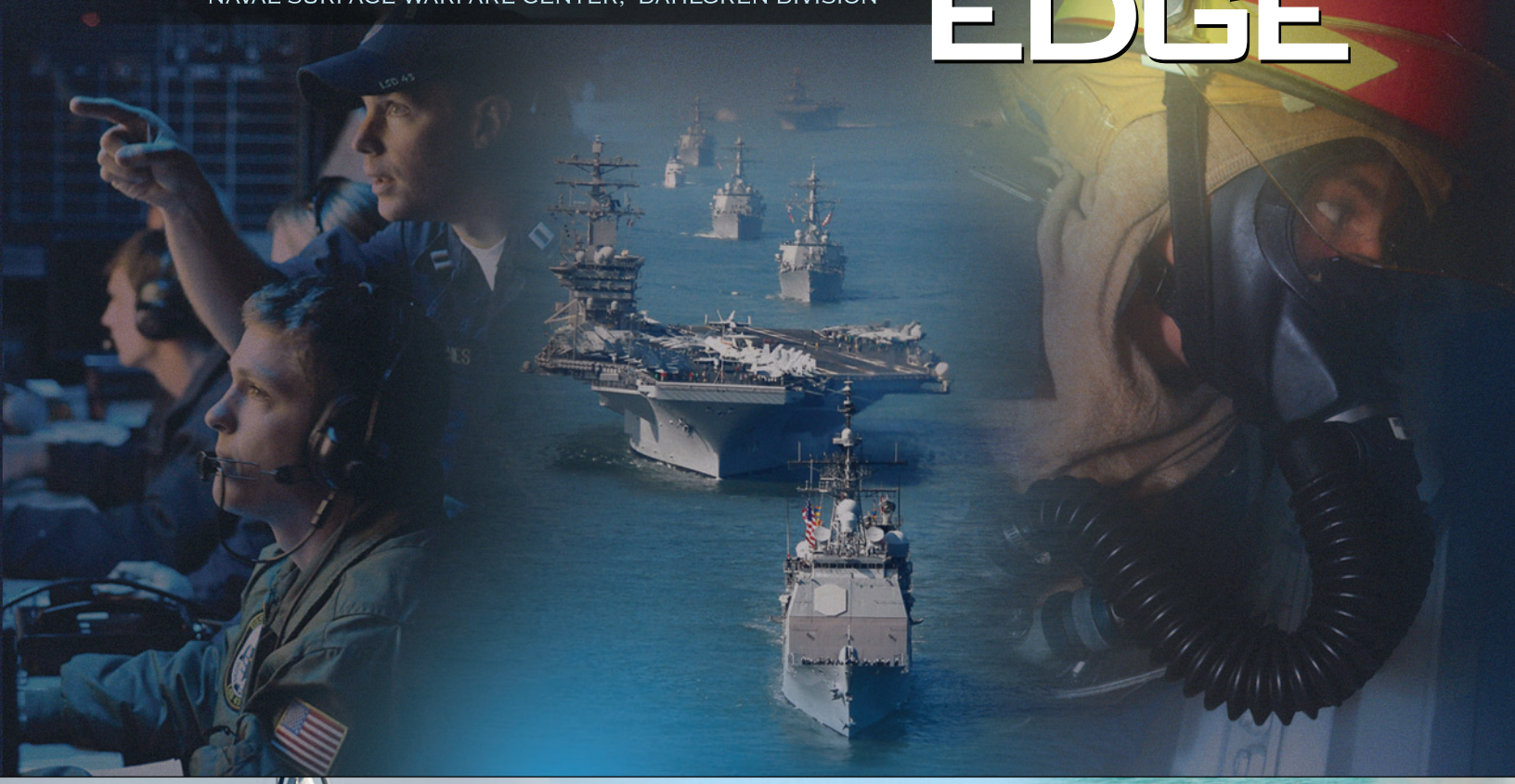
LEADING EDGE

NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION

Volume 7, Issue No. 3



Systems Safety

ENGINEERING

"Safety is a primary measure of the effectiveness of an organization, and it directly impacts readiness. Our culture must never accept accidental death, injury, or occupational illness as a cost of doing business."

SECNAV

NAVSEA
WARFARE CENTERS

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Leading Edge. Systems Safety Engineering. Volume 7, Issue No. 3	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Surface Warfare Center,,Dahlgren Division,6149 Welsh Road, Suite 239,Dahlgren,VA,22448-5130**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

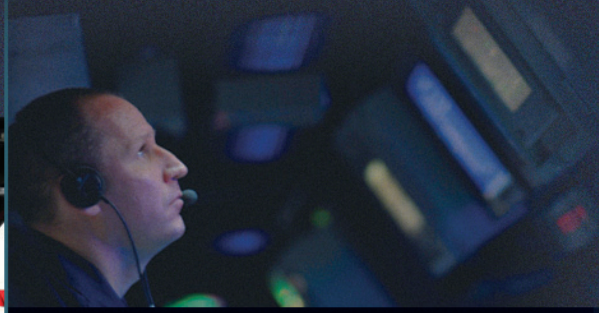
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**134**	

LEADING EDGE
Volume 7, Issue No. 3



Systems Safety Engineering

System safety is the process of "designing in" safety by "designing out" hazards or intentionally reducing the probability and severity of hazards.

Laura M. DeSimone
Executive Director,
Naval Ordnance Safety
and Security Activity

Deputy for Weapons Safety,
Naval Sea Systems Command

LEADING EDGE

Volume 7, Issue No. 3

Table of Contents

Systems Safety Engineering

5 Introduction: Deputy Secretary of the Navy (Safety) Statement
Tom Rollow

6 Introduction: Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Perspective on Systems Safety Engineering
Captain Sheila A. Patterson

7 Introduction: Naval Ordnance Safety and Security Activity (NOSSA) Perspective on Systems Safety Engineering
Laura M. DeSimone

8 Introduction: Engagement Systems Department Perspective on Systems Safety Engineering
Thomas C. (Craig) Smith

9 Introduction: Systems Safety Engineering Division Perspective on Systems Safety Engineering
Melissa A. Lederer

Defining System Safety

10 System Safety: What, Why, and How We Got There
Clifton A. Ericson II

18 Determining the Differences Between Safety and Operational Concerns
Jason Taubel, Shawn T. Thumm, and Steven Gainer

22 The Role of Environment, Safety, and Occupational Health (ESOH) in the System Safety Process
Jessica Delgado and James Engbert

30 The Case for Providing Actionable Safety Hazard, Near Miss, and Mishap Information to the Acquisition Community
James H. Yee, Billie Jo Hynson, and Nga Pham

36 DoD Acquisition and Technology Programs Task Force: Promoting System Safety Throughout the Life Cycle
Elizabeth Rodriguez-Johnson and Mark Geiger

The Players

44 Department of Defense Safety Program Guidance and Policies for the Principal for Safety (PFS)
Peggy L. Rogers

50 Training the Systems Safety Engineer
Mike Zemore and Etienne (Steve) Boscovitch

56 Establishing and Training Best Practices in Systems Safety Engineering
Robert C. Heflin Jr.

60 Navy Safety Review Boards: WSESRB, SSSTRP, and FISTRP
Mary Ellen Caro, David Shampine, and Jack Waller

62 The Navy's Weapon System Explosives Safety Review Board (WSESRB)
Mary Ellen Caro

66 The Navy's Software System Safety Technical Review Panel (SSSTRP)
David Shampine

68 U.S. Navy Fuze and Initiation System Technical Review Panel (FISTRP): Duties, Responsibilities, and Processes
Jack Waller

Table of Contents
(Continued)

The Players (Continued)

72 Joint Service Weapon Safety Review Processes
Robert Gmitter

78 United States Special Operations Command System Safety
Cathi Crabtree

Types of System Safety Efforts

80 Explosive Ordnance Safety
Bill Hammer

86 The Execution and Evolution of Combat System Safety
Mike Zemore

92 Combat System Safety
Kevin Stottlar

100 Shipboard Combat System Training Restoration
Michael Zemore, Rachael Carroll, and Brian Schwark

104 Assessment for the Use of Motor Gasoline on Navy Combatant as an Example of Total Ship Safety
Eric Weissman, Jon Frederick, and Joe Janney

108 Implementation of Pointing and Firing Cutout Zones
David Morgan and Greg Sellers

116 System Safety for Rapid Integration Projects
Carolyn Blakelock

124 NSWCDD's Role as the Lead Navy Technical Laboratory (LNTL) for Laser Safety Within the Department of the Navy (DON)
Sheldon Zimmerman, Robert Aldrich, and Thomas Fraser

LEADING EDGE

Volume 7, Issue No. 3

The Leading Edge Magazine is an official, authorized publication of the Naval Warfare Center Enterprise. The purpose of the publication is to showcase technical excellence across the Warfare Center Enterprise, and promote a broader awareness of the breadth and depth of knowledge and support available to the Navy and DoD at NSWC/NUWC.

Address all correspondence to Corporate Communications, C6
Email: dlgr_nswc_c6@navy.mil; or write to
Commander
Naval Surface Warfare Center, Dahlgren Division
Corporate Communications, C6
6149 Welsh Road, Suite 239
Dahlgren, VA 22448-5130

NSWCDD/MP-09/33

Approved for public release; distribution is unlimited.

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
Tom Rollow

NAVAL SEA SYSTEMS COMMAND
Vice Admiral Kevin M. McCoy, *Commander*
Brian J. Persons, *Executive Director*

NAVSEA WARFARE CENTERS
Rear Admiral James J. Shannon, *Commander, NSWC*
Rear Admiral Thomas G. Wears, *Commander, NUWC*
Donald F. McCormack, *Technical Director, NUWC*
Stephen E. Mitchell, *Technical Director, NSWC*

NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION
Captain Sheila A. Patterson, *Commander*
Carl R. Siel, Jr., *Technical Director*
Russell Coons, *Corporate Communications Director*
Margie Stevens, *Coordinator*
Patrice Waits, *Editor & Layout*
Clement Bryant, *Layout Design & Graphic Artist*
Trey Hamlet, *Graphic Artist/3-D Modeling*

ENGAGEMENT SYSTEMS
Thomas C. (Craig) Smith, *G Department Head*
Melissa A. Lederer, *G70 Division Head*
Robert C. Heflin Jr., *Senior Safety Engineer*

NSWC DAHLGREN
Robert Aldrich
Rachael Carroll
James Engbert
Jon Frederick
Robert Gmitter
Joe Janney
Nga Pham
Kevin Stottlar
Shawn T. Thumm
James H. Yee
Sheldon Zimmerman
Carolyn Blakelock
Jessica Delgado
Thomas Fraser
Steven Gainer
Billie Jo Hynson
David Morgan
Greg Sellers
Jason Taubel
Eric Weissman
Michael Zemore

NSWC DAM NECK
Brian J. Schwark

NSWC CRANE
Cathi Crabtree

NAVAL ORDNANCE SAFETY AND SECURITY ACTIVITY
Mary Ellen Caro
P. L. Rogers
Laura M. DeSimone
David Shampine

NAWC CHINA LAKE
Jack Waller

DUSD ACQUISITION AND TECHNOLOGY
Elizabeth Rodriguez-Johnson

OPNAV NAVAL SAFETY CENTER
Mark Geiger

BOOZ ALLEN HAMILTON, INC.
Bill Hammer

EG&G TECHNICAL SERVICES, INC.
Clifton A. Ericson II

LEADING EDGE

COMBAT

ENGAGEMENT

PLATFORM

Systems Safety

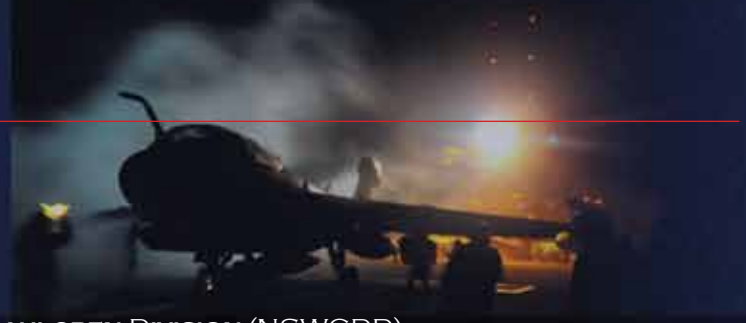
ENGINEERING

Introduction

Deputy Assistant Secretary of the Navy (Safety) Statement

Mr. Tom Rollow
Deputy Assistant Secretary of the Navy (Safety)

Our men and women in uniform are putting their lives on the line every day in defense of our freedoms and way of life. Hence, we all have an inescapable duty and responsibility to equip them with the absolutely best capabilities possible, with safety as a primary and enduring factor. System safety is not nice to have; it is an integral and essential part of the systems engineering process. To that end, the Department of the Navy (DON) is focused on integrating system safety into the overall acquisition, systems engineering, and management process—eliminating hazards where possible and making sure that serious and high risks are brought to the attention of the leadership that can provide resources or alter operations to prevent mishaps. DON manages mishap risk using MIL-STD-882D, *Standard Practice for System Safety*, to identify, analyze, and mitigate hazards, and reconcile residual risk. Our sustained involvement of system safety in acquisition programs is indispensable toward mitigating hazards, avoiding preventable mishaps, and providing sustained affordable readiness for the fleet. System safety is a key enabler in the acquisition and systems engineering process.



