System safety is often not fully appreciated for the contribution it can provide in creating safe systems that present minimal chance of deaths and serious injuries. System safety invokes and applies a disciplined, formal, and planned methodology for purposely designing safety into a system. A system can be made safe only when the system safety methodology is consistently applied and followed. Safety is more than eliminating hardware failure modes; it involves designing the safe system interaction of hardware, software, humans, procedures, and the environment, under all normal and adverse failure conditions. Safety must consider the entirety of the problem, not just portions of the problem; i.e., a systems perspective. System safety anticipates potential problems and either eliminates them or reduces their risk potential through the use of design safety mechanisms applied according to a safety order of precedence.

The basic interrelated goals of system safety are to:

- Proactively prevent product/system accidents and mishaps
- Protect the system and its users, the public, and the environment from mishaps
- Identify and eliminate/control hazards
- Design and develop a system presenting minimal mishap risk
- Create a safe system by intentionally designing safety into the overall system fabric

System safety is a process for conducting the intentional and planned application of management and engineering principles, criteria, and techniques for the purpose of developing a safe system. System safety applies to all phases of the system life cycle. The basic system safety process involves the following elements:

- System Safety Program Plan (SSPP) development
- Hazard Identification
- Risk Assessment
- Risk Mitigation and Verification
- Risk Acceptance
- Hazard Tracking

Since many systems and activities involve hazard sources that cannot be eliminated, zero mishap risk is often not possible. Therefore, the application of system safety becomes a necessity in order to reduce the likelihood of mishaps, thereby avoiding deaths, injuries, losses, and lawsuits. Safety must be designed intentionally and intelligently into the system design or system fabric; it cannot be left to chance or forced in after the system is built. If the hazards in a system are not known, understood, and controlled, the potential mishap risk may be unacceptable, with the result being the occurrence of many mishaps.

Why System Safety?

In order to achieve their desired objectives, systems are often forced to utilize hazardous sources in the system design, such as gasoline, nuclear material, high voltage, or high-pressure fluids. Hazard sources bring with them the potential for many different types of hazards, which if not properly controlled, can result in mishaps. In one sense, system safety is a specialized trade-off between ***utility value*** and ***harm value***, where utility value refers to the benefit gained from using a hazard source, and harm value refers to the amount of harm or number of mishaps that can potentially occur from using the hazard source. For example, the explosives in a missile provide a utility value of destroying an intended target; however, the same explosives also provide a harm value in the associated risk of inadvertent initiation of the explosives and the harm that would result. System safety is the process for balancing utility value and harm value through the use of design safety mechanisms. This process is often referred to as designed-in safety.

Systems have become a necessity for modern living, and each system spawns its own set of potential mishap risks. Systems have a trait of failing, malfunctioning and/or being erroneously operated. System safety engineering is the discipline and process of developing systems that present reasonable and acceptable mishap risk, for both users and nearby nonparticipants. System safety was established as a systems approach to safety, where safety is applied to an entire integrated system design, as opposed to a single component. System safety takes a sum of the parts view rather than an individual component view.

To design systems that work correctly and safely, an analyst needs to understand and correct how things can go wrong. It is often not possible to completely eliminate potential hazards because a hazardous element is a necessary system component that is needed for the desired system functions, and the hazardous element is what spawns hazards. Therefore, system safety is essential for the identification and mitigation of these hazards.

System safety identifies the unique interrelationship of events leading to an undesired event in order that they can be effectively mitigated through design safety features. To achieve this objective, system safety has developed a specialized set of tools to recognize hazards, assess potential mishap risk, control hazards, and reduce risk to an acceptable level.

Mishaps are the direct result of hazards that have been actuated. Accidents happen because systems contain many inherent hazard sources, which cannot be eliminated since they are necessary for the objectives of the system. As systems increase in complexity, size, and technology, the inadvertent creation of system hazards is a natural consequence. Unless these hazards are controlled through design safety mechanisms, they will ultimately result in mishaps.

System safety is an intentional process, and when safety is intentionally designed into a system, mishap risk is significantly reduced. System safety is the discipline of identifying hazards, assessing potential mishap risk, and mitigating the risk presented by hazards to an acceptable level. Risk mitigation is achieved through a combination of design mechanisms, design features, warning devices, safety procedures, and safety training.

When Should System Safety Be Used?

Essentially, every organization and program should always perform the system safety process on every product or system. This is to make the system safe and also to prove the system is safe. Safety cannot be achieved by chance. This concept makes sense on large safety-critical systems, but what about small systems that seem naturally safe? Again, a system should be proven safe, not just assumed to be safe. A system safety program can be tailored in size, cost, and effort through scaling, based on standards, common sense, and risk-based judgment.

The system safety process should particularly be invoked when a system can kill, injure, or maim humans. It should always be applied as good business practice, because the cost of safety can easily be cheaper than the costs of not doing safety. When system safety is not performed, system mishaps often result, and these mishaps generate associated costs in terms of deaths, injuries, system damage, system loss, lawsuits, and loss of reputation.

The History of System Safety

From the beginning of mankind, safety seems to have been an inherent human genetic element or

force. The Babylonian Code of Hammurabi states that if a house falls on its occupants and kills them, then the builder shall be put to death. The Bible established a set of rules for eating certain foods, primarily because these foods were not always safe to eat given the sanitary conditions of the day. In 1943, the psychologist Abraham Maslow proposed a five-level hierarchy of basic human needs, and safety was number two on this list. System safety is a specialized and formalized extension of our inherent drive for safety.

The system safety concept was not the invention of any one person, but rather a call from the engineering community, contractors, and the military to design and build safer systems and equipment by applying a formal, proactive approach. This new safety philosophy involved utilizing safety engineering technology combined with lessons learned. It was an outgrowth of the general dissatisfaction with the fly-fix-fly, or safety by accident, approach to design (i.e., fix safety problems after a mishap has occurred) prevalent at that time. System safety as we know it today began as a grass-roots movement that was introduced in the 1940s, gained momentum during the 1950s, became established in the 1960s, and formalized its place in the acquisition process in the 1970s.

The first formal presentation of system safety appears to be by Amos L. Wood at the Fourteenth Annual Meeting of the Institute of Aeronautical Sciences (IAS) in New York in January 1946. In a paper titled "The Organization of an Aircraft Manufacturer's Air Safety Program," Wood emphasized such new and revolutionary concepts as:

- Continuous focus of safety in design
- Advance analysis and postaccident analysis
- Safety education
- Accident preventive design to minimize personnel errors
- Statistical control of postaccident analysis

Wood's paper was referenced in another landmark safety paper by William I. Stieglitz titled "Engineering for Safety," presented in September 1946 at a special meeting of the IAS and finally printed in the IAS *Aeronautical Engineering Review* in February 1948. Mr. Stieglitz's farsighted views on system safety are evidenced by the following quotations from his paper:

> Safety must be designed and built into airplanes, just as are performance, stability, and structural integrity. A safety group must be just as important a part of a manufacturer's

> organization as a stress, aerodynamics, or a weights group…
>
> Safety is a specialized subject just as are aerodynamics and structures. Every engineer cannot be expected to be thoroughly familiar with all developments in the field of safety any more than he can be expected to be an expert aerodynamicist.
>
> The evaluation of safety work in positive terms is extremely difficult. When an accident does not occur, it is impossible to prove that some particular design feature prevented it.

The need for system safety was motivated through the analysis and recommendations resulting from different accident investigations. For example, on 22 May 1958, the Army experienced a major accident at a NIKE-AJAX air defense site near Middletown, New Jersey, that resulted in extensive property damage and loss of lives to Army personnel. The accident review committee recommended that safety controls through independent reviews and a balanced technical check be established, and that an authoritative safety organization be established to review missile weapon systems design. Based on these recommendations, a formal system safety organization was established at Redstone Arsenal, Huntsville, Alabama, in July 1960, and AR 385-15, *System Safety*, was published in 1963.

The Navy experienced explosives mishaps on USS *Oriskany* on 26 October 1966, on USS *Forrestal* on 29 July 1967, and on USS *Enterprise* on 15 January 1969. These mishaps caused the loss of many lives, significant ship damage and aircraft loss, and came close to sinking these aircraft carriers. These mishaps motivated new safety programs and concepts for Navy weapon systems and set the stage for the system safety process (see also the Navy Safety Review Board article authored by Caro, Shampine, and Waller in this issue of *The Leading Edge*). Based on the many recorded mishaps, the Secretary of Defense (SECDEF) created the Department of Defense (DoD) Explosives Safety Board (DDESB) to establish a basic set of standards and criteria to reduce explosives related mishaps and their resulting impact. The Chief of Naval Operations (CNO) established the Weapon System Explosives Safety Review Board (WSESRB) to ensure that required explosive safety criteria was incorporated in the design and use of all weapons and/or explosive systems.

As a result of numerous United States Air Force (USAF) aircraft and missile mishaps, the USAF also became an early leader in the development of system safety. In 1950, the USAF Directorate of Flight Safety Research (DFSR) was formed at Norton Air Force Base (AFB), California. It was followed by the establishment of safety centers for the Navy in 1955 and for the Army in 1957. In 1954, the DFSR began sponsoring USAF–industry conferences to address safety issues of various aircraft subsystems by technical and safety specialists. In 1958, the first quantitative system safety analysis effort was undertaken on the Dyna-Soar X-20 manned space glider.

The early 1960s saw many new developments in system safety. In July 1960, a system safety office was established at the USAF Ballistic Missile Division (BMD) at Inglewood, California. BMD facilitated both the pace and direction of system safety efforts when, in April 1962, it published the first systemwide safety specification BSD Exhibit 62-41 titled *System Safety Engineering: Military Specification for the Development of Air Force Ballistic Missiles*. The Naval Aviation Safety Center was among the first to become active in promoting an interservice system safety specification for aircraft: BSD Exhibit 62-82, modeled after BSD Exhibit 62-41. In the fall of 1962, the Air Force Minuteman Program Director, in another system safety first, identified system safety as a contract deliverable item in accordance with BSD Exhibit 62-82.

The first formal SSPP for an active acquisition program was developed by the Boeing Company in December of 1960 for the Minuteman Program. The first military specification (Mil-Spec) for safety design requirements—MIL-S-23069, *Safety Requirements, Minimum, Air Launched Guided Missiles*—was issued by the Bureau of Naval Weapons on 31 October 1961.

In 1963, the Aerospace System Safety Society, which later became the current System Safety Society, was founded in the Los Angeles area. In 1964, the University of Southern California's Aerospace Safety Division began a master's degree program in Aerospace Operations Management from which specific system safety graduate courses were developed. In 1965, the University of Washington and the Boeing Company jointly held the first official System Safety Conference in Seattle, Washington. By this time, system safety had become fully recognized and institutionalized.

Presently, the primary reference for system safety is MIL-STD-882, which was developed for DoD systems. It evolved from BSD Exhibit 62-41 and MIL-S-38130, *Safety Engineering of Systems and Associated Subsystems and Equipment, General Requirements for*. BSD Exhibit 62-41

was initially published in April 1962 and again in October 1962; it first introduced the basic principles of safety but was narrow in scope. The document applied only to ballistic missile systems, and its procedures were limited to the conceptual and development phases "from initial design to and including installation or assembly and checkout." However, for the most part, BSD Exhibit 62-41 was very thorough; it defined requirements for systematic analysis and classification of hazards and the design safety order of precedence used today. In addition to engineering requirements, BSD Exhibit 62-41 also identified the importance of management techniques to control the system safety effort. The use of a system safety engineering plan and the concept that managerial and technical procedures used by the contractor were subject to approval by the procuring authority were two key elements in defining these management techniques.

In September 1963, the USAF released MIL-S-38130. This specification broadened the scope of the system safety effort to include "aeronautical, missile, space, and electronic systems." This increase of applicable systems and the concept's growth to a formal Mil-Spec were important elements in the growth of system safety during this phase of evolution. Additionally, MIL-S-38130 refined the definitions of hazard analysis. These refinements included system safety analyses:

- System-integration safety analyses
- System failure-mode analyses
- Operational safety analyses

These analyses resulted in the same classification of hazards, but the procuring activity was given specific direction to address catastrophic and critical hazards.