Introduction

Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Perspective on Systems Safety Engineering

Captain Sheila A. Patterson, USN
Commander, NSWCDD

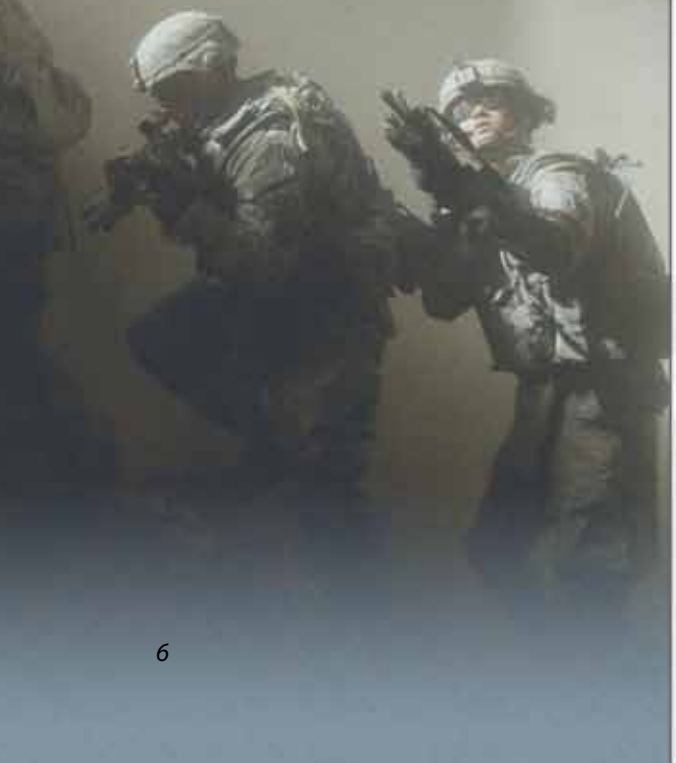
At the Naval Surface Warfare Center (NSWC) Dahlgren, we proudly boast that we have in some way touched every weapon system deployed by the U.S. Navy, as well as many deployed by the other services. One of the most important contributions we make is ensuring that these systems are safe in the hands of the warfighter. Over the years, we have tested and certified thousands of weapons and combat systems and fully comprehend the need to integrate safety in every phase of development from design to fielding.

Our systems safety engineers are second to none and have established processes that ensure that safety is an integral factor in the development of the system. Thanks to our outstanding leadership and the dedication of our systems engineers and support staff, we are now able to avoid mishaps and mitigate risks to the greatest extent possible.

In this edition of the *Leading Edge*, you will have an opportunity to see how safety standards and practices have evolved. You will get an inside view of the safety review boards, whose ultimate goal is to ensure that the weapons and weapon control systems that the Navy and Marine Corps field are safe for the users. You will also gain a better understanding of the board's role in evaluating weapon systems developed by other services and ensuring that they are also safe to carry and operate from Navy platforms.

As evidenced in many of the examples cited in this Systems Safety Engineering issue of the *Leading Edge*, incorporation of safety requirements and allocation of resources for safety analysis and testing early allows a program to plan and execute the weapon system safety program and uncover safety issues early, when they are less expensive, and solutions are easier to incorporate into the system design. Late identification of safety issues not only can have significant impact on cost and schedule, but more importantly, they can result in serious safety risks for individuals.

This Systems Safety Engineering issue of the *Leading Edge* demonstrates how seriously we take system safety at NSWC Dahlgren. Without exception, we are deeply committed to ensuring that the systems we provide are safe to use and perform consistently and accurately to keep our men and women in uniform out of harm's way. I am proud to stand at the helm of a Command where, through the innovation and tireless dedication of our safety engineering teams, we are making such a significant impact on today's warfare systems at sea and combat systems in theater.



Introduction

Naval Ordnance Safety and Security Activity (NOSSA) Perspective on Systems Safety Engineering

Laura M. DeSimone
Executive Director,
Naval Ordnance Safety and Security Activity

Deputy for Weapons Safety,
Naval Sea Systems Command

The ever-increasing complexity of today's weapon and combat systems present unique challenges to the system safety community. As weapon system complexity increases, so does the potential for a minor design flaw or human error to evolve into a mishap. The use of weapons, especially aboard ships, is inherently hazardous, and it is unlikely that all hazards can be prevented. However, the mishap risk associated with weapons and explosives can usually be mitigated to an acceptable level. It is therefore imperative that weapon systems be systematically analyzed, using the most advanced techniques appropriate, in order to reduce the mishap risk associated with hazards. System safety is the process of "designing in" safety by "designing out" hazards or intentionally reducing the probability and severity of hazards.

The Weapon System Explosives Safety Review Board (WSESRB) was established in 1967 following two destructive and deadly explosives mishaps aboard U.S. Navy aircraft carriers USS *Oriskany* and USS *Forrestal*. The WSESRB is chartered by the Chief of Naval Operations to provide independent oversight of the Department of the Navy weapon programs' safety efforts. From the very onset of the WSESRB, it has been accepted that explosives safety oversight is best accomplished by ensuring maximum compliance with longstanding safety requirements through the life-cycle development of each weapon system.

WSESRB reviews provide program managers an objective, independent assessment of their safety program. The system safety program ensures identification of hazards to the fullest extent possible, and provides for the introduction of protective design measures to mitigate the hazards early in the system development process. The ultimate goal of a WSESRB review still stands as the Navy's focal point for the prevention of mishaps involving ammunition, explosives, and related systems, thereby eliminating deaths, injuries, lost workdays, and property and environmental damage. Mishap prevention costs are generally less than the mishap costs; therefore, a robust safety system program reduces the total expected system costs.

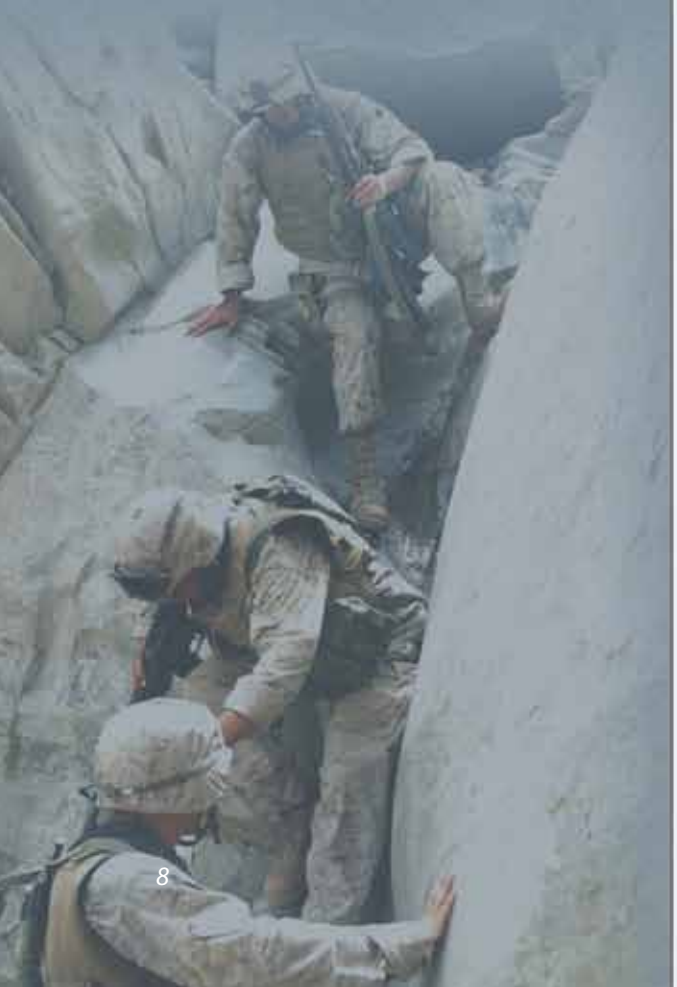
The Department of Defense has adopted system safety as a primary engineering discipline, within systems engineering, stressing preventive measures. The results of a thorough and rigorous system safety program are generally not visible, because the system safety program has been successful in preventing mishaps, and prevented mishaps are not a quantifiable metric. Through the collective efforts of our dedicated system safety professionals, the Navy and Marine Corps weapon and combat system developers deliver safe, effective, and affordable systems to our warfighters.

Introduction

Engagement Systems Department Perspective on Systems Safety Engineering

Thomas C. (Craig) Smith
NSWCDD
Head, Engagement Systems Department

In an era of increasingly irregular warfare and sophisticated enemy tactics, it is more important than ever that we maintain a technological edge in the engagement systems we provide to the warfighters who defend our nation's freedom. Integral to that premise is the precept that those engagement systems be designed to fulfill their mission as reliably and efficiently as possible. Concurrent with that premise is that our engagement systems are designed and fielded such that they maintain the highest degree of safety possible for the people who use them in the conduct of their duties. Meshing these two objectives sometimes presents a set of complex obstacles. It is often the paradox of modern weapon systems that safety and reliability are at odds. The highest degree of one may preclude the highest degree of the other. Therein lies the challenge of systems safety engineering, and we at the Naval Surface Warfare Center (NSWC) are meeting that challenge. Systems safety engineering is devoted to meeting the needs of our men and women in uniform by providing them with weapon systems that are safe to manufacture, store, transport, field, operate, and maintain, while simultaneously ensuring that they maintain high reliability in their functionality. From Marine Corps infantry weapons to major naval combat systems, systems safety engineering strives to ensure that those who volunteer to risk their lives in the face of enemy fire on behalf of this nation need not fear any consequence in the use of their own systems.



Introduction

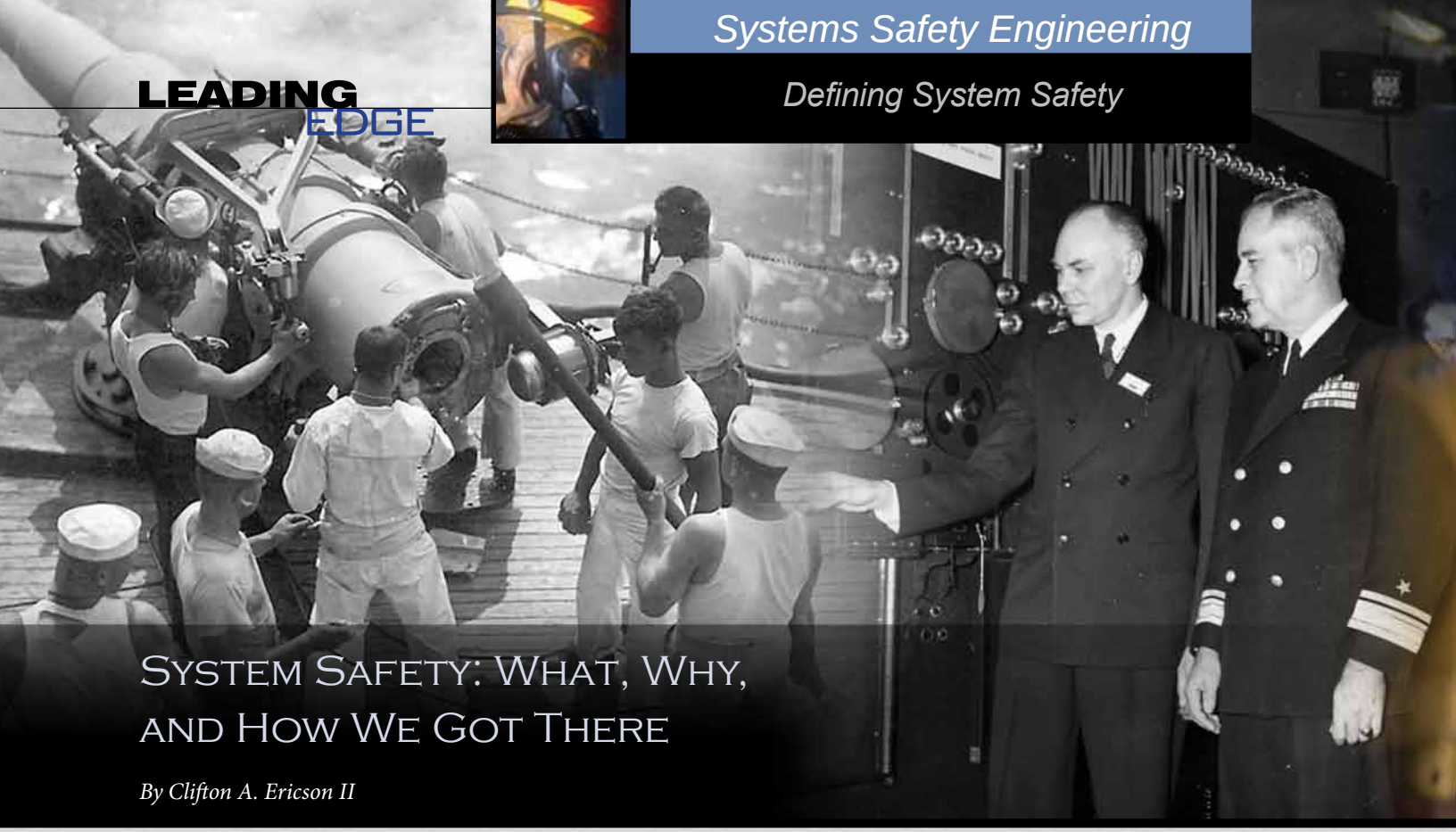
Systems Safety Engineering Division Perspective on Systems Safety Engineering

Melissa A. Lederer
NSWCDD
Head, Systems Safety Engineering Division

This issue of the *Leading Edge* showcases systems safety engineering. It introduces the history of the discipline, explains what system safety is, the roles of review boards, and how it is executed. While a significant chain of policy requirements does exist for performing system safety, the real justification for the exercise of safety analysis is that it simply makes sense. Ensuring that systems are safe helps to save lives, prevent the loss of costly military assets, and prevent damage to the environment. In this issue, you will learn about the numerous ways that system safety is supporting the warfighter.

The system safety practitioner is a unique individual. In addition to being system safety experts, they must be educated in a variety of scientific and engineering disciplines, as well as maintain a significant level of proficiency in program management. Their required level of overall knowledge about the system that they support is exceeded by very few. These professionals face tremendous challenges in their efforts to provide innovative, proactive, and reliable systems safety engineering services. Traditionally, and even more so in the current wartime environment, they are often faced with conflicting requirements, insufficient budgets, and the stress of compressed timelines. As you read the articles in this issue, I hope you will gain an understanding for the complexity of the discipline and an appreciation for the people who have dedicated their careers to ensuring that warfare systems have been subjected to a quality system safety analysis.

The bottom line is that keeping warfighters safe from injury, safeguarding the environment, and protecting equipment is what system safety is all about.



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.

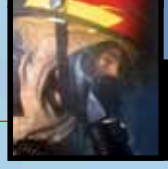
Although system safety is more than MIL-STD-882, the discipline tended to grow and improve with each improvement in MIL-STD-882. System safety is now a process that is formally recognized internationally and that is used to develop safe systems in many countries throughout the world.

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.

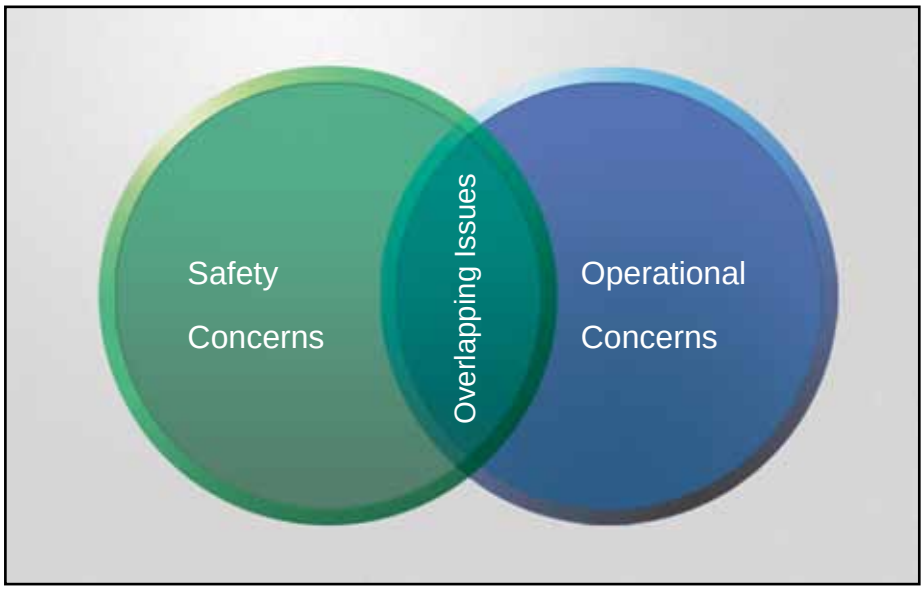


Figure 1. Overlap of Safety Concerns and Operational Concerns

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.

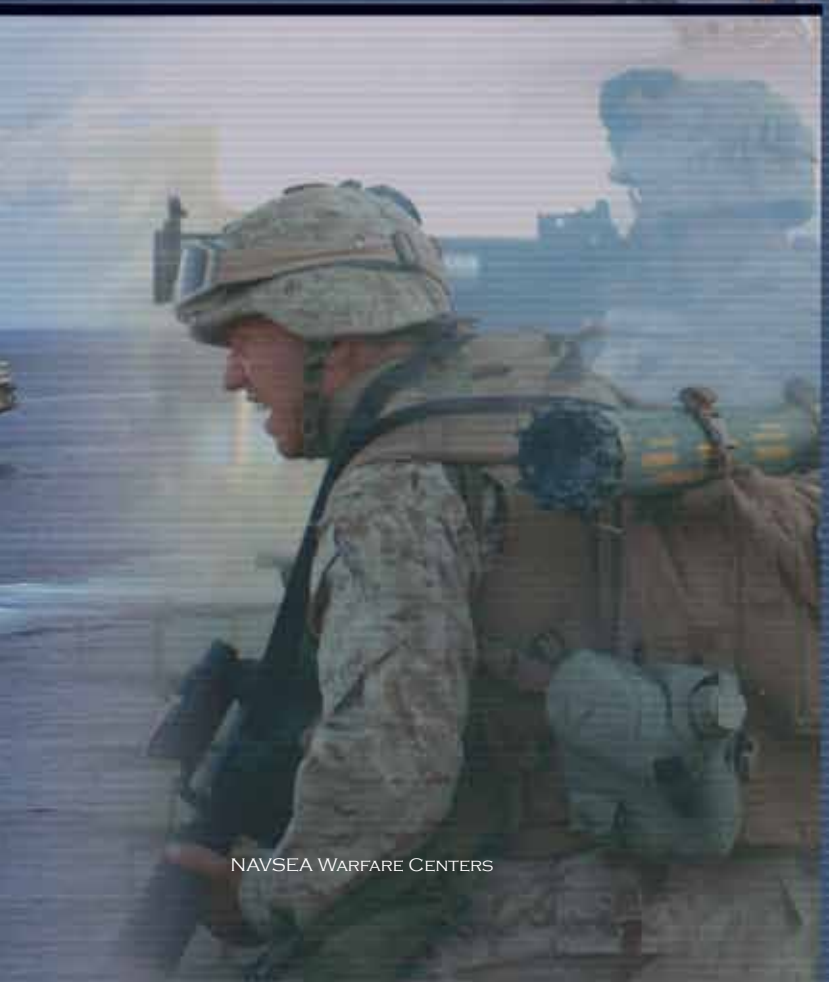
If the concern involves the misidentification of a target, caused by the target, resulting in the target being fired upon, it is *not* a safety concern. An example would be a civilian craft approaching a U.S. Navy ship in such a manner that it meets the entire criterion for the use of deadly force. If 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

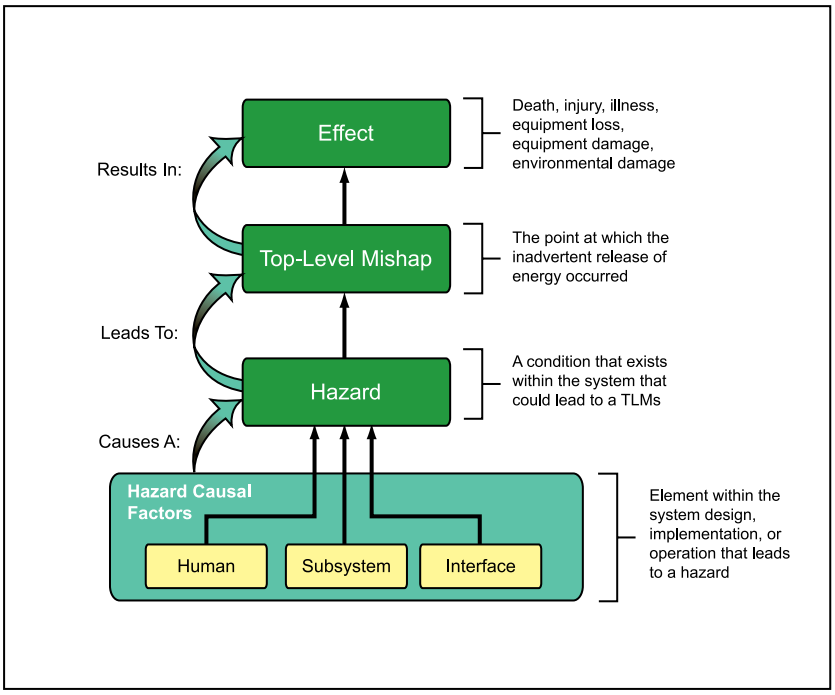


Figure 1. Hazard Relationships

- 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.