In June 1966, MIL-S-38130 was revised. Revision A to the specification once again expanded the scope of the system safety program by adding a system modernization and retrofit phase to the life-cycle phases definition. This revision further refined the objectives of a system safety program by introducing the concept of "maximum safety consistent with operational requirements." On the engineering side, MIL-S-38130A also added another safety analysis: the Gross Hazard Study, which is now known as the Preliminary Hazard Analysis. This comprehensive, qualitative hazard analysis was an attempt to focus attention on hazards and safety requirements early in the concept phase and was a break from other mathematical precedence.

But changes were not just limited to introducing new analyses; the scope of existing analyses was expanded as well. One example of this was the operating safety analyses, which would now include system transportation and logistics support requirements as well. The engineering changes in this revision were not the only significant changes. Management considerations were highlighted by emphasizing management's responsibility to define the functional relationships and lines of authority required to "assure optimum safety and to preclude the degradation of inherent safety." This was the beginning of a clear focus on management control of the system safety program.

MIL-S-38130A served the DoD well, allowing the Minuteman program to continue to prove the worth of the system safety concept. By August 1967, a triservice review of MIL-S-38130A began to propose a new standard that would clarify and formalize the existing specification, as well as provide additional guidance to industry. By changing the specification to a standard, there would be increased program emphasis and accountability, resulting in improved industry response to system safety program requirements. Some specific objectives of this rewrite were to obtain a system safety engineering program plan early in the contract definition phase and maintain a comprehensive hazard analysis throughout the system's life cycle.

MIL-STD-882 Becomes Bedrock of System Safety Procedures

In July 1969, MIL-STD-882 was published—*System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for*. This landmark document continued the emphasis on management and expanded the scope to apply to all military services in the DoD. The full life-cycle approach to system safety was also introduced at this time. The expansion in scope required a reworking of the system safety requirements. The result was a phase-oriented program that tied safety program requirements to the various phases consistent with program development. This approach to program requirements was a marked contrast to earlier guidance, and the detail provided to the contractor was greatly expanded. Since MIL-STD-882 applied to both large and small programs, the concept of tailoring was introduced, thus allowing the procuring authority some latitude in relieving the burden of the increased number and scope of hazard analyses. Since its advent, MIL-STD-882 has been the primary reference document for system safety.

The basic version of MIL-STD-882 lasted until June 1977, when MIL-STD-882A was released. The major contribution of MIL-STD-882A centered on the concept of risk acceptance as a

criterion for system safety programs. This evolution required introduction of hazard probability and established categories for frequency of occurrence to accommodate the long-standing hazard severity categories. In addition to these engineering developments, the management side was also affected. The responsibilities of the managing activity became more specific as more emphasis was placed on contract definition.

In March 1984, MIL-STD-882B was published, reflecting a major reorganization of the "A" version. Again, the evolution of detailed guidance in both engineering and management requirements was evident. The task of sorting through these requirements was becoming complex, and more discussion on tailoring and risk acceptance was expanded. More emphasis on facilities and off-the-shelf acquisition was added, and software was addressed in some detail for the first time. The addition of Notice 1 to MIL-STD-882B in July 1987 expanded software tasks and the scope of the treatment of software by system safety.

With the publication in January 1993 of MIL-STD-882C, hardware and software were integrated into system safety efforts. The individual software tasks were removed, so that a safety analysis would include identifying the hardware and software tasks together in a system.

The mid-1990s brought the DoD acquisition reform movement, which included the Military Specifications and Standards Reform (MSSR) initiative. Under acquisition reform, program managers are to specify system performance requirements and leave the specific design details up to the contractor. In addition, the use of Mil-Specs and standards would be kept to a minimum. Only performance-oriented military documents would be permitted. Other documents—such as contractual item descriptions and industry standards—are now used for program details. Because of its importance, MIL-STD-882 was allowed to continue as a military standard, as long as it was converted to a performance-oriented military standard practice. This was achieved in MIL-STD-882D, which was published as a DoD Standard Practice in February 2000.

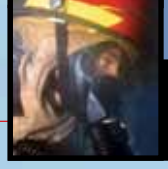
Although system safety is more than MIL-STD-882, the discipline tended to grow and improve with each improvement in MIL-STD-882. System safety is now a process that is formally recognized internationally and that is used to develop safe systems in many countries throughout the world.

Summary

We live in a perilous world comprising many different hazards that present the risk of potential mishaps. Hazards and risk are inevitable; one cannot live life without exposure to hazards. However, this doesn't mean that mishaps are inevitable. We also live in a world composed of technological systems. When viewed from an engineering perspective, most aspects of life involve interfacing with systems of one type or another. For example, consider the following types of systems we encounter in daily life:

- Toasters
- Television Sets
- Homes
- Electrical Power
- Electrical Power Grid
- Hydroelectric Power Plant

Commercial aircraft are systems that operate within a larger transportation system and a worldwide airspace control system. The automobile is a system that interfaces with other systems, such as other vehicles, fuel filling stations, highway systems, bridge systems, etc. Everything can be viewed as a system at some level, and the unique interconnectedness and complexity of each system presents special challenges for safety. Hazards tend to revolve around systems. Safety must be earned through the system safety process—it cannot be achieved by chance.



Determining the Differences Between Safety and Operational Concerns

By Jason Taubel, Shawn T. Thumm, and Steven Gainer

Determining the differences between operational and safety concerns has become increasingly challenging given the increased complexity of systems being developed for use in the U.S. Navy.

Case in point: new ship platforms are being developed with semiautonomous antiterrorism/force protection (AT/FP) weapons replacing manned AT/FP mounts. The increased complexity of these systems—resulting from the use of remote and cutting-edge optics, active stabilization, and detect-control-engage sequences controlled by hardware/software/firmware combinations—creates new operational and safety concerns (see Figure 1).

Knowing the differences between the two is critical in conducting accurate mishap risk assessments as well as in determining operational effectiveness. The following article presents examples and guidelines associated with the separation of operational and safety concerns using a simple case study to illustrate the challenges faced by the systems safety engineer.

The challenge of delineating between an operational concern and a purely safety concern is that in many cases the two disciplines are not mutually exclusive. In reality, there are many overlapping issues, and the only absolute certainty is that personnel, equipment, and the environment must be protected to the maximum extent practicable given the nature of warfare, mission requirements, and fiscal constraints.

The increasing complexity and autonomy of naval systems has resulted in an approach that focuses not just on the design of a system but also on system integration. This is especially true when multiple systems are being assembled into an overarching system of systems.

This system integration approach has been adopted by the system safety community working in the Systems Safety Engineering Division at the Naval Surface Warfare Center, Dahlgren Division (NSWCDD). The Systems Safety Engineering Division is tasked with performing or providing government oversight for contractors performing hazard analyses in accordance with MIL-STD-882D, *Standard Practice for System Safety*. The Platform System Safety Branch focuses on the design and integration of ship platforms and the systems that comprise those platforms. Recent analyses that focus on the integration of AT/FP systems have demonstrated the increased difficulty of discerning between safety and operational concerns.

The recent implementation of the Platform System Safety Approach and the increased complexity make shipboard AT/FP systems (see Figure 2) an ideal case study to help develop guidelines for the systems safety engineer to use to delineate between purely safety and operational concerns, as well as those issues that have both safety and operational applicability. Bottom line—this challenge is not going away anytime soon.

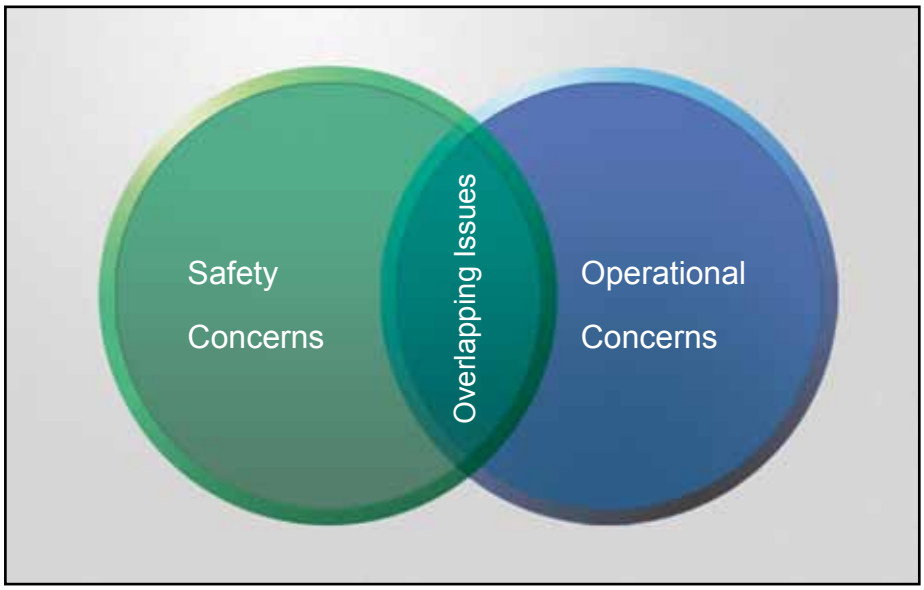


Figure 1. Overlap of Safety Concerns and Operational Concerns

Figure 2. Antiterrorism/Force Protection Weapons Station Aboard T-AO 193

It is important to remember that regardless of whether issues are safety or operational, they need to be addressed in order to provide the warfighter with systems that are both safe to use and operationally effective.

AT/FP systems are generally understood as machine guns located around the perimeter of a ship platform to protect from asymmetric threats. As part of the Platform System Safety Approach, the weapon, mount, and ammunition—as well as the operator—are all considered part of the AT/FP system.

One approach that can be used to separate safety and operational concerns is to create a set of guidelines or "Rules of Engagement" that can be used to categorize each issue or concern. The following list of guidelines has been successfully utilized to help separate safety and operational concerns for AT/FP systems.

- If the concern is commonly mitigated by a safety device/interlock, it is a safety concern.
- If the concern involves unintentional firing of weapons, it is a safety concern.
- If the concern involves a weapon system firing, and it hits the ship in which it was fired from, it is a safety concern.
- If the concern involves weapon system failure/inability to engage the enemy, resulting in ownship personnel injury/death or ship/equipment damage, it is not a safety concern.
- If the concern involves weapon system unsuccessfully engaging the enemy, resulting in ownship personnel injury/death or ship/equipment damage, it is not a safety concern.
- If the concern involves the misidentification of a target, caused by the target, resulting in the target being fired upon, it is not a safety concern.
- If the concern involves the misidentification of a target, caused by the firing vessel, resulting in the target being fired upon, it is a safety concern.

These guidelines are further defined using the following descriptions and scenarios:

If the concern is commonly mitigated by a safety device/interlock, it is a safety concern. It should be noted that safety devices can, and often do, impact operational effectiveness. It is the responsibility of the systems safety engineer to maintain a dialog with the appropriate design team to ensure that operational effectiveness is minimally impacted by safety devices. For example, a deck-mounted, manually operated weapon system introduces the risk of the gunner falling overboard, an obvious safety concern. The installation of a railing

is safety mitigation; however, the railing should be installed in such a way as to have minimal impact on operational effectiveness of the weapon system.

If the concern involves unintentional firing of weapons, it is a safety concern. Safety devices, mechanical and software interlocks, safety procedures, human system integration, and safety testing all serve to prevent unintentional firing. Safety devices and procedures that are meant to prevent unintentional firing must be balanced with the operational requirement for those weapons to by fired when needed. Not balancing these requirements can result in the warfighter purposely defeating a safety device in order to increase operational effectiveness.

If the concern involves a weapon system firing, and it hits the ship in which it was fired from, it is a safety concern. Mechanical weapon stops, as well as pointing and firing cutout zones, are often employed to prevent such mishaps.

If the concern involves weapon system failure/inability to engage the enemy, resulting in ownship personnel injury/death or ship/equipment damage, it is *not* a safety concern. This issue speaks to the ability of a system to accomplish its mission. While the overall survivability of the crew may be in question in the event that the system does not engage a target, this is an operational issue, not a safety issue. However, it must be understood that system safety applies during combat operations, and the system safety program needs to address combat-specific hazards when the system's design, operators, or interfaces contribute to the hazard.

If the concern involves weapon system unsuccessfully engaging the enemy, resulting in ownship personnel injury/death or ship/equipment damage, it is *not* a safety concern. If the weapon system engages an enemy threat and misses the target, resulting in enemy-induced damage, it is not considered a systems safety engineering concern, as the ownship weapon system did not cause the damage—the enemy's weapon did. This situation clearly represents a significant operational performance and survivability concern, but it is not an issue from the systems safety engineering perspective. If the systems safety engineer were to adopt these performance types of issues as safety issues, then it would significantly water down the effectiveness of the safety program, as virtually all issues would become safety issues.

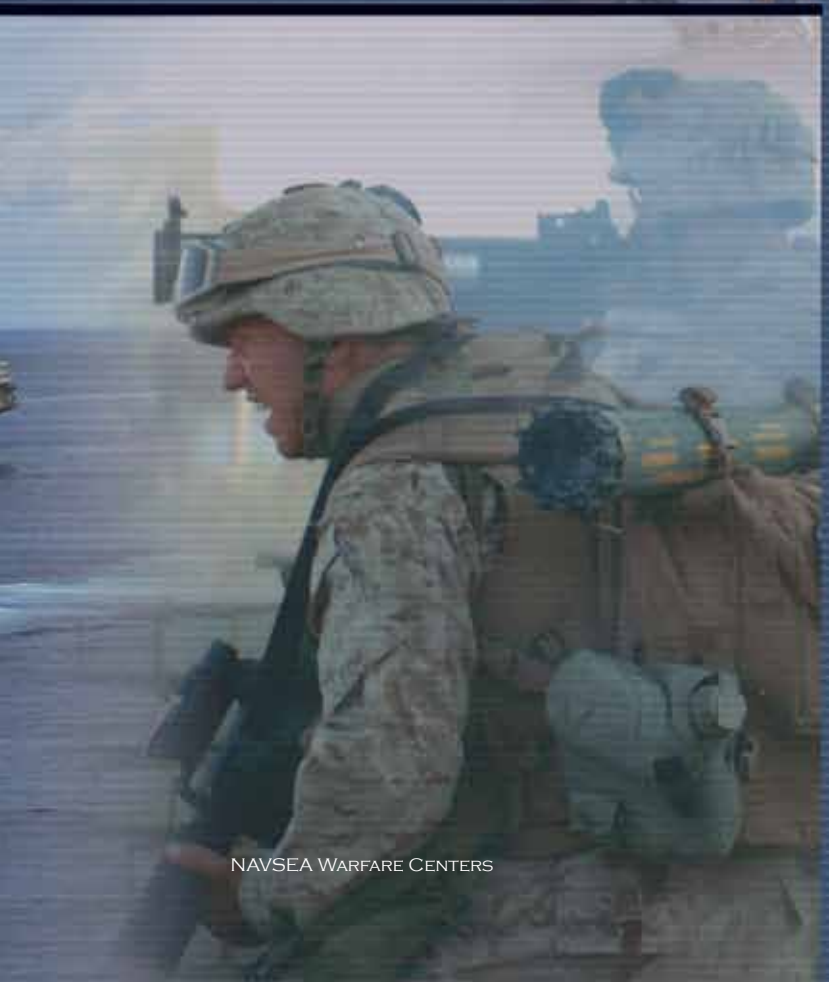
If the concern involves the misidentification of a target, caused by the target, resulting in the target being fired upon, it is *not* a safety concern. An example would be a civilian craft approaching a U.S. Navy ship in such a manner that it meets the entire criterion for the use of deadly force. If the approaching craft fails to respond to ownship and is engaged, it is not a safety concern for the naval vessel. While the naval vessel could employ less lethal force, the decision to do so or not is an operational consideration and not based on safety.

If the concern involves the misidentification of a target, caused by the firing vessel, resulting in the target being fired upon, it is a safety concern. An example would be if a future remote weapon system used an image-recognition program, similar to facial recognition, to detect if the passengers on a small boat were armed, and a software error resulted in identifying the boat as hostile when it was not. If a nonhostile boat were engaged because the rules of engagement were not restrictive enough, that would be an operational and safety concern.

These guidelines are not meant to be all inclusive or apply to all systems but present an example from which system safety programs can develop more enhanced guidelines for their specific systems. Emerging technology in naval systems has always presented new and unique issues that continually challenge systems safety engineers. This boundary will need to be revisited and redefined as systems become even more complex and technologically dependent.

The Role of Environment, Safety, and Occupational Health (ESOH) in the System Safety Process

By Jessica Delgado and James Engbert



NAVSEA Warfare Centers

Imagine, if you will, that you are the program manager (PM) for a large military acquisition program that involves multiple components, including an armored transport vehicle and the munitions that it will fire. This particular system is critical to operations in theater, and your program team is doing everything possible to get the system fielded on time, or early, and within budget. To achieve this goal, your acquisition strategy involves using nondevelopmental items when and where possible, resulting in the pending purchase of thousands of penetrator rounds manufactured outside of the United States. These rounds not only come with a proven record from the foreign services that have used them, but they also have been further qualified by your team against U.S. standards.

Everything has been progressing well thus far; until one day—during the course of a routine design meeting, which includes the involvement of your safety and environmental personnel—an issue is brought up that keeps you up at night. A member of the safety team has brought to your attention that your penetrating round contains a tungsten/nickel/cobalt alloy, a material that has received widespread Department of Defense (DoD) attention over the past few years due to suspected carcinogenic impacts associated with its use. As if that isn't enough, it is further revealed that the use of tungsten nylon bullets has been discontinued within the Army due to suspected leaching into groundwater and subsequent contamination of the area's groundwater.

Supporting details related to both these issues—including ongoing studies, DoD actions, and even the involvement of the Environmental Protection Agency (EPA)—is then presented to the design team. In the midst of this informational buzz, you realize that you are going to have to make some difficult decisions that are likely to influence the success of your program, not just in terms of mission fulfillment, but also in terms of warfighter safety and environmental health. How should you proceed?

Fortunately for you and for all acquisition personnel in similar roles, DoD promotes and, in effect, requires the integration of environment, safety, and occupational health (ESOH) into the systems engineering process. This article will attempt to define ESOH, explain why it is important, and delineate how it is communicated to decision makers—all within the context of the DoD acquisition process. In doing this, some insights as to a path forward for the tungsten scenario presented above will be revealed.

ESOH...What is it?

Within DoD, the acronym ESOH is used to describe the three separate, but related, disciplines of environment, safety, and occupational health (OH) as they relate to risk within the system acquisition process. The following paragraphs provide individual definitions and will attempt to shed some light on the culture that may have influenced the prominence of these disciplines within DoD.

The environmental component of ESOH deals with environmental issues related to the system's impact upon the natural environment in which people live. This includes, but is not limited to, such things as:

- Water, soil, and air pollution
- Harm to marine mammals, including dolphins and manatees
- Destruction of endangered species habitats, such as the gray wolf

The entire life cycle must be assessed when evaluating environmental risk, including manufacturing, testing, fielding, and demilitarization and disposal. It is also appropriate to consider compliance with the National Environmental Policy Act (NEPA) and Executive Order (EO) 12114, *Environmental Affects Abroad of Major Federal Actions*, when assessing environmental ESOH risk. These two elements of environmental risk are so highly regarded within DoD that they are called out separately within Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*, and other guiding DoD documents.

Of the three parts of ESOH risk, the environmental component may be the most challenging to evaluate per the risk assessment methodologies employed by DoD acquisition safety professionals, most notably those found within Military Standard (MIL-STD)-882D, *Standard Practice for System Safety*. Often, many unknowns surround long-term fielding of a military system, which make assessment of potential hazards or associated mishaps difficult during the initial acquisition process. For instance, it would be very difficult to take into account the progression and maturation of environmental research and regulations that would likely occur during a system's lifetime, Likewise, it would be difficult to ascertain the many locations it may function in around the world—all characterized and influenced by their own unique set of requirements and sensitive environmental issues and areas. As an alternative approach, the safety process would serve the program well by communicating ESOH risks that could potentially become programmatic risks. For instance, failure of a program to even address NEPA or EO 12114 could negatively impact a program's performance, schedule, or cost and should be communicated to the PM as part of the system safety process.

As a point of clarity, a good definition of the term ***environment*** associated with ESOH also includes a discussion of what it is not intended to capture: specifically, the impact of the environment, both natural and man-made, upon a system. In other words, what are the impacts to the system caused by such things as lightning strikes, saltwater, and electromagnetic interference? Those impacts are instead captured in other parts of the systems engineering process not directly related to ESOH. While these two very different uses of the term ***environment*** do enjoy some overlap within the acquisition process—such as the case of corrosion, which can simultaneously impact both a system's integrity (via oxidation) and the health of the environment (via the hazardous components used to counteract oxidation)— they are, for the most part, very different disciplines and should be treated as such. A thorough understanding of this distinction will serve the acquisition professional well in understanding ESOH in the acquisition process.

In terms of the tungsten example previously discussed, potential environmental ESOH risks worthy of consideration by the program team mostly include those upon groundwater and soils due to possible releases from materials spent on the training and test ranges. The PM is responsible, therefore, for assessing this environmental ESOH risk as accurately as possible and to communicate that risk to all decision makers involved in the program. If the PM and the team determine that significant risk exists, and if the acquisition program is still in the early stages, it may be feasible to find another suitable material and still meet program cost, schedule, and performance. In cases where the program is further down in the acquisition life cycle or where no suitable replacements exist that are realistic, then the ultimate decision whether to proceed as planned is made, taking into account the ESOH risk and the mission priority. If the program moves forward, the risk must be accepted.

As for historical influences that may have shaped DoD's own interest in addressing environmental risks, they likely parallel a general tone of environmental responsibility in the United States beginning in the late 1960s, spurred on by such events as Rachel Carson's 1962 penning of the controversial *Silent Spring*, the passing of NEPA in 1969, and President Nixon's establishment of the EPA in 1970. This era of environmental stewardship continued as this country watched a number

of man-made environmental disasters occur, such as the Love Canal unveiling in 1978 and the Three Mile Island incident in 1979.

The ***safety*** component of ESOH deals with safety issues associated with the system. Although most emphasis is usually placed upon identifying safety ESOH risks associated with the operation of the system—as that is where the majority of hazards are realized into mishaps—the entire life cycle should be assessed, to include manufacturing, testing, maintenance, storage, handling, and demilitarization and disposal. Direct assessment of the manufacturing process usually falls outside the scope of the acquisition safety professional, as these risks are normally characterized as OH and are addressed by the manufacturing facility through corporate safety and health policies and procedures. Such assurances for a safe workplace can also be made through contract requirements. Examples of risks associated with safety are inadvertent explosion (of a munition), pinch points, and vehicle rollover.

Safety ESOH risk lends itself very well to the risk assessment methodologies employed by the DoD acquisition safety professional, most notably those found within MIL-STD-882D. Here, one finds solid methodologies for assessing, reporting, communicating, and accepting safety ESOH risks within the acquisition process.

Again, with reference to the tungsten example, one does not readily find any direct safety ESOH risks; however, upon closer assessment, the impact of a friendly-fire incident (for which the tungsten hazard is most readily realized due to muscle-tissue penetration) would certainly be considered a safety issue, even if somewhat indirect in nature. Although there may also be ESOH risks associated with manufacturing or demilitarization/disposal of the tungsten material that could be classified as safety risks, they might better be captured in the OH portion of ESOH.

Regarding historical influences upon safety in DoD, one sees a slow evolution of safety within 20th-century industrial America that DoD paralleled, whether they were in the areas of automobile safety, appliance safety, or home safety. Additionally, within DoD's unique history reside a number of tragic events that were instrumental in driving the safety train within defense systems, including—but not limited to—the Army's Nike missile accident in 1958 and the Navy's tragic explosions aboard USS *Oriskany* and USS *Forrestal* in 1966 and 1967, respectively. These events clearly showed the need for greater safety effort within all of DoD, so a prompt response was elicited.