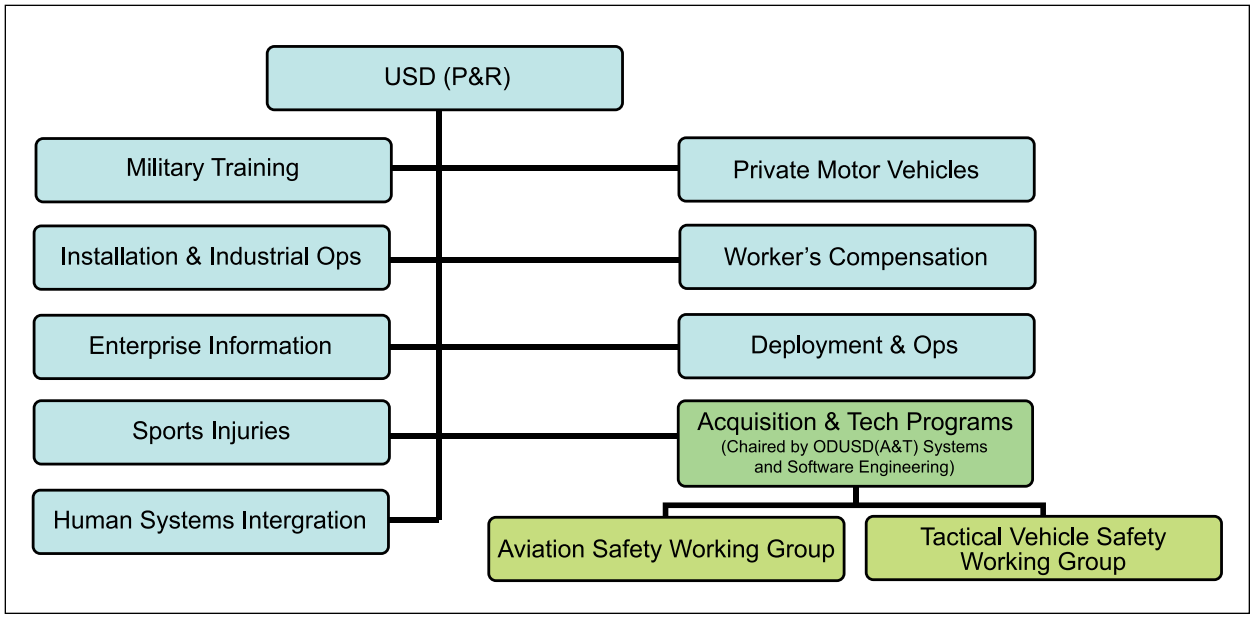


Figure 1. ATP TF Within the DSOC Organization

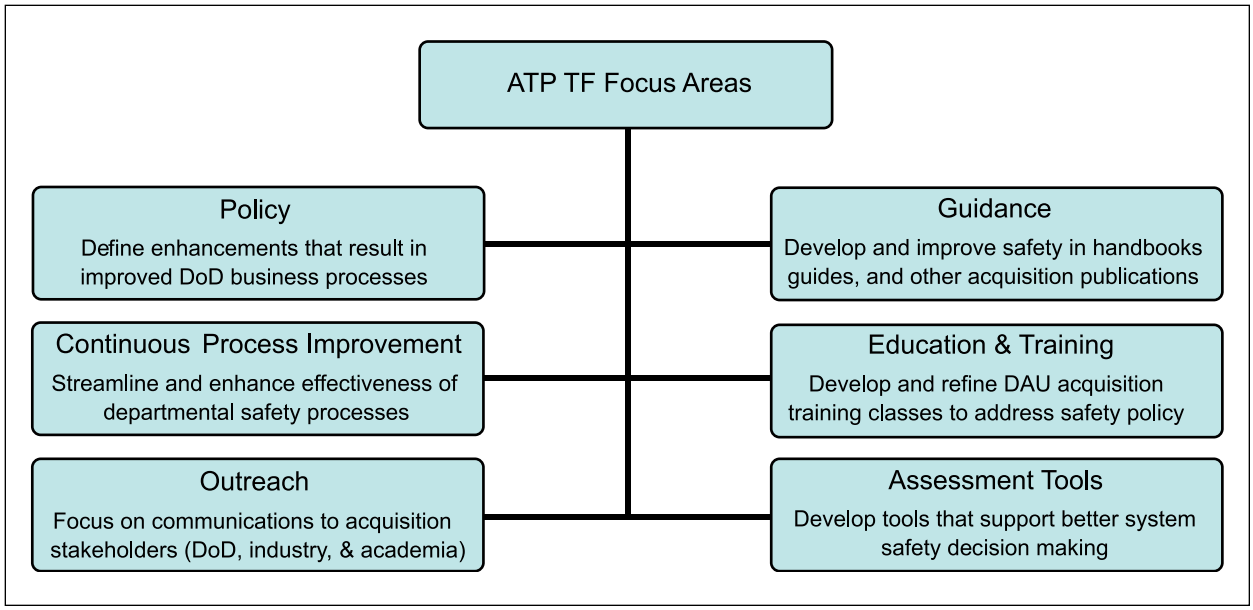


Figure 2. ATP TF Focus Areas

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

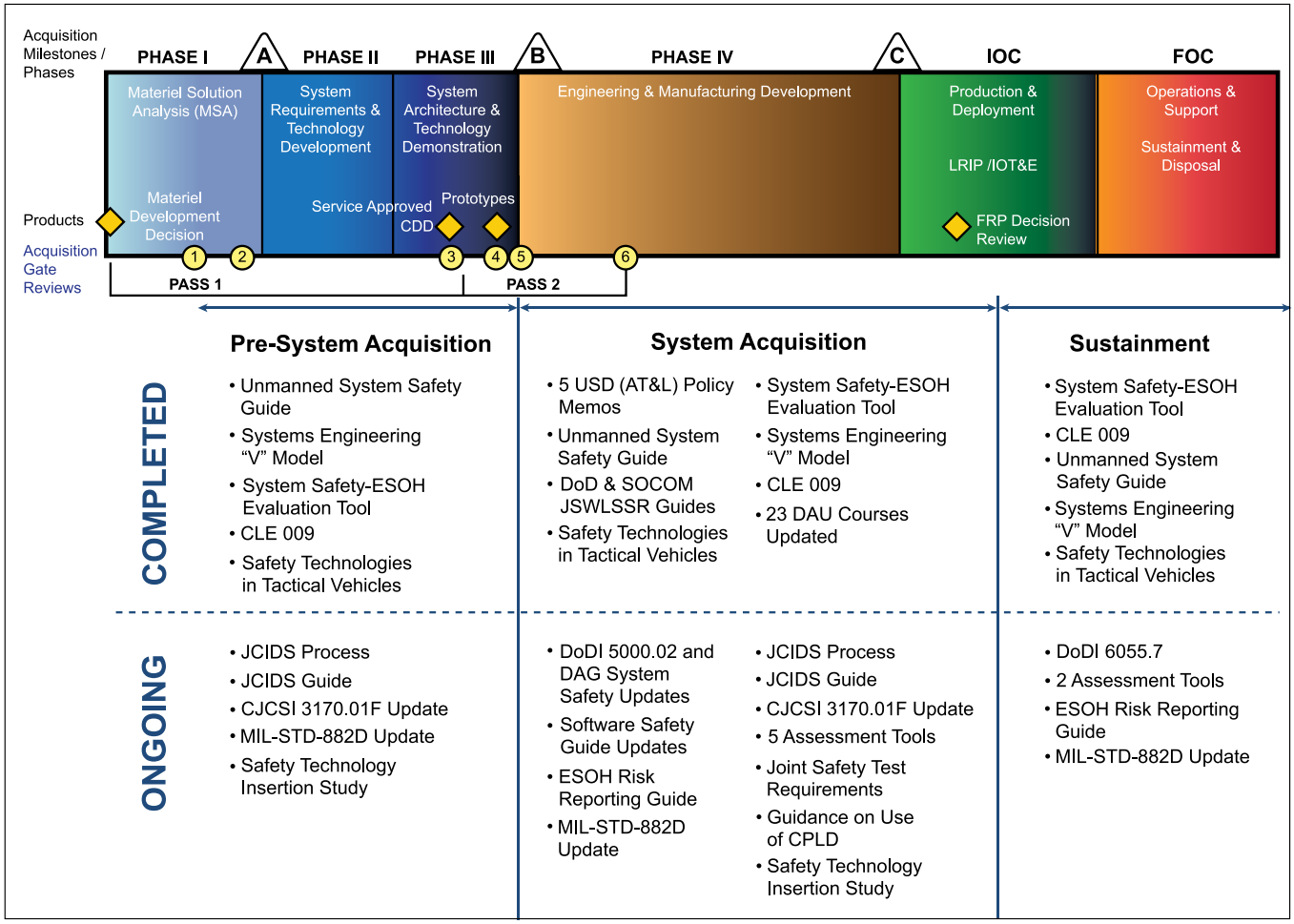


Figure 3. ATP TF Accomplishments and Initiatives by Life-Cycle Phase

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

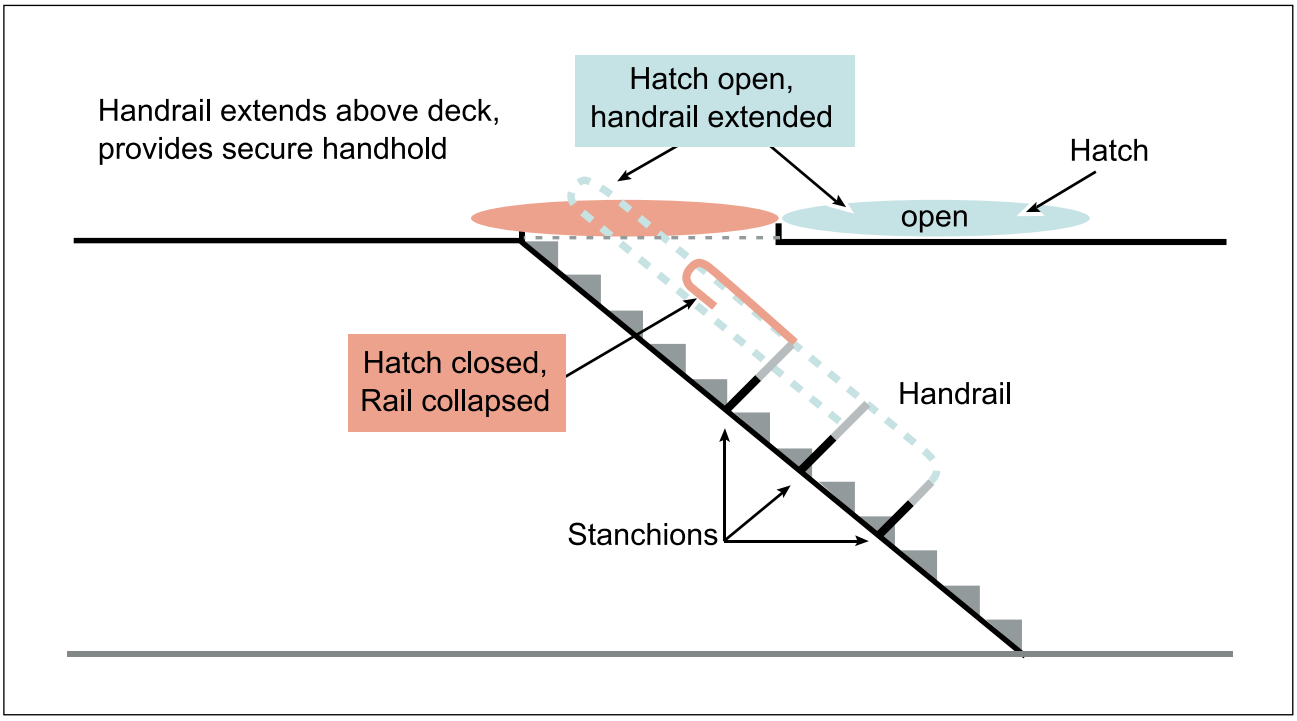


Figure 4. Handrail Extension for Shipboard Ladder

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.

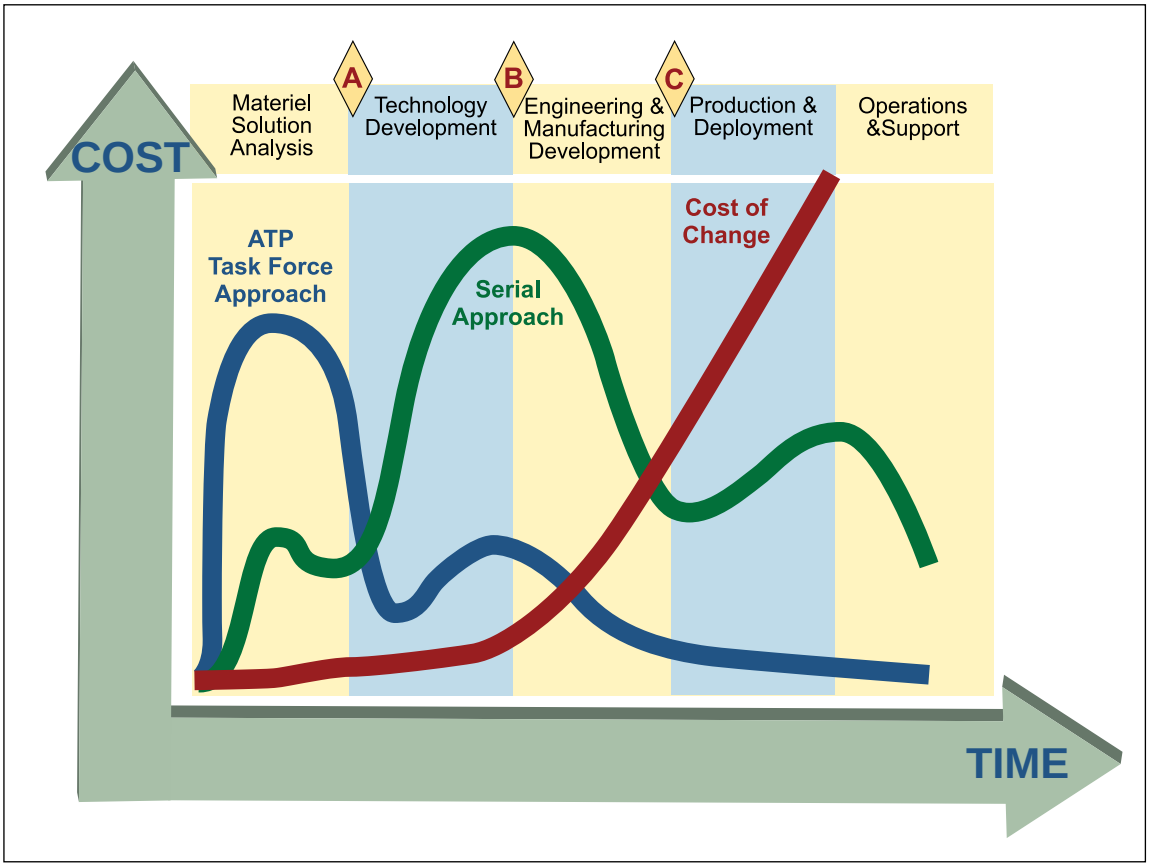


Figure 5. ATP TF Early Emphasis on Safety

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

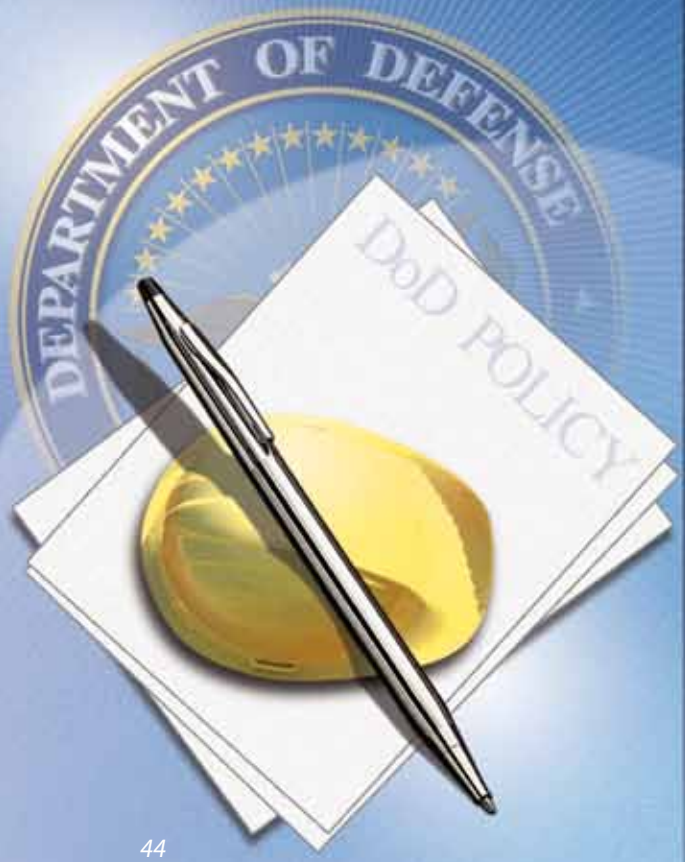
System Safety Metrics Method, ATP TF, 2009, http://www.acq.osd.mil/atptf/guidance/System-Safety-Metrics-Method.pdf

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

Department of Defense Safety Program Guidance and Policies for the Principal for Safety (PFS)

By Peggy L. Rogers

Author's Note:
This article is a condensed version of a much longer, more exhaustive paper developed on the subject. Please contact the author for a full version of the article.