The OH component of ESOH also deals with safety issues of the system; however, it tends to address those risks to humans associated with its manufacturing, maintenance, and disposal, as well as any life-cycle risks associated with the use of hazardous materials (HAZMATs) in the system.

Additionally, OH would address some aspects of human systems engineering that adversely impact the warfighter. Examples of the former might include:

- Use of carcinogenic solvents during manufacturing
- Toxic gas and noise resulting from weapon firing
- Cadmium exposure associated with handling of corroded equipment

Examples of the latter might also include:

- Eyestrain due to poor video displays
- Trip hazards due to poorly designed floor plates
- Low-hanging light fixtures in a common passageway

A point worth noting when discussing OH in the context of acquisition is the frequent direct overlap between safety risks and OH risks, whereby a risk may be classified in both categories. The important thing is that it is captured in one of the ESOH assessments.

Whereas OH ESOH risks can and should be managed via MIL-STD-882 methodologies, additional techniques are sometimes necessary and encouraged to communicate these risks to those who might benefit the most. For instance, if manufacturing a particular military system is known to endanger a plant worker's health, such as the milling of beryllium materials, the safety professional may need to communicate that risk directly to the contractor to ensure that workers are being adequately protected. Alternatively, if the material has been targeted for reduction or elimination within DoD, the safety professional needs to ensure that other options are being considered by the program. Although the MIL-STD-882 process provides for this type of interchange, the timing of some OH risks (in particular, early on during manufacturing) is different from that of typical safety risks (such as those experienced during fielding), thus possibly necessitating additional reporting and communication.

In terms of the tungsten example previously discussed, potential OH ESOH risks worth assessing would include those associated with manufacturing the metal alloys. Additionally, consideration of test-range contamination and its impact on human health would warrant consideration as part of OH in conjunction with environmental impact.

Some basic historical research reveals an awareness in this country spanning back at least into the early 20th century, when child labor laws were on the forefront of the American conscious. The level of rigor, however, with which modern Occupational Safety and Health Administration (OSHA) oversight and regulations function was not fully realized until the past few decades, as science and research started producing evidence of afore-unnoted health hazards, both occupational and nonoccupational (e.g., cigarette smoking is bad for one's health; asbestos materials shouldn't be inhaled; exposure to leaded gasoline is harmful to developing humans).

ESOH...Why is it important?

Among the many roles and responsibilities that a PM faces are the tasks of integrating ESOH considerations into the systems engineering process and managing ESOH risks within the program. These requirements are identified within DoDI 5000.02, which charges the PM with the following responsibilities:

- The PM shall integrate ESOH risk management into the overall systems engineering process for all developmental and sustaining activities.
- The PM shall eliminate ESOH hazards where possible and manage ESOH risks where hazards cannot be eliminated.
- The PM shall ensure that appropriate human systems integration and ESOH efforts are integrated across disciplines and into systems engineering.

By way of DoDI 5000.02, DoD also endorses the use of MIL-STD-882D, which provides its own level of instructions and definitions germane to the role of the PM in addressing ESOH issues in the acquisition process; these include:

- DoD is committed to protecting private and public personnel from accidental death, injury, or occupational illness.
- Within mission requirements, DoD will also ensure that the quality of the environment is protected to the maximum extent practical.
- DoD has implemented environmental, safety, and health efforts to meet these objectives. Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations.

This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities.

System safety is the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk within the constraints of operational effectiveness and

suitability, time, and cost, throughout all phases of the system life cycle.

A mishap is an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Aside from complying with DoDIs and accepted safety methodologies, integrating ESOH into systems engineering just makes good business sense. Unaddressed, ESOH risks can readily translate into programmatic risks, ultimately costing the program in terms of performance, cost, and schedule. Failure to address environmental concerns can lead to poor public relations and, ultimately, to program shutdown. Failure to address safety concerns can result in preventable injuries to the warfighter, and failure to address OH issues can lead to a poorly performing and unhealthy workforce. This list could go on, but it is sufficient to say that early identification and management of all ESOH risks will go a long way to both ensuring compliance with all applicable ESOH laws and regulations, and moving toward the ultimate success of the acquisition program and safety for the warfighter.

As a final note regarding the PM's task of integrating ESOH considerations into the systems engineering process, it is useful to point out that safety methodologies and instructions provided by DoD and industry provide some latitude for its implementation into an acquisition program. For instance, some safety programs focus on the safety portion of ESOH in their analyses and documentation and rely on the additional support of subject matter experts in the area of environment and OH risks. Other programs prefer a more comprehensive approach, whereby the safety professional takes ownership of the entire ESOH spectrum in their analyses and documentation. It is also important to realize that when discussing ESOH in the context of acquisition, the three components of ESOH may overlap. For instance, toxic gas could be regarded as an environmental risk, a safety risk, and an OH risk. In some cases, it may be adequate to capture the risk under only one of the categories (e.g., for safety and OH, either one may suffice). For others, it may be necessary to call them out under both categories (e.g., for hazards impacting both the environment and the human). Regardless of the safety professional's approach, the important thing is that all three elements of ESOH are sufficiently considered in the system safety process.

ESOH...How is it communicated?

The venue that connects the relationship among the environment, safety, and OH aspects of ESOH in DoD acquisition programs takes the form of a document dubbed the Programmatic Environment, Safety, and Occupational Health Evaluation, more commonly known as the PESHE.

According to DoDI 5000.02, the PM, regardless of the program's Acquisition Category level, shall prepare a PESHE that incorporates the MIL-STD-882D process. This document includes:

- The identification of ESOH responsibilities
- The strategy for integrating ESOH considerations into the systems engineering process
- The identification of ESOH risks and their status
- A description of the method for tracking hazards throughout the life cycle of the system

The composition of the PESHE is finely attuned with the aforementioned definition of system safety. The PESHE also includes identifying hazardous materials, wastes, and pollutants (discharges/emissions/noise) associated with the system and planning for their minimization and/or safe disposal , as well as a compliance schedule covering all system-related activities for the NEPA and EO 14112.

DoDI 5000.02 also states that a summary of the PESHE shall be incorporated in the Acquisition Strategy. The PESHE is not only a required document per DoD and the Department of the Navy (DON), but as already discussed, elements of it are also required by statutory requirements, such as NEPA compliance, which is mandated in sections 4321–4370d of title 42 of the U.S.C. These requirements are also flowed down into other DON and United States Marine Corps (USMC) documents, such as Secretary of the Navy Instruction (SECNAVINST) 5000.2D, Chief of Naval Operations Instruction 5090.1C, and Marine Corps Order P5090.2A—all of which stipulate the development of the PESHE in DON and USMC acquisition programs. For example, SECNAVINST 5000.2D—an instruction that governs the implementation and operation of the defense acquisition system and the joint capabilities integration and development system for DON and USMC acquisition programs—states the following:

> This Acquisition Strategy shall incorporate a summary of the Programmatic ESOH Evaluation (PESHE), including ESOH hazards, associated risks, and proposed mitigation plans; a strategy for integrating ESOH considerations in the systems engineering process; identification of ESOH responsibilities; a method for tracking progress; and a schedule for NEPA (42 U.S.C. sections 4321–4370d) and EO 12114 compliance for events or proposed actions throughout a program's life cycle.

This programmatic document is a tool to communicate to decision makers how ESOH affects the program. For all programs, the PESHE shall be written at Milestone[a] (MS) B and updated at MS C. The PESHE shall be updated again at Full Rate Production/Deployment, where it transitions from an initial planning document to an ESOH risk-management tool. For ship programs, the PESHE process is to commence even earlier, being first required at MS A.

A typical PESHE includes sections discussing programmatic efforts in the following five areas:

1. **Environmental Compliance**—This section describes procedures for determining environmental compliance, defines compliance requirements, and analyzes possible impacts of compliance on the program's cost, schedule, and performance.
2. **NEPA/EO 12114**—This section describes the preparation requirements of detailed statements on major federal actions significantly affecting the quality of the human environment This section also includes a compliance schedule of programmatic activities with NEPA/EO 12114 and planned NEPA documentation as applicable.
3. **System Safety/OH**—This section describes the procedures used to identify and eliminate hazards; defines risk levels; and summarizes the impact of potential health and safety hazards, including loss of life, personnel injury, damage to environment, or damage to equipment.
4. **Explosive Safety**—This section identifies explosives ESOH risks and mitigation procedures.
5. **Hazardous Material (HAZMAT)/Pollution Prevention (P2)**—This section outlines the goals of the HAZMATs/waste program and related issues, and includes the process for identifying, tracking, handling, and disposing of HAZMATs that cannot be eliminated. In terms of P2, this section describes programmatic P2 initiatives and processes for preventing or minimizing impacts on natural resources.

The importance of the PESHE does not reside exclusively in the fact that it is required for all acquisition programs. More importantly, it ensures awareness, proper planning, and compliance of ESOH issues throughout the program's life cycle. This versatile document also serves as a "snapshot" of how ESOH issues and risks are being managed. This "snapshot" describes past, present, and future programmatic activities related to ESOH, and in

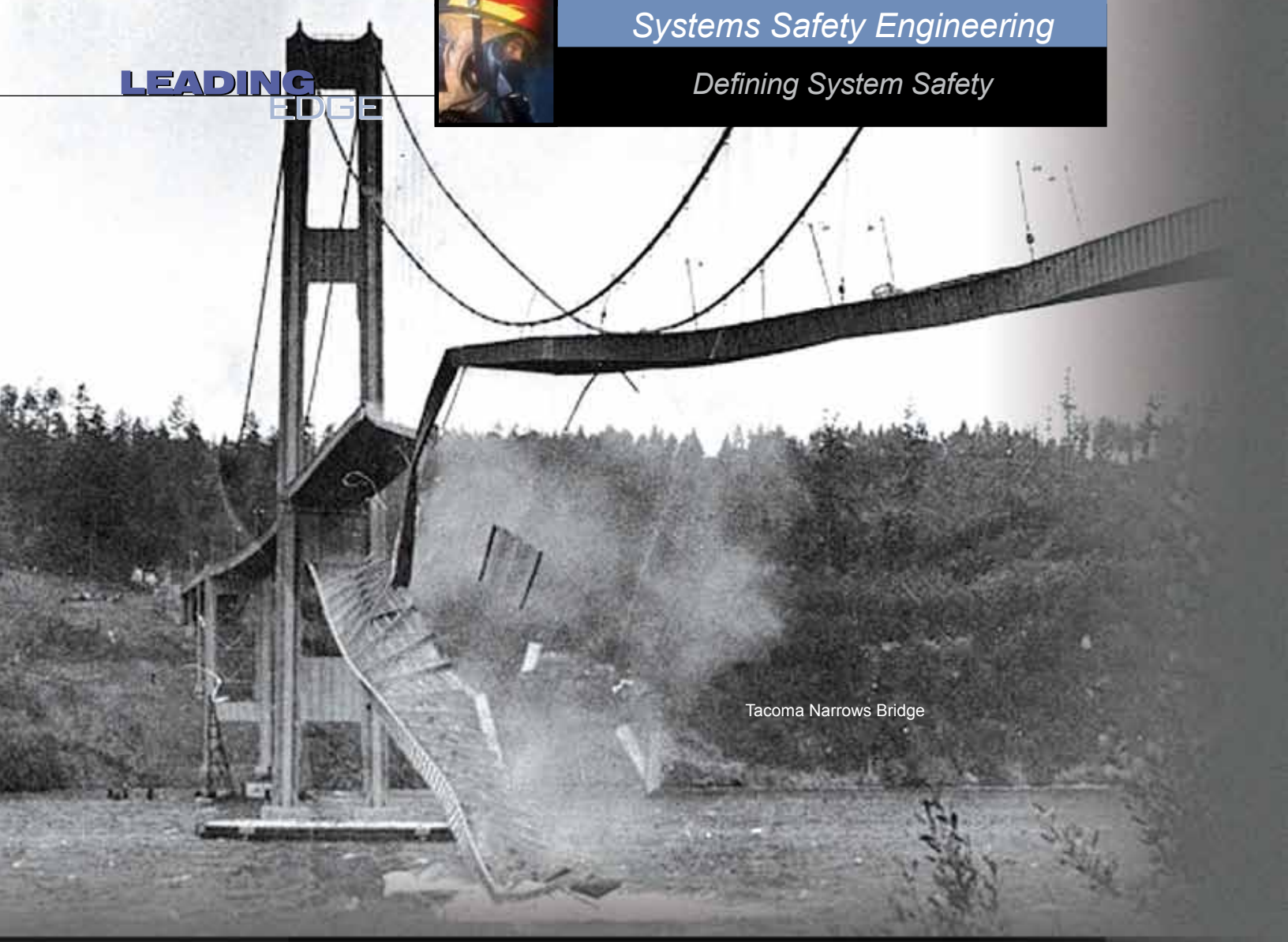
that sense, the PESHE also provides a history of all efforts to comply with ESOH policies and regulations while minimizing and mitigating associated risks. On the other hand, the PESHE is also a "self-correcting exercise." The very exercise of developing the PESHE may reveal flaws, deficiencies, or needs of the program that can be corrected or anticipated before final signature of the document. For example, if an early PESHE version reveals the presence of a HAZMAT of concern, the program has an opportunity to plan by avoiding or minimizing the use of the particular HAZMAT. Had the PESHE process not been undertaken, this deficiency may not have been uncovered until a key programmatic review such as a Milestone Decision Authority review, where the chances of programmatic risks increase and can be translated into schedule delays and additional costs to resolve the problem.

The PESHE is not designed to supersede other ESOH plans, analyses, and reports (e.g., System Safety Management Plan, P2 Plan, and Health Hazard Assessment). Instead, the PM incorporates these documents by reference, as appropriate. However, to the maximum extent possible, the PM should minimize duplication of effort and documentation and give preference to recording ESOH information in the PESHE, as opposed to maintaining a series of overlapping, redundant documents. Ultimately, the PESHE is a stand-alone document that contains enough material to inform the reader about the entire programmatic ESOH effort.

In summary, ESOH describes the three separate, but related disciplines of environment, safety, and OH as they relate to risk within the system acquisition process. Its importance resides mainly in the PM's responsibilities of integrating ESOH into the systems engineering process and managing ESOH risks within the program's life cycle. The venue used for these purposes is the PESHE, which serves as a planning document in the early stages of the program and evolves to a risk-management tool as the program progresses. The ultimate goal of incorporating ESOH into a program's life cycle is to achieve a holistic balance between minimizing risks to the program, the environment, and the end user while pursuing the delivery of equipment capable of accomplishing its mission.

Endnote

a. The point at which a recommendation is made and approval sought regarding starting or continuing an acquisition program. MSs in acquisition programs are:
   A—Approves entry into Technology and Development Phase
   B—Approves entry into the Engineering and Manufacturing Phase
   C—Approves entry into Production and Deployment



Tacoma Narrows Bridge

The Case for Providing Actionable Safety Hazard, Near Miss, and Mishap Information to the Acquisition Community

By James H. Yee, Billie Jo Hynson, and Nga Pham

The great liability of the engineer compared to men of other professions is that his works are out in the open where all can see them. His acts, step by step, are in hard substance. He cannot bury his mistakes in the grave like the doctors. He cannot argue them into thin air or blame the judge like the lawyers. He cannot, like the architects, cover his failures with trees and vines. He cannot, like the politicians, screen his shortcomings by blaming his opponents and hope the people will forget. The engineer simply cannot deny he did it. If his works do not work, he is damned.—Herbert Hoover

Herbert Hoover understood well the weighty responsibility and accountability that has burdened the engineer since the beginning of time. Although man may boast of magnificent engineering achievements, his pride may be appropriately tempered by many more failures over time. Engineering history is replete with mistakes, failures, and mishaps. We need look no further than the *Titanic*, the Tacoma Narrows Bridge, and the space shuttle *Challenger* to see stark examples of engineering shortcomings, and their associated consequences. Only a relative few have been immortalized in the annals of history owing to their tremendous cost in lives and/or resources. Countless more have escaped the scrutiny of the broader public eye and the indelible ink of the historian. However, each one can be the source of leading indicators and lessons critical to the understanding and prevention of future mishaps.

Arguably, the greatest tragedy of mistakes occurs if we don't learn from them. Learning from our mistakes affords the best insurance against repeating history or, even worse, permitting greater calamity. As much as learning from mistakes seems to be an elementary concept, for one reason or another, we sometimes fail to do it. Whether attributable to expediency, cost cutting, poor communication, or just plain engineering arrogance, the result is the same…increased risk.

In an inherently hazardous environment, such as that associated with military operations, the likelihood of mistakes is elevated, and the consequences are increasingly grave. Given this fact, it is incumbent upon the Navy acquisition community to ensure that the systems that are delivered to our Sailors and Marines are both safe and effective. ***Safe*** is a relative term, and it is unrealistic to expect that every system will be effective and safe 100% of the time. Mistakes, failures, and mishaps have been, and unfortunately probably will be, a part of military operations until the end of warfare. So the challenge to the acquisition community is to do everything within its power to design and develop systems that are as safe and fault tolerant as practicable, learn and incorporate the lessons from operational use, and continuously strive to avoid the mistakes of the past.

Navy Safety Philosophy and Mandate

Safety is of primary importance in our society and our military. Sending our nation's sons and daughters into harm's way is difficult enough without having to worry about self-inflicted injuries. Recently, the Secretary of the Navy, Chief of Naval Operations, and Commandant of the Marine Corps signed out the Department of the Navy (DON) Safety Vision. This document reinforces past policies and underscores the department's commitment to safety by reflecting on progress toward achieving safety objectives and plotting a course for the future.

Notably, related to hazard awareness and communication, the Safety Vision requires Navy commands to:

> **Aggressively and transparently communicate safety successes, share hazard awareness and share near-miss lessons learned.**
>
> - The tenets of any successful safety program include the ability to rapidly assess and share hazard information and disseminate lessons learned. Decisive leadership is critical in creating an environment whereby subordinate commands feel empowered to do this without fear of adverse action. Sharing urgent safety information need not be confined to established and often cumbersome reporting systems—organizations should utilize the most effective and efficient means at their disposal.[1]

This requirement is part of the Safety Vision because Navy leadership understands that effective information sharing is a critical prerequisite to effective decision-making and subsequent action. However, the fact that the requirement is included as part of the course for the future implies that we are not there yet.

Arguably, the safety culture varies between the different Navy warfighting communities (e.g., air, surface, subsurface, special operations). The level of safety risk that is deemed acceptable varies, as well

as the propensity and willingness to share safety-related information. The reasons for this variance are broad, subject to opinion, and beyond the scope of this discussion. Nonetheless, the mandate from the Safety Vision requires the culture to migrate from wherever it is right now to a point where there is open and efficient sharing of safety information throughout the enterprise, both good and bad.

Achieving this objective will afford opportunity for timelier and better informed safety decision-making across all stakeholders. The stakeholder community ranges from the individual Sailor to the highest echelon commands. Every Sailor and command needs to play a proactive role in the identification and mitigation of safety hazards primarily because hazards can reside anywhere. Within this paradigm, the acquisition community can, and must, play a central role.

Acquisition Community: Uniquely Positioned to Influence Safety

The ability to leverage safety information from the fleet is essential to the end objective of eliminating or mitigating mishap risk. In November 2005, Deputy Assistant Secretary of the Navy for Safety (DASN (Safety)) issued a progress report on the Secretary of Defense's (SECDEF's) challenge of 50% mishap reduction. Within that report, DASN (Safety) highlighted a new challenge in the FY06–11 Department of Defense Strategic Planning Guidance to continue reducing mishaps and mishap rates by 75% by the end of FY08, using FY02 statistics as a baseline. The principles underlying this effort are threefold:

1. Mishaps should not be accepted as business as usual
2. Most mishaps are preventable
3. Mishap prevention leads to increased readiness

In June 2006, the SECDEF issued a memorandum on reducing preventable mishaps. The tenets of this memorandum have since been reaffirmed by the current Secretary. In this memorandum, SECDEF emphasized accountability at all levels with regard to mishap prevention. He also states,

> If we need to change our training, improve our material acquisition, or alter our business practices to save the precious lives of our men and women, we will do it. We will fund as a first priority those technologies and devices that will save lives and equipment. We will retrofit existing systems, and consider these devices as a "must fund" priority for all new systems. We can no longer consider safety as "nice to have."

Although this challenge encompasses all facets of Department of Defense (DoD) operations, including off-duty and ashore mishaps involving military personnel, the acquisition community has a unique opportunity to make a significant contribution toward achieving mishap reduction objectives, thereby improving the overall safety posture and readiness of the fleet.

The acquisition community is in the best position to eliminate or substantially mitigate hazards associated with systems because of early involvement in concept exploration and system development. Factoring safety into requirements, design decisions, and component selections is the most cost-effective way to reduce or eliminate mishap risk.

Figure 1 illustrates the relationships among hazard causal factors, hazards, mishaps, and effects. The following is an example of each element within the hierarchy:

> An exposed sharp edge in a relay cabinet (hazard causal factor) frays the insulation on a wire (hazard) leading to inadvertent retraction of missile restraining latches and a dropped weapon (mishap). As a result, the missile suffers stabilizer damage (effect).

The most effective approach to mishap prevention is the mitigation or elimination of hazards that may potentially lead to a mishap. Truly effective elimination and substantial mitigation of hazards is most achievable during the system development process. In the previous example, elimination or covering of the sharp edge would be the most effective way to mitigate the hazard's causal factor.

What is commonly referred to as the safety design order of precedence in MIL-STD-882D (series), *Standard Practice for System Safety*, lists "eliminating hazards through design selection" as the first and most effective method for ensuring safety. Subsequent mitigations, in order of preference, include incorporating safety devices, providing warning devices, and developing procedures and training.

The challenge facing the acquisition community continues to grow in dimension and complexity. The Maritime Strategy calls for an unprecedented level of joint, interagency, and coalition integration and interoperability to support naval operations comprising:

- Forward Presence
- Deterrence
- Sea Control
- Power Projection

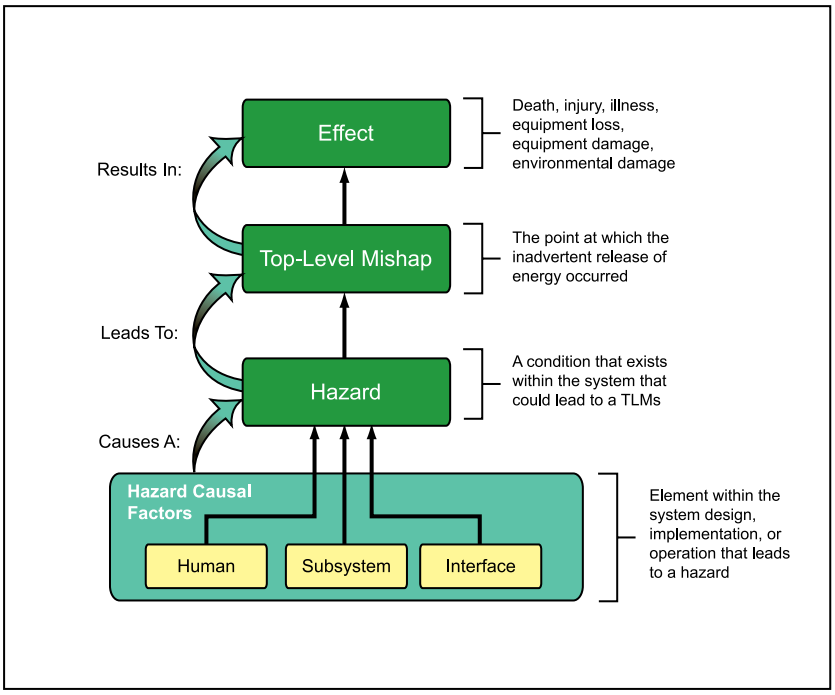


Figure 1. Hazard Relationships

- Maritime Security
- Humanitarian Assistance
- Disaster Response

Combined with a push toward near-seamless interoperability, this mandate multiplies the complexity of the technical challenges facing acquisition professionals. Likewise, there is a commensurate increase in the complexity of the system safety challenges.