Navy acquisition programs, particularly weapon system programs, identify a Principal for Safety (PFS) to act on behalf of the program manager (PM) to ensure that the systems being deployed into military service are safe. The role of the PFS is complex and diverse in the duties and responsibilities that are expected of these individuals. The myriad of standards, guidebooks and policies providing requirements for the safety program can be overwhelming. However, an understanding of these policies and standards is essential to the PFS in fulfilling their responsibilities. This article briefly explores those standards and offers a glimpse at the impact they have on the PFS in the conduct of the safety program.

Principal for Safety (PFS)

The PFS is the "eyes and ears" of the PM/managing authority (MA) in regards to all safety matters of a system. The PFS is employed to ensure that the best interests of the fleet with regard to safe development, operation, maintenance, and disposal of a system is taken into consideration when making acquisition decisions. He or she serves at the pleasure of the PM and should have a working relationship with the PM and any program office representatives designated. It is the job of the PFS to inform the PM of the safety risk associated with design decisions implemented or concepts planned for the systems under their purview. The PFS must be embedded in the design and development team(s), yet stay objective, keeping the best interests of the user in

mind. It is very easy as an embedded team member to lose objectivity when schedule (would using "budget" work) plays such an important role in the decision-making process. The PFS is required to have a wide range of knowledge regarding all aspects of the system. The PFS must be able to rely on the design and development team members, as well as subject matter experts (SMEs), to accomplish the mission of fielding as safe a system as possible within technological and programmatic constraints. Facilitating this interaction while maintaining independence and objectivity is the challenge faced by the PFS.

It's the Law

We all want what is best for our warfighters. We especially want to ensure that we provide our troops with the safest equipment and systems possible. This idea is important enough that the U.S. government, via the U.S. Congress, passed legislation to institutionalize the concept into law. The Department of Defense (DoD) is required, by law, to establish and maintain an explosives safety program. U.S. Code Title 10, Section 172 provides this mandate. It instructs the military to establish joint boards to oversee preventing hazardous conditions from arising that may endanger life and property. Since its enactment into law, the concept of a system safety program and the responsibilities therein have been further delineated by DoD and the Navy through a multitude of directives and instructions, each of which defines in some measure how the PFS performs the duties of the role.

Directives

Department of Defense Directive (DoDD) 5000.1

DoDD 5000.1, *The Defense Acquisition System*, of 12 May 2003, provides a specific section on safety. Enclosure 1.23,"Safety," states that:

> Safety shall be addressed throughout the acquisition process. Safety considerations include human (includes human/system interfaces), toxic/hazardous materials and substances, production/manufacturing, testing, facilities, logistical support, weapons, and munitions/explosives. All systems containing energetics shall comply with insensitive munitions criteria.

Whether the systems that we work on are weapons or explosives related, they are all required to address safety. As the point person for safety, the PFS is responsible for guiding the system safety program in the development and implementation of a System Safety Program Plan that will address all aspects of the system life cycle and, thereby, all aspects of the acquisition process.

Department of Defense Instruction (DoDI) 5000.02

DoDI 5000.02, *Operation of the Defense Acquisition System*, of 8 December 2008, was recently updated and has numerous references to safety.

The acceptance of risk by the appropriate authority is one section of this instruction. After all design and procedural mitigations have been identified, employed, and documented for the safety program, the residual safety risk in the system must be accepted by the appropriate authority. The PFS is responsible for ensuring that residual system safety risk has been identified and quantified in terms of hazards, which could potentially result in mishaps, and for further ensuring that the extent of that risk is clearly communicated to the level of authority charged with accepting the risk or with deciding that it is not acceptable.

Instructions

Secretary of the Navy Instruction (SECNAVINST) 5000.2C

SECNAVINST 5000.2C, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System*, dated 19 November 2004, provides direction for program acquisition and joint capabilities integration development strategies. There are many areas in this instruction that address safety.

For the PFS, the SECNAVINST 5000.2C requirements should be documented as part of a programs formal acquisition strategy. When a PFS joins a program, depending on the life cycle or development phase the program is in, the PFS should investigate what were the submission documentation for these strategies and review to ensure that the program is in compliance with the requirements of this instruction.

SECNAVINST 5100.10H

SECNAVINST 5100.10H, *Department of the Navy Policy for Safety, Mishap Prevention, Occupational Health, and Fire Protection Programs*, dated 15 June 1999, directs the Chief of Naval Operations/Commandant Marine Corps (CNO/CMC) to establish safety programs. The entire instruction should be read and understood by the PFS.

Office of the Chief of Naval Operations Instruction (OPNAVINST) 5100.19D

OPNAVINST 5100.19D, *Navy Occupational Safety and Health (NAVOSH) Program Manual for Forces Afloat*, dated 5 October 2000, documents the overall administrative, organizational, and training aspects of the NAVOSH program, including policy and responsibilities. The purpose is to provide commanding officers, safety officers, managers, supervisors, and workers for afloat commands with the guidance and direction necessary to implement the NAVOSH Program.

A PFS engaged in conducting safety analysis of a system designed for shipboard use may gain a wealth of knowledge regarding the safe conduct of afloat operations by reading and understanding this instruction. Of particular interest is Volume II, Section C, "Surface Ship Safety Standards." Insight into how business is conducted afloat is very beneficial to the PFS, especially for one who does not have direct military operational experience.

OPNAVINST 5100.24B

OPNAVINST 5100.24B, *Navy System Safety Program Policy*, dated 6 February 2007, is the policy that guides implementation of system safety in the Navy. It discusses the background, applicability, and Navy System Safety Policy specifically. It also clearly defines the responsibilities of the different entities involved in military operations. The instruction discusses implementation of safety programs and provides details to guide the reader.

This instruction will help the PFS understand the policy and direction on who has authority over, and responsibility for, the safety programs under their purview. It will help guide them in a general understanding of Navy system safety and the documented requirements for the programs.

OPNAVINST 8000.16C

OPNAVINST 8000.16C, *Naval Ordnance Maintenance Management Program (NOMMP)*, dated 1 September 2006, is issued to define responsibilities, policies, and procedures for conducting the Naval Ordnance Maintenance Management Program at all levels.

The PFS that assesses ordnance handling and topside design configurations will be most interested in this instruction. It offers details as to when and what type of ordnance program reviews and inspections are required, as well as the government organizations performing those reviews and inspections.

OPNAVINST 8020.14

OPNAVINST 8020.14/MCO P8020.11, *DON Explosives Safety Policy Manual*, dated 1 October 1999, gives the Weapon System Explosives Safety Review Board (WSESRB) the technical authority for matters concerning Department of the Navy (DON) explosives safety. Enclosure (1) is the Explosives Safety Policy Manual, which provides 18 chapters of explosives safety information, ranging from establishment of the Explosives Safety Program to Explosives Mishap Investigations and Reports.

This instruction provides important distinctions for programs with regard to when they will be reviewed by the WSESRB. This will drive the PFS tasking and safety schedule working lock step with the system developmental plans and schedules. The PFS must have a working knowledge of the overall development schedule to ensure that the safety program is being reviewed by the WSESRB at the appropriate milestones.

Naval Sea Systems Command (NAVSEA) OP 4

NAVSEA OP 4, *Ammunition and Explosives Safety Afloat*, dated 1 July 2006, is the mandatory instructions and regulations for safe ammunition handling and ordnance operations aboard ship. NAVSEA OP 4 provides technical direction and procedures, including ship design requirements and standards for the safe handling, stowage, and use of all ammunition and explosives afloat. It is applicable to all ships owned or operated by the Navy, and it is also applicable to other vessels—such as the Military Sealift Command (MSC)—which carry naval ammunition and explosives.

The PFS responsible for ordnance handling, stowage, and use must thoroughly study and know the information contained in OP 4 in order to effectively analyze risk associated with ordnance items.

Naval Sea Systems Command Instruction (NAVSEAINST) 5000.8

This instruction of 21 July 2008, *Naval SYSCOM Risk Management Policy*, defines the requirements for system safety, as well as programmatic risk for naval services, which includes:

- Naval Sea Systems Command
- Naval Air Systems Command
- Naval Supply Systems Command
- Naval Facilities Engineering Command and
- Marine Corps Systems Command

The instruction perpetuates policy and assigns responsibility across all Naval Systems Commands (SYSCOMs) and affiliated Program Executive Offices (PEOs) for a consistent methodology in managing risk. It discusses system safety risk and the management of the system safety process.

For the PFS, this instruction continues the advancement of the system-of-systems safety analysis concept for system safety assessments. Few present-day systems operate in a stand-alone environment with no integration with other systems. This facilitates identifying and communicating residual safety risk among SYSCOMs. It also helps the PFS communicate risk to other safety programs with which they interface.

NAVSEAINST 5100.12A

NAVSEAINST 5100.12A, *Requirements for Naval Sea Systems Command System Safety Program for Ships, Shipborne Systems and Equipment*, dated 11 December 1995, provides guidance to NAVSEA directorates, PEOs, PMs, and MAs on setting up and tailoring safety programs for ships, shipborne systems, and equipment. Section 7.d of this instruction provides the requirements and responsibilities for the Naval Ordnance Safety and Security Activity (NOSSA) (formerly known as the Naval Ordnance Center). One of those requirements specifically calls out the provision of the WSESRB chair.

Enclosure (1) of this instruction provides guidance to the PFS on tailoring system safety program requirements, but the PFS should be cautioned on the outdated concepts and requirements recommended. The PFS should read this document in its entirety. It is an easy read and helps distinguish, for the PFS, the responsibilities of managing activities.

NAVSEAINST 8020.6E

NAVSEAINST 8020.6E, *Department of the Navy Weapon System Explosives Safety Review Board*, of 11 March 2008 defines WSESRB processes and procedures for the conduct of weapons- and ordnance-related safety program reviews. Section 8.i gives clear guidance on the responsibilities and the expectations of the Program PFS.

NAVSEAINST 9410.2

NAVSEAINST 9410.2, *Naval Warfare Systems Certification Policy*, of 18 July 2005 is a naval joint SYSCOM instruction that defines platform certification criteria for ship platform and strike force combat systems in support of the Fleet Response Plan processes. It includes combat system safety and force level safety as a requirement in the review process.

The PFS that has the responsibility for combat systems, platforms, and strike force (force level) will be required to define risk for the decision makers certifying these platforms. Although steps have been made in the area of combat system safety risk definition, identification, and methodology, the area of force level and platform safety is new and emerging for the safety community.

Guidance and Policy

System Safety Program Requirements

MIL-STD-882C, *System Safety Program Requirements*, dated 19 January 1993, is the overarching document that guides government and contractor safety programs. It specifies the analytical tasks that should be performed when conducting a comprehensive safety program. MIL-STD-882C does a good job of guiding the safety team on what needs to be done, but the currently approved version, 882D, is lacking in the "how-to" area for generation of the safety analysis products.

The PFS needs to be familiar with both the D version and its predecessor, MIL-STD-882C. The C version of the document provides the PFS with some of the analytical detail lacking in D, while D offers stronger guidance in the hazard/mishap relationship.

Weapon System Safety Guidelines Handbook

NAVSEA SW020-AH-SAF-010, *Weapon System Safety Guidelines Handbook,* is a comprehensive handbook that provides more of the "how-to" with regards to safety analytical tasks, in contrast to the MIL-STD-882 guidance. This guidelines handbook provides DON best practice for the development of a System Safety Program in accordance with MIL-STD-882, and provides the management and technical principles of systems safety engineering. The context of the handbook provides a wealth of analytical techniques that the PFS and safety engineer can utilize and tailor according to the needs of their safety program.

WSESRB Interactive Safety Environment (WISE)

NOSSA has implemented an online interaction safety learning tool called WISE. This online curriculum has a wealth of system safety information and data. It represents a safety knowledge management tool for the execution of any system safety program for the DON. The tool allows the WSESRB to promote safety practices more effectively by widely communicating best practices, tacit knowledge, and supporting system safety certification requirements for U.S. Navy and Marine Corps PFSs. The completion of the WISE curriculum is planned as a minimum requirement for the certification of a PFS, pending release of NAVSEAINST 12410.5. The WISE online tool can be accessed at: https://nossa.nmci.navy.mil/wise/WISE_home.aspx

Software System Safety Handbook

The Joint Software System Safety Committee released the *Software System Safety Handbook* in December 1999. The generation of this handbook was a joint effort developed by the Joint Services Computer Resources Management Group, the U.S. Navy, the U.S. Army, and the U.S. Air Force. The handbook was developed to "provide management and engineering guidelines to achieve a reasonable level of assurance that software will execute within the system context with an acceptable level of safety risk."

For the safety engineer or PFS that deals with software controls within their system, this is the guidance to follow. Fewer and fewer systems are developed today without some type of software controls. Whether it is a computer chip preprogrammed with a few lines of firmware or millions of lines of computer code, all software must be analyzed for its contribution, or lack of mitigations, to hazards. This handbook puts the PFS on a path to analyze the safety criticality of software, along with the hazard analysis techniques and tools to get there.