This fact alone underscores the case for providing actionable safety hazard, near-miss, and mishap information to the acquisition community. The increasing complexity of our systems, not to mention the value of our people, necessitates an acquisition process in which learning is a core part of the culture. The consequences of failure are high, and propagation of hazards is unacceptable.

The Value of Hazard Awareness

Lessons learned through fleet operations and mishaps provide a rich source of information that can and should be used to increase awareness and understanding of hazards. The fundamental value of such information is multidimensional. Primary benefits include:

- *Validating or invalidating previously incorporated hazard mitigations*—Mitigations are normally incorporated into the system design before actual fielding. Sometimes, due to various reasons, what was thought to be an adequate mitigation during system development and test may have reduced effectiveness in actual employment. Fleet hazard/mishap information will provide information on hazard mitigation effectiveness.
- *Providing insight into how a system is being used in the fleet, and how that usage diverges from original design intent*—Usage outside of the original concept of employment may adversely impact the safety of a system. Safety is a highly contextual facet of system performance that is in large part reliant upon use of a system as designed, in the anticipated environment, by an operator population with specific skills. A stark illustration of this point taken from an actual mishap is when a man decided to use a lawn mower to trim his hedge. This type of unintended utilization of a lawn mower resulted in serious injury due to the bypassing of safety mitigations and the introduction of new and unforeseen hazards.
- *Providing insight into significant changes in the technical, operational, and/or physical aspects of the environment*—Hazard mitigations in the design of a system are incorporated based on the defined concept of operations (CONOPS). Given the ever-expanding

maritime mission, it is certainly within the realm of possibility that key aspects of the environment have changed enough to impact safety. Fleet hazard/mishap information may provide critical insight into these changing factors.

- *Highlighting the safety qualities of various design methods, materials, software, etc.*—The rapid infusion of new systems into the warfare environment will likely shed light on the safety performance of associated concepts, technologies, and materials. Fleet hazard/mishap information may provide early and valuable input to current and future design and upgrade decisions.
- *Surfacing new, unforeseen hazard conditions*—Despite the best intentions to eliminate and mitigate all hazards, time and money are seldom sufficient to afford the opportunity to do so. Operational use will likely uncover new, unforeseen hazards that should be addressed before they precipitate a mishap. Using fleet hazard/mishap information, the acquisition community may be able to detect leading indicators of unexpected safety issues, allowing for preemptive action and incorporation into design guidance.

The ability to leverage actionable safety information to realize these benefits is crucial to improving safety throughout the fleet. However, in a world of vast and competing demands, there are a number of significant challenges to providing actionable safety hazard, near-miss, and mishap information to the acquisition community.

The Current Challenges

The primary challenges to transitioning actionable safety information from the fleet to the acquisition community are threefold. First, there is the challenge of nurturing the requisite atmosphere in which the reporting of safety information is part and parcel to the culture. Second, there is the challenge of defining, developing, and implementing the processes and mechanisms via which the information may be communicated. Finally, there is the challenge of defining the specific safety information itself.

A positive safety culture is a critical aspect to any successful safety-related program. The culture must be geared toward open and timely reporting without fear of negative consequences. Tying safety performance to rewards and recognition can certainly be a good thing. However, an unintended consequence may be the emergence of a culture

that discourages reporting of hazards and near mishaps that do not exceed the mandatory reporting threshold. This culture would emerge if reporting would result in negative impacts to things such as other awards and promotion.

Part and parcel to a positive reporting culture is the implementation of processes and mechanisms for reporting that are readily available, easy to understand, and user friendly. Reporting mechanisms that do not meet these requirements will quickly become a burden to Sailors and will likely discourage reporting. The design and implementation of reporting mechanisms need to leverage, to the greatest extent possible, processes and tools that are already institutionalized in the shipboard environment, taking care not to require duplicate information.

Last, but not least, the best safety culture combined with the latest processes and reporting mechanisms are all for naught without clear data definition. A clear and widely accepted data standard for mishap, near miss, and hazard reporting is crucial to the utility of the data by the acquisition community. Absent data standardization, the potential for inaccurate analyses and conclusions is high. With proper data standardization, the acquisition community will be able to perform appropriate analyses, and provide reliable and value-added safety recommendations for consideration in current and future system development efforts.

These challenges, although formidable, are not insurmountable. There are collaborative efforts within the Navy safety community and fleet geared toward addressing all these challenges and coming up with viable solutions pursuant to the DON Safety Vision. As the saying goes,

> Nothing worthwhile comes easily. Half effort does not produce half results. It produces no results. Work, continuous work, and hard work is the only way to accomplish results that last.

A key ingredient to ultimate success in safety is continuing to focus on ways to improve the process. With support from senior Navy leadership, the threats posed by hazardous environments will be mitigated, and the fleet will be safer.

Reference

1. SECNAV Memorandum for Distribution, Subject: DON Safety Vision, 22 January 2009, safetycenter.navy.mil/DON-Safety/ltr_FinalVisionStatementwithexplanatorypara.pdf.

DoD Acquisition and Technology Programs Task Force: Promoting System Safety Throughout the Life Cycle

By Elizabeth Rodriguez-Johnson and Mark Geiger

The Department of Defense (DoD) Acquisition and Technology Programs Task Force (ATP TF) seeks to put action behind the words, "We have no greater responsibility than to take care of those who volunteer to serve." The DoD set goals in 2003 and 2006 to reduce prevent able accidents by 50 percent and 75 percent, respectively. In May 2007, the Secretary of Defense reiterated the Department's target as "zero preventable accidents," stating, "We can no longer tolerate the injuries, costs, and capability losses from preventable accidents."

The Defense Safety Oversight Council (DSOC) was established in 2003 to implement and monitor actions designed to achieve the goal of reducing preventable accidents. The DSOC is chaired by the Under Secretary of Defense for Personnel and Readiness (USD (P&R)). The ATP TF is one of nine DSOC task forces (see Figure 1) and is chaired by the Deputy Director, Human Capital and Specialty Engineering, Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering. The ATP TF promotes improving communication between the systems engineering and system safety communities. It is responsible for reviewing acquisition policies and processes and for studying issues concerning safety technology, such as how to insert safety technology into existing systems. The task force also includes two working groups: the Aviation Safety Working Group and the Tactical Vehicle Safety Working Group.

ATP TF responsibilities include the following:

- Ensure that acquisition policies and procedures address safety requirements
- Review and modify, as necessary, relevant DoD standards with respect to safety
- Recommend ways to ensure acquisition program office decisions consider system hazards
- Recommend ways to ensure milestone decision reviews and interim progress reviews address safety

The ATP TF divides its initiatives into six focus areas as shown in Figure 2.

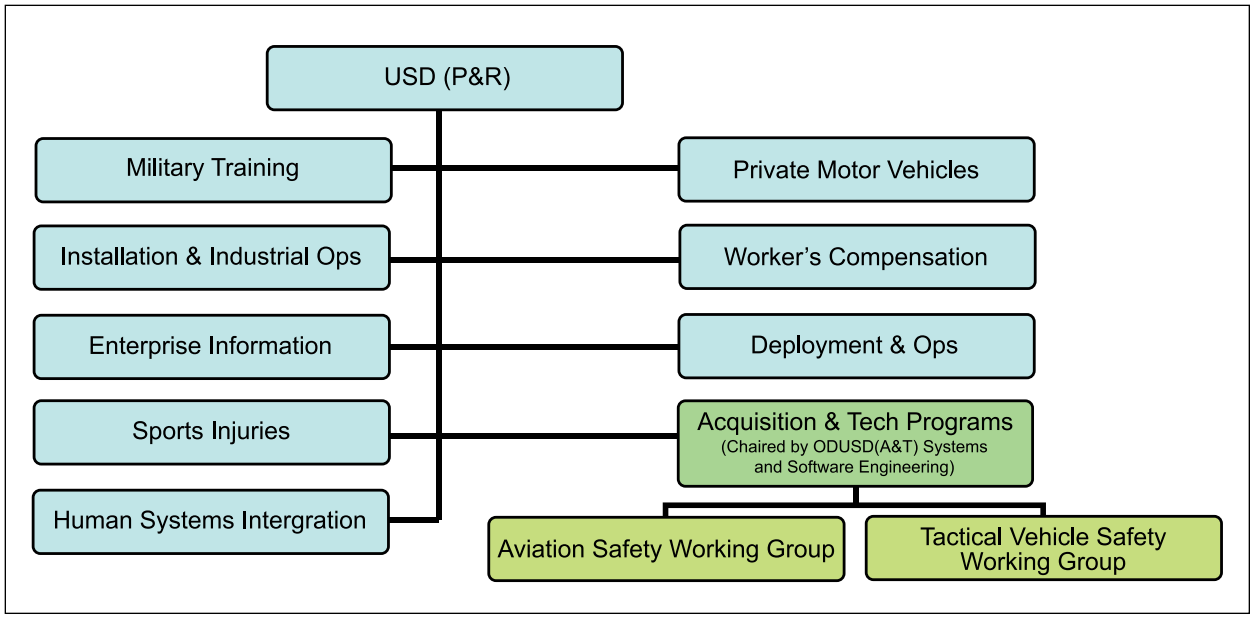


Figure 1. ATP TF Within the DSOC Organization

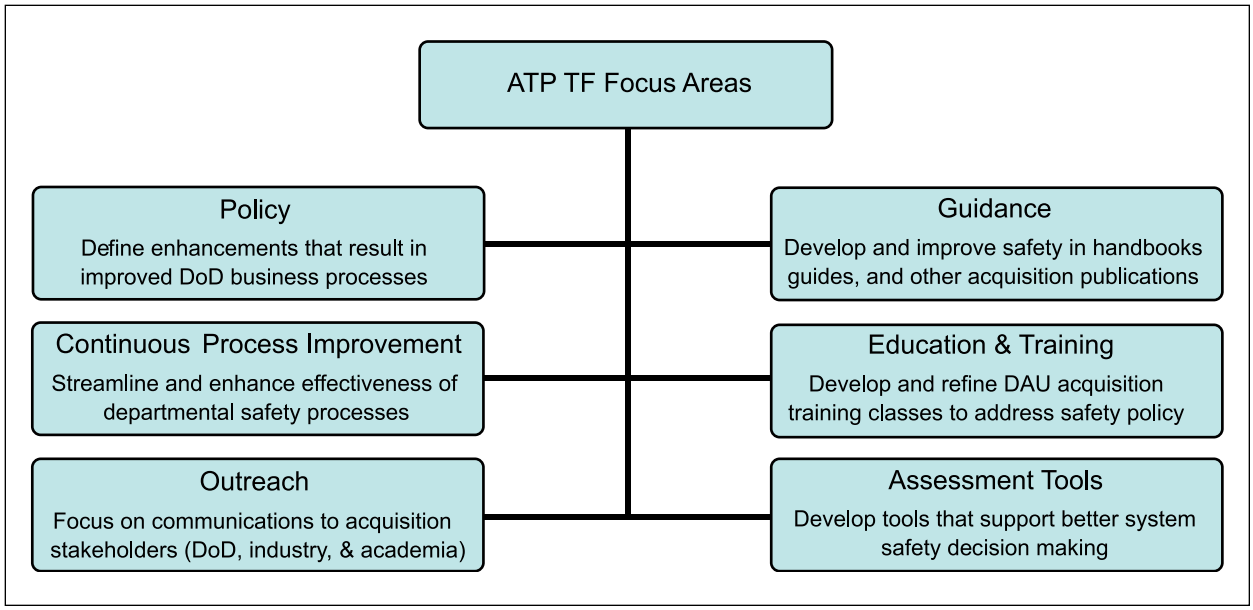


Figure 2. ATP TF Focus Areas

DoD Policy and Guidance

The ATP TF focuses on safety policy, guidance, and procedures throughout the acquisition life cycle. One of the ATP TF's major accomplishments has been to incorporate safety into the Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*, dated 8 December 2008. As the foundation for processes for all DoD acquisition programs, the instruction has a huge impact on how programs operate. The ATP TF drafted language to add an emphasis on safety. For example, the language calls for briefing ***high*** and ***serious*** risks using the MIL-STD-882D, *Standard Practice for System Safety*, methodology at appropriate acquisition program reviews and fielding decisions. It also requires user representatives to be a part of the risk acceptance process throughout the life cycle and to provide formal concurrence for all ***serious*** and ***high*** risk acceptance decisions.

ATP TF also contributed language to DoDI 5000.02 to address mishap reporting. The language calls for program managers to support system-related Class A and Class B mishap investigations by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk-mitigation measures, especially those corrective actions that minimize human errors.

Figure 3 depicts several other ESOH-related initiatives the ATP TF has completed and is undertaking in relation to the DoDI 5000.02 and SECNAV 5000.2D acquisition life cycle.

Joint Safety Certification

The ATP TF has completed several guides, including the *Joint Services Weapons/Laser Systems Safety Review (JSWLSSR) Guide to Support the U.S. Special Operations Command (USSOCOM)*. USSOCOM approached the ATP TF with concerns

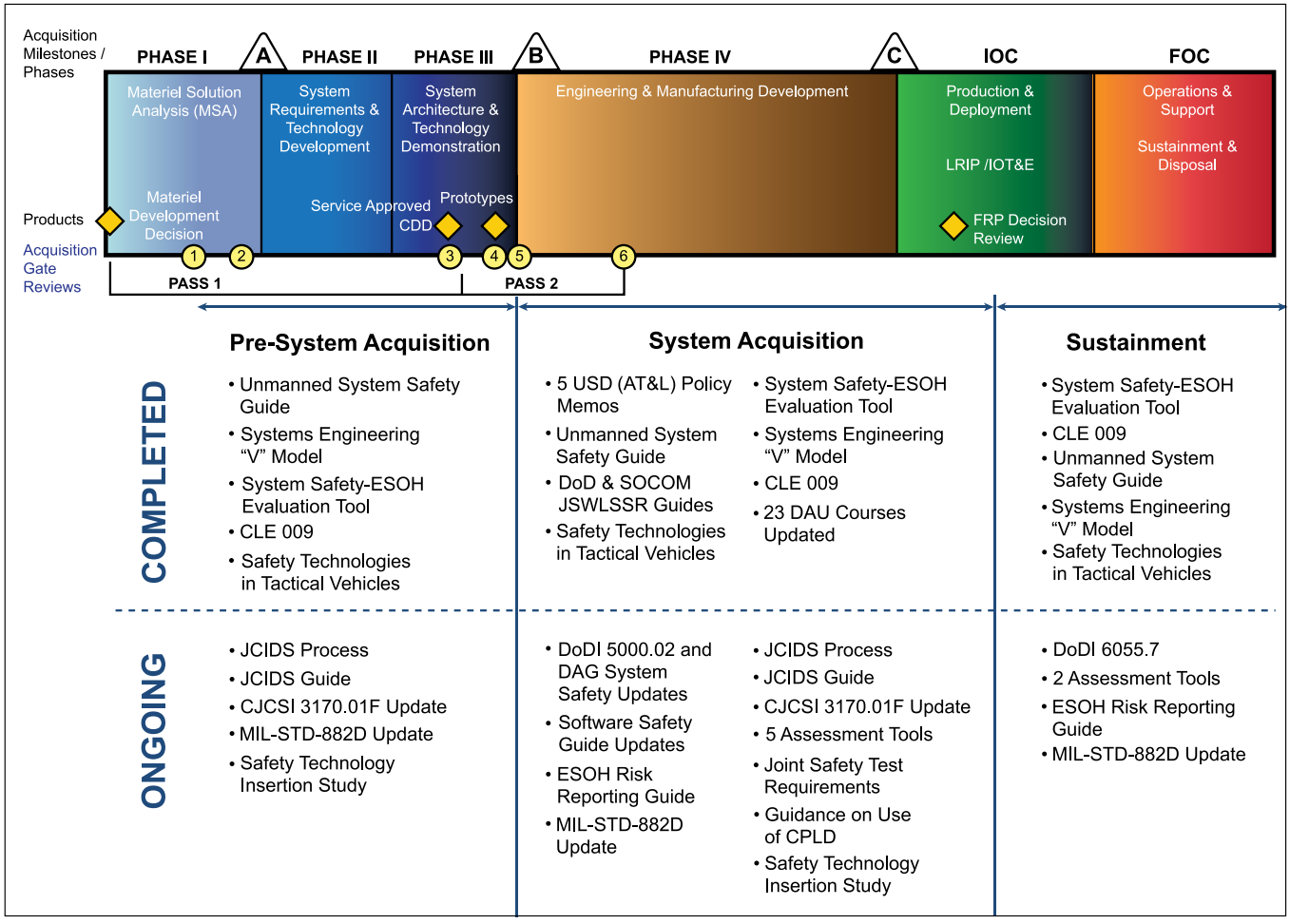


Figure 3. ATP TF Accomplishments and Initiatives by Life-Cycle Phase

that, because of a lack of existing policy, joint programs were required to complete multiple safety certifications through the different services. The process was repetitive and delayed the progress of fielding weapons.

In collaboration with weapon safety representatives from USSOCOM, the Army, Navy, Marine Corps, Air Force, and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the ATP TF drafted new guidance that streamlines the safety certification process. This collaborative review process accelerates the fielding of weapon systems to the USSOCOM warfighter without compromising safety. The response has been positive, and stakeholders have suggested that all joint weapon programs—not just USSOCOM programs—should have a similar process outlined in a DoDI. The ATP TF is currently drafting the Office of the Secretary of Defense (OSD) Joint Weapon and Laser System Safety Review Guide and a proposed DoDI, and is coordinating both documents with the services.

Safety Practices in Defense Acquisition University (DAU) Courses

In the area of education, the ATP TF has championed incorporating best safety practices into DAU systems engineering courses and has created a DAU Continuous Learning Module on "System Safety in Systems Engineering" (CLE 009). DAU courses reach all members of the acquisition workforce and have the potential to make a significant impact on the way current and future leaders view safety in the acquisition process.

More than 4,000 students have taken CLE 009. In addition, the ATP TF has sponsored the revision of 23 DAU courses to incorporate a safety component. The ATP TF reviewed all appropriate courses in detail and revised them to include a safety element.

For example, the DAU course "Fundamentals of Systems Engineering" (SYS 101) was updated as part of the ATP TF initiative for FY 2008. DoDI 5000.02 mandates that safety be addressed throughout the acquisition process. The ATP TF team made conservative modifications to the overview section of the course to convey that the discipline of systems engineering plays a vital role in developing not only effective and supportable defense systems, but also safe weapon systems. Table 1 shows an example of a modified paragraph.

Periodically, ATP TF subject-matter experts in the appropriate acquisition and environment, safety, and occupational health (ESOH) disciplines will continue to review and make recommendations for revision to the DAU courseware. The systems engineering courses are the highest priority for incorporation of ESOH content because the DoD acquisition process requires that ESOH hazard identification and risk management be effectively integrated into the systems engineering process as a design consideration.

Safety Assessment Tools

Among its initiatives, the ATP TF has sponsored several research studies, resulting in assessment tools to assist programs in measuring the effectiveness of their designs and their safety programs. Examples include:

- Noise Exposure Assessment Tool (NEAT)
- Evaluation of handrail extension devices for shipboard inclined ladders
- Proactive application of ergonomics for cost-benefit analysis in design
- System Safety Metrics Method

Table 1. Sample DAU Course Modification

Old Wording – **DAU SYS 101 Overview**	New Wording – **DAU SYS 101 Overview**
The discipline of Systems Engineering plays a key role in helping to unify the technical vision of a product; to effectively manage all the diverse skills needed to develop modern defense systems; and to help ensure that effective, supportable systems get fielded.	The discipline of Systems Engineering plays a key role in helping to unify the technical vision of a product; to effectively manage all the diverse skills needed to develop modern defense systems; and to help ensure that effective, **safe**, and supportable systems are fielded.

- Collaborative project with the Government Services Agency (GSA) and the National Institute for Occupational Safety and Health (NIOSH) to have low-vibration power hand tools and antivibration gloves made available in the federal supply systems to prevent the occurrence of hand-arm vibration syndrome[a]

Noise Exposure Assessment Tool (NEAT)

The effects of noise exposure have often been given insufficient attention in the design phase because life-cycle costs and human effects lack the acute and immediately quantifiable impact of other categories of mishaps. The NEAT project used information and approaches from the Navy Undersea Medical Research Institute and the Center for Naval Analyses to develop a general tool for assessing the life-cycle cost of noise exposures with and without acoustic control measures. Prior research validated an existing relationship between noise exposures and hearing loss sustained in "industrial" workers (ANSI Standard S3.44-1996) when applied to a Navy population with more prolonged exposures.

Using the research, the project developed a well-documented tool for broader application to a range of systems and equipment. The tool allows for projection of the cost of noise exposures from a defense system (ship, aircraft, vehicle, or facility) and provides estimated costs of compensation and related medical effects with and without given levels of exposure controls. This information provides a means to provide cost-benefit analysis for implementation of noise controls (or their relative absence) in design. An ancillary part of the tool identifies the level of managerial responsibility required to accept the level of risk described in accordance with defense acquisition regulations (DoDI 5000.02 application of MIL-STD-882D) and speech/communication impairment associated with noise levels.

Handrail Extension Devices for Shipboard Inclined Ladders

With ATP TF sponsorship, the Naval Surface Warfare Center, Carderock Division (Philadelphia Detachment), is spearheading a project to reduce injuries associated with shipboard inclined ladders. The project was initiated when a Naval Safety Center analysis showed that approximately 50 percent of shipboard falls were linked to descending inclined ladders.

Design factors were evaluated as consistent with the ladder angle (not readily subject to retrofit) and limitations of the handrails. In locations where the hatch must be able to close, prohibiting use of a typical handrail, current designs use a chain and stanchion to provide a handrail that is somewhat less stable than a fixed one and subject to being improperly rigged. Researchers are evaluating an extendable handrail as an alternative (see Figure 4). The design might be compared to a trombone slide; the handrail extends and can be locked in place temporarily, then retracted to allow the hatch to close. If prototype deployment on a carrier is successful, PMS 278 (in-service aircraft carriers program) anticipates using the design for retrofit of certain shipboard ladders.

Ergonomics

Ergonomic interventions have frequently improved the safety and efficiency of existing operations and have yielded excellent return on investment of technology; however, it has been difficult to estimate the economic and human impact of ergonomics and human systems integration approaches upon new systems and equipment. How do you quantify savings from a mishap that did not occur? Furthermore, how does a design engineer with limited ergonomics or safety background know which risk factors may be present and how to evaluate their relative hazards?

An ATP TF-sponsored project described methods for identifying ergonomic risk factors in design, provided an illustrated guide describing common process stressors/risk factors, and developed a detailed guide showing risk factors at each stage of the system life cycle for common defense systems. The associated manual and report demonstrate approaches to the evaluation of prospective risk via the presence of known ergonomic risk factors. Readily understood examples are used to demonstrate the risk reduction and manpower savings associated with alternative design approaches. These examples can be used to justify early investment in products, such as materials handling equipment, on the basis of long-term manpower savings (a critical performance parameter for major acquisition programs) and reduced risk to operators and maintainers.