Conclusion

Although this article has provided the PFS with a list of policies and guidance for conducting a systems safety engineering program, it is not exhaustive. Each program will have its unique requirements in accordance with specific acquisition milestones from concept development through sustainment and disposal. The area of systems safety engineering can be a fulfilling systems engineering discipline for the analyst or engineer. It can be very rewarding in the benefits that it provides to PMs, system designers, MAs, and most importantly, to the warfighter.

Training the Systems Safety Engineer

By Mike Zemore and Etienne (Steve) Boscovitch

- System Designs
- Materials
- Functions and Functional Allocations
- Computer Programs
- Interfaces (e.g., digital, electrical, mechanical, human/machine)
- Fuels
- Propellants
- Chemicals
- System Life Cycle
- Faults
- Fault Tolerances
- Redundancies
- Operations
- Operational Procedures
- System Effects
- Safety Procedures
- Human Tendencies
- Environmental Effects
- System Disposal

Systems safety engineering is an engineering discipline closely related to, and rooted in, systems engineering. However, training in systems engineering or a systems engineering academic degree does not fully prepare employees to perform system safety analyses within the framework of systems safety engineering standards, methods, and techniques. A typical systems safety engineer will develop to become an expert on the elements listed in the shaded box to the left.

Training an individual to conduct the requisite analyses for a given system has historically taken years of on-the-job training and individual mentoring. Today's engineering environment forces the acceleration of system safety training, leveraging academic opportunities and computer Internet-accessible, online capabilities. This article will discuss several opportunities available for introductory training in Navy systems and systems safety engineering. The impact will be enhanced, expedited, self-directed weapon system/system safety training applicable to naval weapons and weapon systems. Stakeholders will benefit with increased knowledge from their systems safety engineer, thus reducing the costs of systems safety engineering analyses and enhancing the safety of deployed systems.

The Naval Surface Warfare Center, Dahlgren Division, Systems Safety Engineering Division's (NSWCDD/G70's) function is to plan and perform systematic and rigorous systems safety engineering analyses for naval warfare systems. The objective is to predict, assess, and mitigate potential harm to personnel, equipment, and the environment through all system life-cycle phases. The division comprises three branch-level

focal areas: Engagement System, Combat System, and Platform System. Together, the division leads the way for systems safety engineering on surface naval weapon systems including:

- Gun systems
- Launchers
- Missile systems
- United Stated Marine Corps (USMC) weapons
- Integrated surface ship combat systems
- Surface ship topside pointing and firing zones
- Lasers
- Unmanned systems
- Ground platforms
- Integrated surface ship platforms

Given the importance of system safety, the division has embarked on a series of robust training activities to accelerate the learning process in support of customers and stakeholders. The fleet, program managers, program executive office, and the Naval Ordnance Safety and Security Activity (NOSSA) remain the primary customers. Therefore, the goal is to ensure that these customers have the clearest view of safety dispositions and recommendations based on reliable systems safety engineering analyses. The challenge is training professionals to become system safety experts, such that they can perform reliable safety analyses on the elements shown in the shaded box on the previous page. Skills and knowledge in these areas, combined with sound systems safety engineering methods, ensure that professionals can effectively support the customers and the goal of producing and deploying safe systems for the fleet.

In recent times, new training opportunities have presented themselves in the areas of Navy knowledge, academics, and systems safety engineering. Obviously, this occurred through the diligence of many people striving to ensure that personnel, whether civilian or military, have access to training materials and forums designed to enhance and improve capabilities. A large portion of this training is available electronically through self-guided learning sessions. These sessions have proven extremely effective as the foundational elements of systems safety engineering. The resources—Navy Knowledge Online (NKO), academia, and the Weapon System Explosives Safety Review Board (WSESRB) Interactive Safety Environment (WISE)—are available to the safety practitioner the moment they commit to the engineering discipline and are the focus of this article. Utilization of these resources, in conjunction with the division's workforce development classroom instruction, provides the safety practitioner a relevant and robust training experience. The training opportunities available to the safety practitioner with applicability to the systems safety engineering discipline are shown in Figure 1.

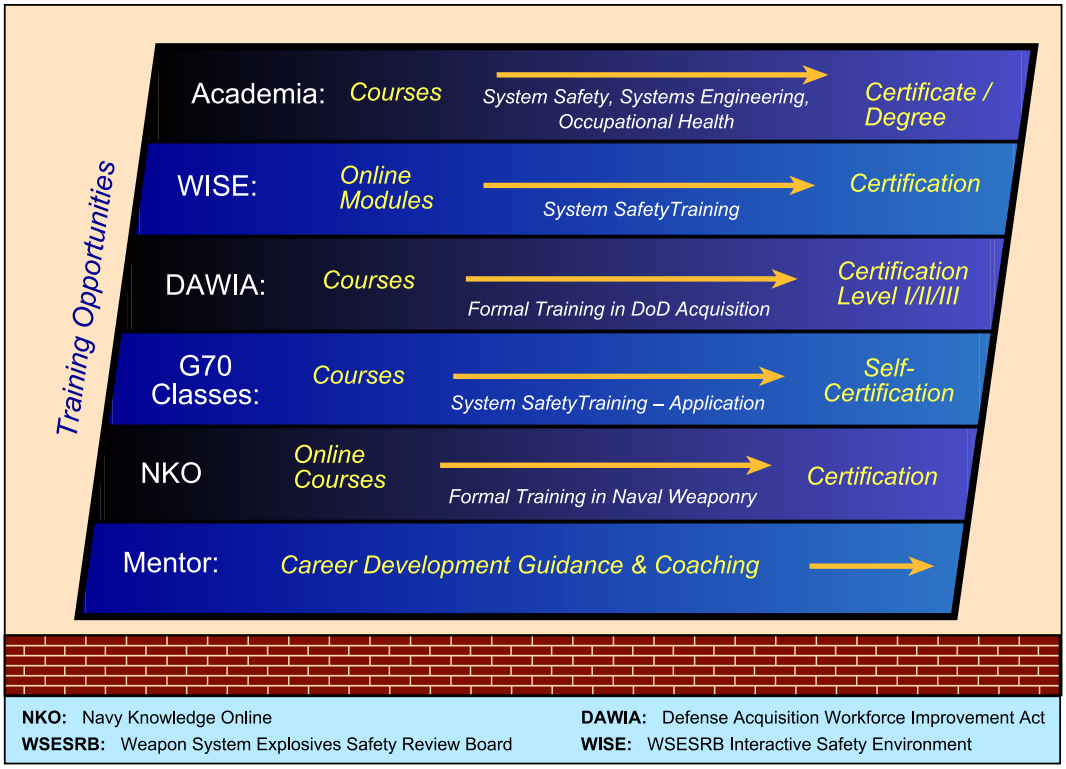


Figure 1. Training Opportunities for the Safety Practitioner

NKO is utilized throughout the Navy fleet and Navy schools as part of a multidisciplinary management approach that strategically applies learning and organizational development disciplines towards the goal of improving both performances and efficiencies. Knowledge management is the key to bringing the right information to the right people at the right time.

NKO does not provide specific online training for systems safety engineering, as would be needed to develop in-depth knowledge of systems safety engineering principles. However, NKO does present a multitude of self-guided studies to establish the foundational understanding of Navy systems, specific designs, operational considerations, and maintainability. An example is the condensed listing of combat system "A" schools shown in Figure 2. An "A" school is the Navy term for skill training. Through this online capability, safety practitioners are able to receive a specific knowledge of any combat system lesson to expand their system knowledge. This system knowledge greatly assists in the development of comprehensive and complete system safety assessments.

Delving down to specific combat system components, safety practitioners can access specific "A" schools and community-of-practice (CoP) lessons to acquire detailed understanding of system designs and functionality. For example, if a safety analysis is intended for a radar system, the practitioner can access basic radar systems theory to better understand radar functionality and then follow up with CoP lessons to understand design and use details. The CoP also provides access to subject matter experts (SMEs), the mechanism for electronic discussions, support, solutions, and lessons learned.

By utilizing NKO, the division has tapped into the Navy's Electronic Learning (E-Learning) environment in order to expedite building the foundations of Navy principles, system designs, and operational uses.

Formal degree programs from accredited colleges and universities also provide G70's capabilities in the science and engineering fields. Unlike many disciplines, systems safety engineering crosses many boundaries when considering the mechanics, materials, architectures, software control, electrical, electronics, integration, and environment of any system or collection of systems. Fortunately, academic programs establish the fundamental concepts and provide an avenue for comprehension as the multifaceted science and engineering principles are applied by the system safety practitioner. Advanced degrees further the capability while facilitating research as a fundamental objective that

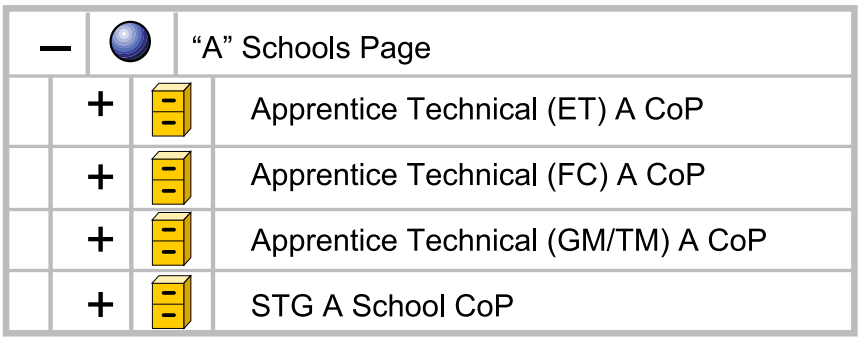


Figure 2. Condensed Listing of Combat System "A" Schools

can be focused and applied in the field of system safety.

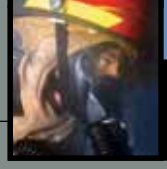
NSWCDD does not endorse one specific degree program since each program offers the practitioner a unique perspective and knowledge set needed within the systems safety engineering discipline. However, it is true that systems safety engineering closely aligns with the concepts, principles, and engineering rigor of the systems engineering program. The National Aeronautics and Space Administration (NASA) definition, provided below, does an excellent job communicating the big picture of systems engineering. Adding the word "safety" to read "Systems safety engineering is a robust…" yields a good understanding for systems safety engineering and its integration and alignment within the systems engineering process.

> Systems engineering is a robust approach to the design, creation, and operation of systems. In simple terms, the approach consists of identification and quantification of system goals, creation of alternative system design concepts, performance of design trades, selection and implementation of the best design, verification that the design is properly built and integrated, and post-implementation assessment of how well the system meets (or met) the goals.—NASA *Systems Engineering Handbook*, 1995, SP-610S.

Beyond traditional degree programs, there are several opportunities for the safety practitioner to gain relevant training within the academic environment. Historically, training in this area has focused on Occupational Safety and Health Administration (OSHA) requirements. While extremely important, OSHA-specific training does not encompass the essence of systems safety engineering as applied to acquisition programs and weapon system safety. Fortunately, there has been movement over the years to offer expanded curriculums that include systems safety engineering methods. Obviously, safety training—whether OSHA or systems safety engineering focused—can enhance the effort and add value for the practitioner, customer, and user. A number of universities (see Figure 3) now offer safety-related courses, certificates, and degrees. Examples are:

- System Safety in Systems Engineering course
  - Defense Acquisition University
- System Safety course
  - University of Southern California
- Software Safety course
  - University of Southern California
- System Safety certificate
  - University of Southern California
- Master of Science degree in Safety Sciences
  - Indiana University of Pennsylvania
- Master of Science degree program in Environmental, Health, and (workplace) Safety Management
  - Rochester Institute of Technology
- Master of Science degree program in Occupational and Environmental Safety and Health
  - University of Washington-W, School of Graduate Studies
- Master of Science degree program in Health and Safety, with a Specialization in Occupational Safety Management
  - Indiana State University, Distance Learning

While NKO and academia support the overall systems safety engineering objective, there remains no formal training or certification process for system safety practitioners. That has led to a NOSSA-sponsored program to develop a Web-based E-Learning tool targeting safety practitioners and acquisition customers that fall under the purview of the WSESRB. Given the thrust to establish a systems safety engineering certification program, this E-Learning, called WISE, provides the capability as an electronically accessible tool to capture and



Systems Safety Engineering

The Players

Figure 3. Advanced Studies

communicate safety processes while testing and potentially certifying safety practitioners at multiple levels of responsibility. The mission statement for WISE is documented as follows:

> To develop a Web-based Safety Engineering Environment that will facilitate execution of Navy weapon systems and ordnance safety processes and procedures, provide safety practitioner training, and establish certification management for individuals serving as Principals for Safety (PFS) for naval and Marine Corps programs.

Developed by EG&G under the guidance and direction of the NOSSA, the WISE program provides open access as a centralized repository of safety knowledge and training as an efficient means of learning and understanding system safety. Each WISE training module is designed to increase knowledge and comprehension of system safety processes for application within an acquisition program. The E-Learning capability comes without cost to the safety practitioner or sponsoring program office. This approach supports the initiative to facilitate training and use of consistent system safety methodologies within the Department of the Navy (DON) with minimal or no impact to program cost or schedule. The expectation is that this investment—applied across DON programs—will enhance the safety of the systems deployed and ease the process for WSESRB review. A snapshot of the WISE home page is shown as Figure 4.