Hand-Arm Vibration Syndrome

Hand-arm vibration syndrome is an irreversible syndrome affecting the nerves and muscles in the fingers and hands of persons with intense and prolonged vibration exposures from using a range of vibrating power hand tools. It has been reported since the early 1900s. Many types of shipyard work and numerous other DoD maintenance operations may create exposures potentially linked

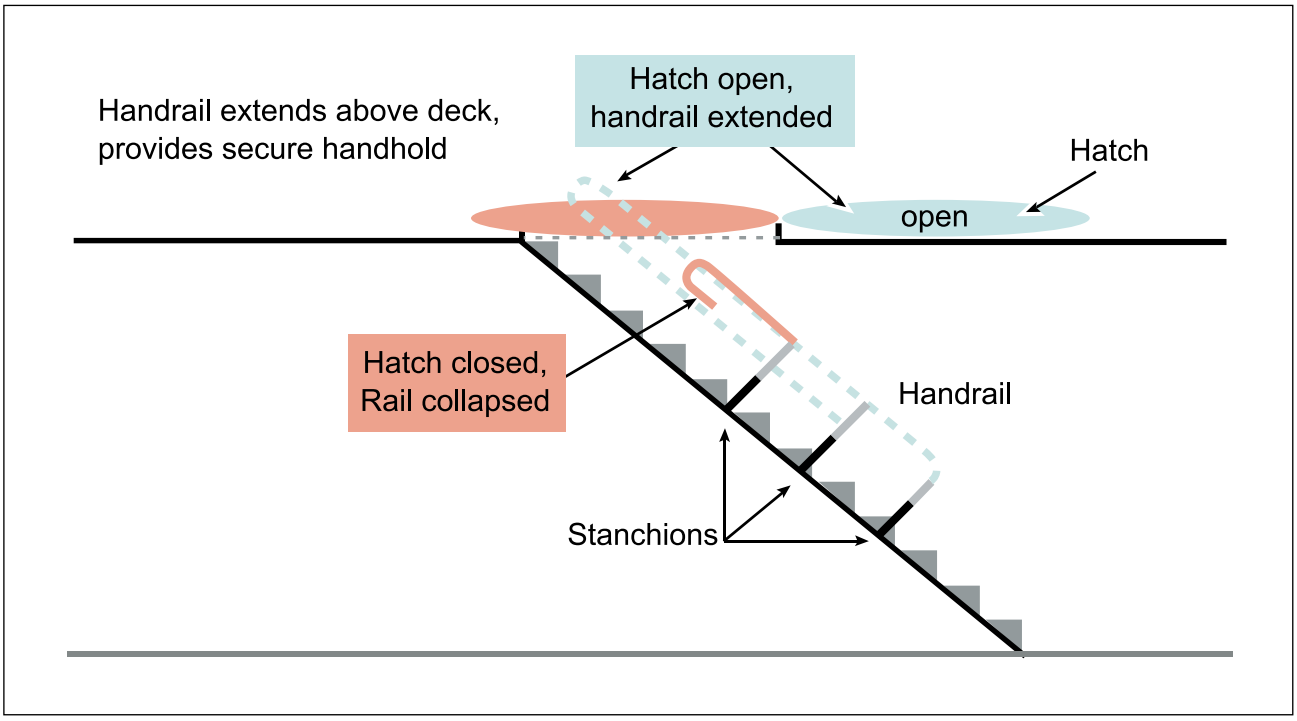


Figure 4. Handrail Extension for Shipboard Ladder

to development of this syndrome. The key to eliminating this preventable disease is through a combination of reduced exposure and improved tools, effective protective equipment, work practice, and education.

An ATP TF project, initiated on the basis of work initially performed at the Puget Sound Naval Shipyard, Washington, has engaged the NIOSH, the GSA office managing procurement of power hand tools, and safety and health representatives from all the services. The working group has developed procurement criteria for power hand tools (considering noise and vibration) and antivibration gloves, and guidance for third-party product evaluation. GSA has introduced several new tools on a trial basis, and groups such as GSA, NIOSH, and the DoD Ergonomics Working Group have developed a long-term cooperative arrangement.

System Safety Metrics Method

The System Safety Metrics Method—released in 2009 and now available for programs—serves as an inexpensive, useful tool to gauge the health of a safety program at any stage of the life cycle. Experience has proven that a strong safety program results in significant savings to the program, reduced need for late application of corrective retrofits, and often more effective systems at lower overall cost. The ATP TF is interested in receiving feedback on the method, which may be downloaded from the ATP TF Web site.

Emphasizing Safety Early in the Life Cycle

As depicted by the blue line in Figure 5, the ATP TF is continuing to focus its initiatives on improving safety in the early stages of the acquisition cycle, because the cost of making a change to a system later in the development cycle is normally prohibitive.

The red line in Figure 5 shows, notionally, how costs increase if a change is made later in the development cycle. The green line in Figure 5 depicts how system safety has traditionally been involved in the acquisition processes; that is, in a more serial manner after the systems and design engineers have developed conceptual designs and then turned those designs over to the system safety engineers for their review and analysis. This "serial design then safety review" approach does not involve the system safety engineers early enough in the concept design process to eliminate potential hazards. Consequently, the ATP TF's focus is to establish DoD safety policy that requires safety to be addressed increasingly earlier in the acquisition cycle.

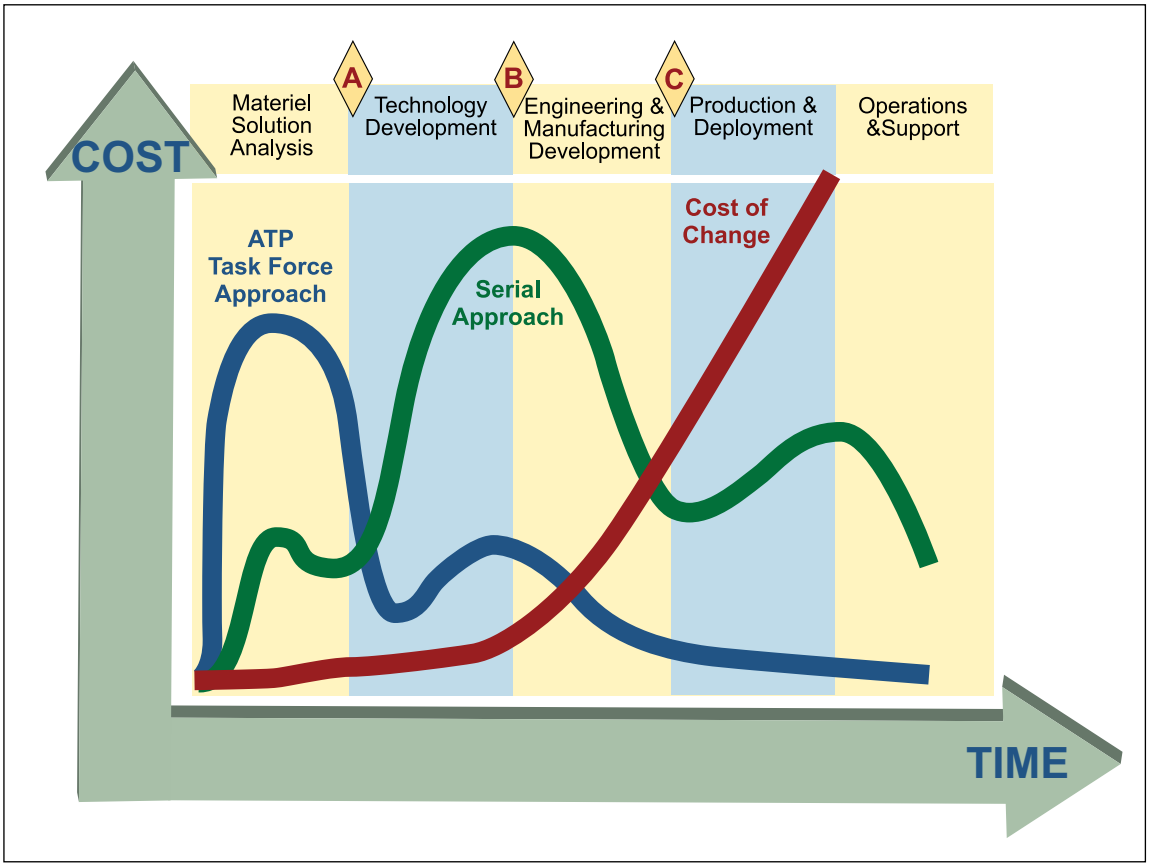


Figure 5. ATP TF Early Emphasis on Safety

For example, one initiative focuses on involving system safety and ESOH professionals routinely in the drafting and review of Joint Capabilities and Integration and Development System (JCIDS) documents, including Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents. ESOH subject-matter experts may be able to provide information to the JCIDS that has the potential to reduce mishaps. This initiative and associated guidebook will support the DoD's goal of reducing risk earlier in the life cycle.

Through coordinated efforts, the ATP TF has accomplished several policy and guidance improvements and continues to pursue new safety initiatives. The ATP TF seeks to incorporate safety considerations early in the life cycle to have the greatest positive impact on programs. To that end, the task force seeks feedback from the services to ensure that it is implementing policy and process changes that have a positive impact on the safety of systems provided to the warfighter, and that we are not overlooking other safety needs that may be visible only to those in the field. Readers are invited to consult the Web site and send feedback on issues that stakeholders believe the task force should address.

Endnote

a. Hand-arm vibration syndrome is an irreversible neurovascular disease affecting the fingers, hands, and potentially, upper arms. It is associated with excessive intense and prolonged exposure to hand-arm vibration, typically from power hand tools. The syndrome is underdiagnosed but has been documented in the United States since the early 1900s. Many operations vital to maintenance of defense systems and facilities have the potential to create significant hand-arm vibration exposures. Further

background information may be found at the Naval Safety Center's Web site, http://www.safetycenter.navy.mil/acquisition/vibration/index.asp

Bibliography

Acquisition and Technology Programs Task Force (ATP TF) Web site, http://www.acq.osd.mil/atptf/

Gates, Robert M., "Zero Preventable Accidents," Secretary of Defense memorandum, 30 May 2007.

Geiger, Mark, "Development of Common Design and Evaluation Guidelines for Access Aids (Ladders) for Military Vehicles and Shipboard Inclined Ladders," Brief, ATP TF, June 2007.

MIL-STD-882D, *Standard Practice for System Safety*, February 2000.

Naval Safety Center, *Acquisition Safety Human Factors Engineering (HFE) and Ergonomics*, http://www.safetycenter.navy.mil/acquisition/ergonomics/default.htm *Note:* The ongoing engagement of product and process owners is being elicited to continue and expand this project.

http://www.safetycenter.navy.mil/acquisition/ergonomics/downloads/DSOC_Ergo_Project_report_2106-08-3.doc

Naval Safety Center, *Introduction to Acquisition Safety*, http://www.safetycenter.navy.mil/acquisition/index.asp

Naval Safety Center, *Noise Evaluation Acquisition Tool (NEAT),* Briefing, 6 November 2008, http://www.safetycenter.navy.mil/acquisition/index.asp

Naval Safety Center, *Noise Exposure and Acquisition Tool (NEAT) Model User's Guide,* 14 November 2008, http://www.safetycenter.navy.mil/acquisition/index.asp

Naval Safety Center, "Worksheet for Inputting the Sound Level Data for Constant Source Exposure," *Noise Evaluation Acquisition Tool*, http://www.safetycenter.navy.mil/acquisition/noise/downloads/Noise_Eval_Acquisition_Tool.xls

Rumsfeld, Donald. "Reducing Preventable Accidents," Secretary of Defense memorandum, 22 June 2006. http://vppcx.org/Memo_Reducing%20Preventable%20Accidents.pdf

Rumsfeld, Donald, "Reducing Preventable Accidents," Secretary of Defense memorandum, 19 May 2003. http://www.dodig.mil/Inspections/IE/sdp_timeline/SecDef%20Memo,%20May%2019,%202003.pdf

System Safety Metrics Method, ATP TF, 2009, http://www.acq.osd.mil/atptf/guidance/System-Safety-Metrics-Method.pdf

Young, John J. "Reducing Preventable Accidents," Under Secretary of Defense for Acquisition, Technology, and Logistics memorandum, 21 November 2006.