G70 continues to strive towards excellence when training new practitioners in systems safety engineering and in performing system safety analyses. With the ever-changing workplace environment, it makes sense to evolve while utilizing the capabilities of NKO and WISE for training opportunities. This, coupled with academic offerings, provides the practitioner the knowledge, skills, and abilities for system safety analysis efforts.

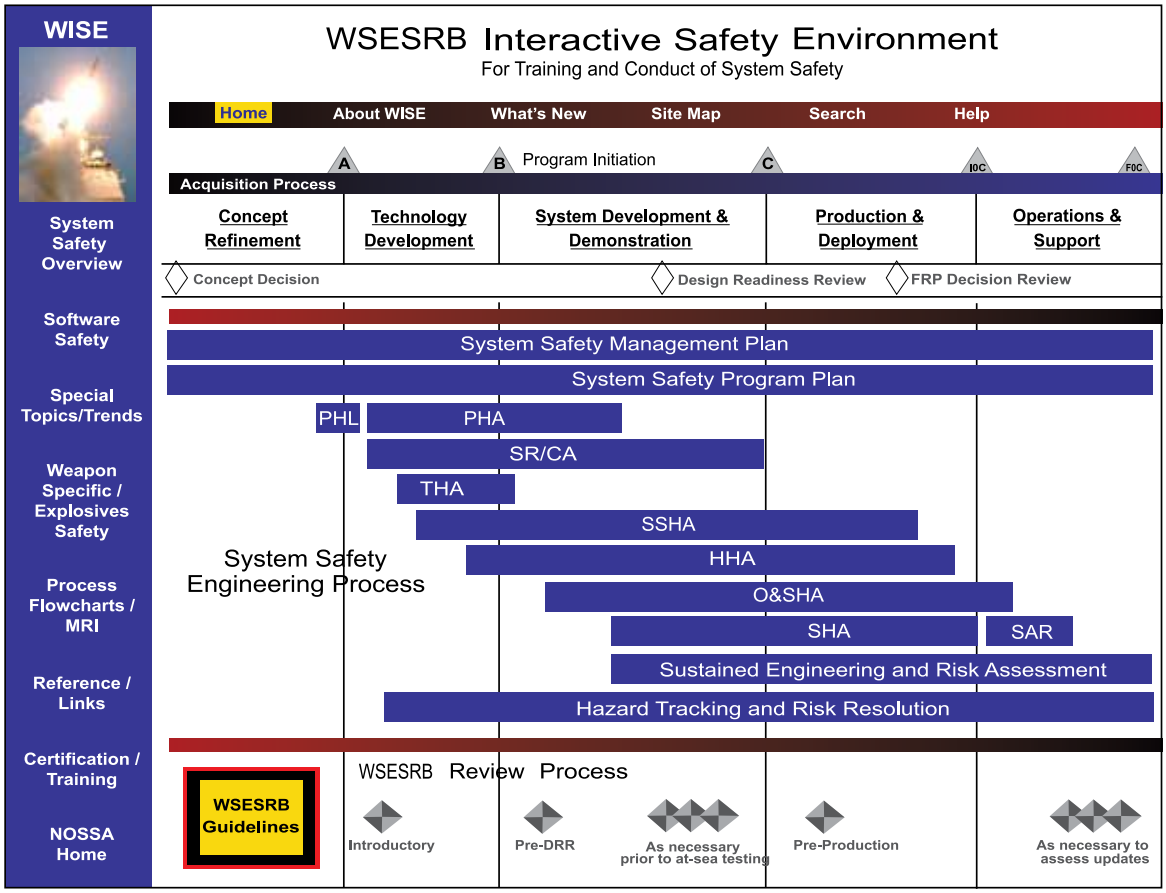


Figure 4. WISE Homepage

Establishing and Training Best Practices in Systems Safety Engineering

By Robert C. Heflin Jr.

This article serves as a follow-on to the previous article, which discussed some of the challenges involved in training systems safety engineers, and some of the ways in which those challenges are being met. Whereas that article focused more on the external and electronic opportunities available, this article will explore the currently ongoing training efforts internal to the Systems Safety Engineering Division designed to develop and implement training in safety analysis best practices as developed within the division.

Locating and recruiting trained systems safety engineers has traditionally been a significant challenge. Though systems safety engineering is a discipline within systems engineering, few institutes of higher learning provide specific systems safety engineering instruction. Therefore, only a small number of college graduates emerge each year with an understanding of what system safety is about. While a new crop of computer scientists, electrical engineers, mathematicians, etc., graduate each year and enter the workforce able to hit the ground running in most career fields, scientists and engineers who land in system safety are often confronted with unique and challenging concepts that their academic training has not exposed them to. Over the past several years, the Systems Safety Engineering Division (G70) of the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) has implemented a series of efforts geared toward developing and standardizing best practices in the implementation of system safety analysis, and providing detailed systems safety engineering training, in utilizing those practices, to the entire division workforce, as well as to support contractor personnel.

The centerpiece of these efforts is known as the Workforce Development Project, referred to as WFD. The initiative grew from a Lean Six Sigma Value Stream Analysis (VSA) of the system safety analysis process as practiced within G70. The VSA was chartered to examine the business model and technical processes utilized within G70 in performing systems safety engineering for the Department of Defense (DoD), producing the necessary artifacts to document the results of those analyses and, ultimately, ensuring the deployment of safe systems for our military forces. During the VSA, G70 senior management and technical personnel deconstructed the overall system safety

analysis process as ideally practiced and identified 34 separate areas of focus that participants concurred are key elements in performing consistent, high-quality safety analysis. While most of these areas fell within the technical analysis process itself, others were associated more closely with associated functions, such as communication and training. During discussions on how to best perform each of these focus areas, it quickly became apparent that insufficient formalized training was the most significant impediment G70 faced in ensuring the performance of consistently high-quality system safety analyses. It was recognized that training in system safety analysis had traditionally been conducted on an informal, one-to-one basis by senior engineers mentoring junior engineers. Over the course of decades— as systems became more and more complex, new technologies were introduced, and computer programs were heavily relied upon to control weapon and ordnance systems—systems safety engineering methodologies and practices were not consistently evolving or being practiced across the division.

Addressing the issue thus necessitated a two-pronged approach. First, safety analysis methodologies within G70 needed to be standardized, and second, a process for training personnel in those methodologies on a consistent basis needed to be formalized. To accomplish the former, G70 embarked on a series of Lean events aimed at developing a concise and consistent process for safety analysis implementation and documentation. Over a 24-month period, individual events were conducted for each of the 34 identified focus areas. Each event included personnel from each of the three branches within the division, as well as contractor support personnel and customer representatives wherever possible. These events reviewed existing methodologies for performing and/or documenting different major elements within the overall system safety process, and established and documented a single best-practice methodology for each of those elements. This best practice was accepted as part of the official consolidated G70 safety analysis process.

The largest and most significant of the 34 focus areas identified in the VSA became the basis for addressing the second part of the problem—training the workforce. The WFD was initiated immediately following the VSA and ran concurrently with the other focus area Lean events over the 2-year period. The objectives of the WFD were to identify the primary training needs with the division and to develop necessary strategies and materials to meet those needs. The team researched in detail the system safety training already available, both commercially and within the government. Mindful of training budget constraints, care

was exercised to avoid "reinventing the wheel" by ensuring that currently available training was utilized wherever prudent, and that effort was not duplicated in developing materials for already available training. The WFD team divided their objectives into short- and long-term needs. For the short term, effort was focused on providing necessary high-level foundational instruction on the overall safety analysis process and the types of systems on which G70 practices safety analysis in a structured classroom environment. The currently ongoing longer term effort, known as WFD Phase II, is aimed at providing the detailed instruction necessary to allow the systems safety engineer to implement the methodologies and best practices developed by the organization through the focus area events, in conducting a thorough system safety analysis on any given system.

To accomplish the short-term goal of providing a high-level foundation of systems and system safety knowledge, the WFD team developed a curriculum consisting of six classes. These six classes focused on introducing the students to U.S. Navy and U.S. Marine Corps systems, describing system safety concepts at a high level and detailing the overall system safety analysis process as designed for practice within G70. Each class was offered on multiple dates and times over a 6-month period to the existing workforce and planned for further future periodic iterations to account for workforce expansion and turnover. Attendance was mandatory for some of the classes and voluntary for others, as necessitated by the importance of the material being presented and the topical familiarity of individual safety engineers.

As the target audience for these classes comprised professionals, subject matter testing was not deemed an appropriate method of verifying comprehension and understanding. Instead, the idea of self-certification was introduced. Under this paradigm, students are required to judge for themselves when they have mastered the information presented. At that time, they inform one of several designated recordkeepers, who ensure that a master WFD database is updated to reflect that certification. During each class, students were provided with multiple contacts considered to be subject matter experts, who were available throughout the 6-month period to aid in the understanding of concepts being discussed. In this fashion, the entire workforce was brought relatively quickly to a common level of basic understanding of the specified concepts.

Once the workforce had achieved these short-term goals of understanding, Phase II of the WFD project was entered and is currently ongoing. The goal of Phase II is to develop and implement an instruction process through which the workforce is

educated in how to apply each of the best practices previously developed during their system safety analyses. The plan for this phase of WFD is to develop a fictitious system and to conduct a complete safety analysis on that system via a series of workshops, which will encompass each of the elements of the safety analysis process for which an individual focus area Lean event was conducted. Development of a useable representative system will require development of not only a design for the system, but also all associated documentation typically associated with the systems analyzed in G70, including but not limited to, a Concept of Operations, System Development Specification, Interface Design Document, maintenance and user documentation, etc.

The workshops will include instruction in methodology by senior division personnel and supervised group projects implementing the methodology for executing the specific aspect of safety analysis being taught. Each workshop will be conducted several times in order to include all division personnel. As the system safety analysis process is one in which each step builds upon the product of the previous steps, at the conclusion of instruction for each aspect of the process, the products of all groups will be meshed into a single, comprehensive analysis product for the system, which will then be carried forward as an input into the next series of workshops.

The example system under development for use in these workshops is designed to be relatively simple to understand while simultaneously encompassing design aspects of many similar systems G70 personnel are currently analyzing. In this way, the system will be easily relatable to by students with varying degrees of systems and system safety experience. Once a safety engineer has completed the entire workshop series, he or she will be well-versed in the G70 best practice methodology for conducting every significant aspect of the system safety analysis process. Once completed and implemented, the workshop series will be repeated periodically as needed as the workforce changes and will be updated as new techniques and technologies emerge to evolve the safety analysis process.

Establishing best practices and training for the workforce in a consistent and repeatable methodology for implementing those practices is a formidable task in any discipline. In system safety, where limited formal education is available outside of the offices of the practitioners, it is particularly daunting. However the Systems Safety Engineering Division is facing this task with a unique and consistent solution, which will provide the capability to train the division workforce and help ensure the safety of our weapon systems and, thus, of those who use them to defend our freedom.

Crew members fighting fires on board USS *Forrestal*, 29 July 1967

Photo Courtesy of U.S. Navy

Navy Safety Review Boards: WSESRB, SSSTRP, and FISTRP

By Mary Ellen Caro, David Shampine, and Jack Waller

In 1967, an electrical anomaly caused a Zuni rocket to be discharged aboard ship during combat operations in the Gulf of Tonkin, causing the worst carrier fire since World War II and killing 134 Sailors. The Navy's response was a concentrated effort to address safety and establish a process to mitigate the chances that such devastation would happen again aboard a naval vessel. Central to that effort was the establishment of an independent board comprising subject matter experts in various system safety-related disciplines within systems engineering, to provide review and oversight of systems executing safety programs. Over time, the increasing number and complexity of systems under development led to the formation of more specialized subpanels to aid the board in that effort. The articles in this section of the Leading Edge describe that board and the subpanels that subsequently grew from the effort to ensure that U.S. Navy weapons are safe to develop and use.

—Robert C. Heflin

USS *Forrestal* at sea, 31 May 1962, with Phantom fighters on deck

Photo Courtesy of U.S. Navy

Firefighters check the burned out hulk of an A-4E Skyhawk destroyed in the worst fire aboard a U.S. aircraft carrier. The fire erupted aboard USS *Forrestal* (CVA 59) on 29 July 1967 as the carrier was on station off Vietnam and killed 134 of the ship's crew.

Photo Courtesy of U.S. Navy

(WSESRB)
Weapon System Explosives Safety Review Board

By Mary Ellen Caro

(SSSTRP)
Software System Safety Technical Review Panel

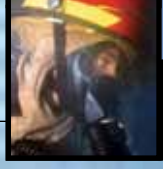
By David Shampine

(FISTRP)
Fuze and Initiation System Technical Review Panel

By Jack Waller

At sea aboard Precommissioning Unit (PCU) *Ronald Reagan* (CVN 76) 7 May 2003 – The Navy's newest *Nimitz*-class aircraft carrier tests its countermeasure wash down systems (CMWDS) during scheduled builder sea trials off the coast of Virginia. CMWDS includes a series of sprinklers in vital areas throughout the ship to help contain the spread of fire or chemical, biological, or radiological (CBR) attacks.

U.S. Navy photo by Photographer's Mate 2nd Class James Thierry. (RELEASED)



The Navy's Weapon System Explosives Safety Review Board (WSESRB)

By Mary Ellen Caro

The Navy's Weapon System Explosives Safety Review Board (WSESRB) serves as the Navy's independent oversight body for weapons and explosives safety. The scope of the WSESRB includes weapon systems being developed or used by both Navy and Marine Corps. The latest draft of NAVSEAINST 8020.6E, *Department of the Navy Weapon System Explosives Safety Review Board*, signed in March 2008, also gives the WSESRB oversight responsibility for directed-energy weapons.

The WSESRB was originally established after a series of catastrophic explosive events, including USS *Forrestal* and USS *Oriskany* conflagrations. The loss of life and property resulting from these mishaps led to recommendations from boards of inquiry investigating these mishaps, resulting in the establishment of the WSESRB in 1967 to review the explosives safety of weapons. The WSESRB is chartered by the Chief of Naval Operations (CNO) to provide independent oversight of the Department of the Navy's (DON's) weapon program safety efforts. The majority of programs reviewed by the WSESRB are acquisition programs for new and upgraded weapon and combat systems.

The Chairperson of the WSESRB is dual-hatted, serving as the Executive Director of the Naval Ordnance Safety and Security Activity (NOSSA) and as Naval Sea Systems Command (NAVSEA) Director of Ordnance Safety (SEA 00VW). This position also carries the Technical Warrant for Weapon Systems, Ordnance, and Explosives—Safety and Security. The WSESRB draws support from NOSSA's Weapons System Safety Directorate (N3). NOSSA N3 provides the Vice Chair and Secretariat. WSESRB membership is composed of representatives from each of the major Navy Systems Commands, Warfare Centers, fleet representatives, the Naval Safety Center, the Navy/Marine Corps Public Health Center, and the Navy Explosives Ordnance Disposal Technology Center. Specific technical expertise is also drawn from the Warfare Centers and the technical warrant holder (TWH) community.

As part of the weapon development process, the WSESRB also looks to the Ship Weapon Integration Team (SWIT), composed of members of NAVSEA and Naval Air Systems Command (NAVAIR) activities—to ensure that the weapon can be safely handled and stowed aboard ship.

The ultimate goal of the WSESRB is to ensure that the weapons and weapon control systems that the Navy and Marine Corps field are safe for the users. The Board also evaluates weapon systems developed by other services to ensure that they are safe to carry and operate from Navy platforms.

Early engagement of the WSESRB review process benefits the DON, as well as the acquisition program manager (PM). Early incorporation of safety requirements and allocation of resources for safety analysis and testing allows a program to plan and execute the weapon system safety program and uncover safety issues when they are less expensive, and solutions are easier to incorporate into the system design. Late identification of safety issues can have a significant impact on cost and schedule and can pose safety risks to users.

The goal of the WSESRB is to ensure that during development, weapons are analyzed and tested for their safety characteristics. Has the weapon been exposed to all of the environments that it will likely see in its lifetime? Are there any safety issues or risks resulting from these analyses and tests? Areas of review include:

- Energetic material qualification
- Hazard assessment tests
- Insensitive munitions
- Electromagnetic environmental effects testing, including Hazards of Electromagnetic

Radiation to Ordnance (HERO) and electrostatic discharge
- Temperature and vibration exposures
- Shipboard shock and packaging tests

Two areas require special attention for the systems that the Navy is currently developing: software and fuzing/initiation systems. More software is being used to execute safety-critical functions within weapons or within the systems controlling their selection and launch. With the advent of electronic safe and arming devices, fuzing systems have become more complex, and their safety functions are being distributed throughout the system architecture. For these reasons, there are two subpanels of the WSESRB: the Software System Safety Technical Review Panel (SSSTRP) and the Fuze and Initiation System Technical Review Panel (FISTRP). Acquisition programs brief these panels separately from the WSESRB, allowing more time to be spent on these safety-critical aspects of a program. The SSSTRP and FISTRP support the Board, and their findings are not official until they have been approved by the WSESRB.

Weapon acquisition programs come before the WSESRB at several points in their acquisition life cycle to obtain Board concurrence before proceeding to the next stage of development. Normally, there is an introductory review upon a contract award to assess the planned safety analysis and testing program. This review can benefit PMs in the early stages of a program acquisition by ensuring the needed testing and analysis are available by the time the program is ready to proceed to production.

Another time for WSESRB review is prior to a Critical Design Review (CDR). At CDR, the design is usually frozen, which makes changes in the design to eliminate or mitigate a safety issue difficult and costly. The CDR WSESRB review can mitigate the need for later design changes. The Board expects programs to follow MIL-STD-882's "Safety Order of Precedence" in the mitigation of hazards and risks. Design changes to eliminate a hazard are preferable to installing a safety device (e.g., protection mechanism such as a guard), which in turn, is preferable to a warning device. The least preferred method of risk mitigation is the use of training and procedures. Humans make errors, and even a small error can have catastrophic results when employing weapons and ordnance systems.

A WSESRB review is also required prior to the deployment of a system to ensure that all of the safety testing and analysis has been completed with no unresolved safety issues. At this time, the risk of the system is characterized, documented, and communicated to the user community. It is also a review where the board ensures that training programs have been established and

documentation—in the form of operating and maintenance procedures—are in place for safe operation of the system.

One other time where WSESRB approval is required is for a test event aboard ship where developmental weapons or weapon systems are being used. This is one area where the fleet will see the effects of the WSESRB process. Acceptance trials, Combat System Ship Qualification Trials, and predeployment workups are some of the events requiring WSESRB approval.

The WSESRB Secretariat (NOSSA N3) is available to the PMs and program Principals for Safety to coordinate WSESRB reviews. Points of contact have been established for different families of weapon systems. The Secretariat staff can make recommendations for WSESRB reviews and facilitate scheduling Board meetings. Each review by the WSESRB (or an associate board; i.e., the SSSTRP or FISTRP) requires the submission of a technical data package. The expectations for these data packages are found in NAVSEAINST 8020.6E.

WSESRB reviews provide Navy and Marine Corps PMs with an objective assessment of their safety program from a panel of subject matter experts. This review is the Navy's focal point for the prevention of mishaps involving ammunition, explosives, and related systems—thereby eliminating deaths, injuries, lost workdays, and property and environmental damage.

The Navy's Software System Safety Technical Review Panel (SSSTRP)

By David Shampine

The Software System Safety Technical Review Panel (SSSTRP) is part of the safety team at the Naval Ordnance Safety and Security Activity (NOSSA) and was organized to support the Weapon System Explosives Safety Review Board (WSESRB). The goal sought in establishing the SSSTRP is to provide a more thorough review of the complex safety issues related to software control of systems and to reduce the burden on both the program office and the WSESRB in the review of systems that are software intensive or where software is the only issue being addressed. In addition, the SSSTRP may be used in lieu of interim WSESRB reviews not associated with major milestones. Decisions regarding substitution of the SSSTRP review for a WSESRB review are normally decided on a case-by-case basis by the WSESRB Chairperson.

WSESRB meetings are scheduled during the second full week of each month, while SSSTRPs are scheduled during the 2-week period following WSESRB week. The majority of program offices try to complete an SSSTRP review prior to going into a WSESRB meeting. The SSSTRP meeting workload is coordinated by the SSSTRP Team to be in concert with the WSESRB agenda during regularly scheduled weekly meetings. The Systems Safety Engineering Division of the Naval Surface Warfare Center, Dahlgren Division plays a significant role in providing technical subject matter experts (SMEs) as panel members to the SSSTRP. Other organizations—such as the Naval Undersea Warfare Center, Newport and the Naval Air Warfare Center, China Lake—also provide SMEs on a regular basis. These panel members are selected from a pool of professionals with backgrounds in computer science, computer engineering, and system safety.

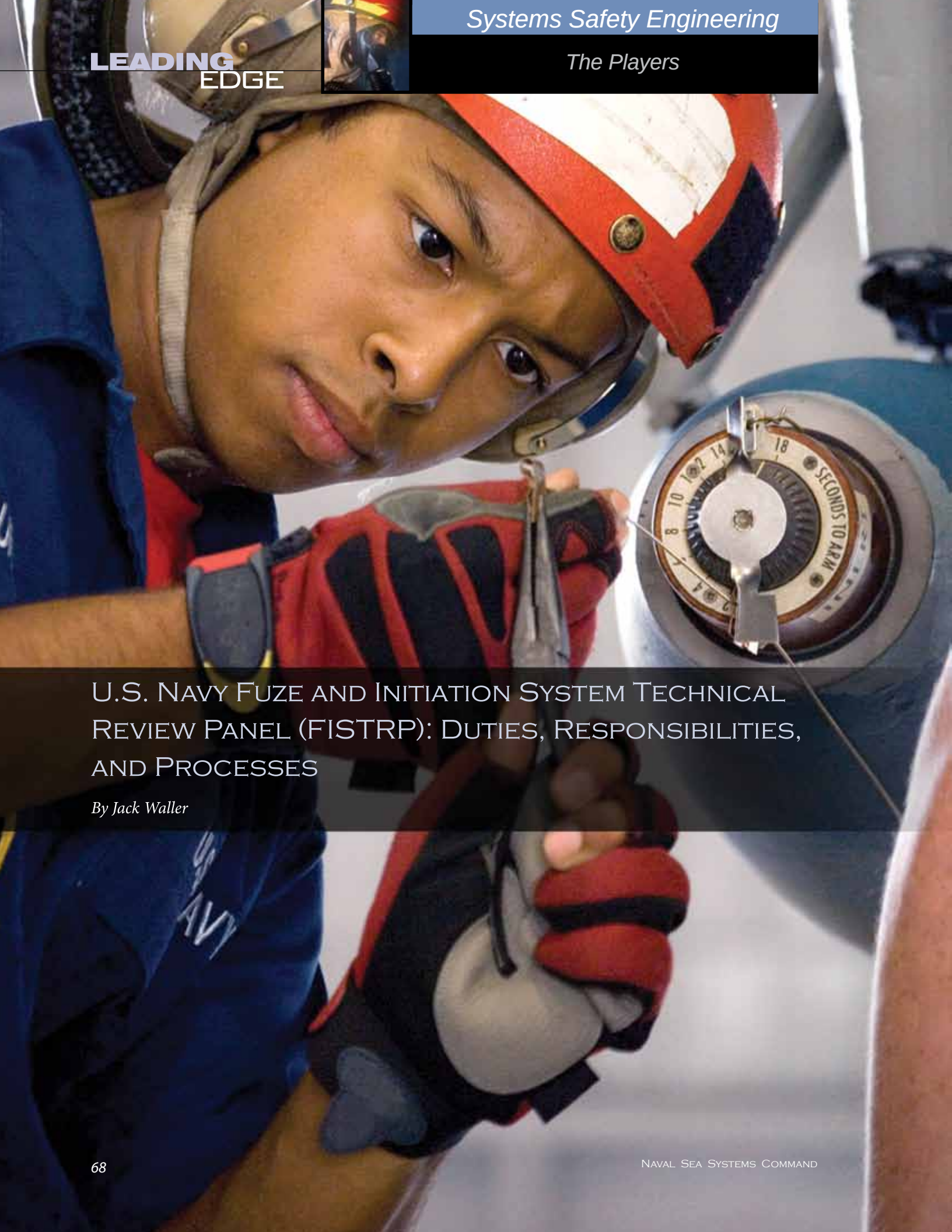
In preparation for an SSSTRP review, the program office provides a detailed Technical Data Package (TDP) that

has been developed in accordance with the guidelines established in NAVSEAINST 8020.6E, Enclosure 8. This package is submitted no later than 21 days in advance of the target date for the meeting. Once the TDP is received by the WSESRB, it is reviewed by the NOSSA Point of Contact and the SSSTRP Chairperson for technical content to ensure it meets the intended guidelines, and the formal presentation, if required, is then placed on the schedule. If the Chairperson determines that the issues pertinent to the review do not require a formal presentation, the program may be allowed to pursue its purpose via letter. In such a case, the TDP is allowed to stand on its own merit, and the data is disbursed electronically and reviewed by panel members individually.

SSSTRP meetings consist of three parts: the pre-brief, the presentation, and the caucus. The pre-brief is conducted by the Chairperson and is meant to set the tone for the presentation. Any preliminary issues discovered by panel members during the review of the TDP are discussed during the pre-brief and are identified as potential focus points for discussion during the presentation. The presentation is scheduled to last no more than 6 hours, with the program office being responsible for managing both the content and the time to present the safety case for the system under review. The caucus immediately follows the presentation, with its attendance limited to the panel members and the program's Principal for Safety. During this phase of the process, the panel members discuss the data presented in the data package and during the presentation, and then develop recommendations and action items for the program to aid in improving their safety program. At the end of the meeting, the program representatives are provided with a draft copy of the results of the review, with the caveat that it is not final until approved by the WSESRB.

Additionally, the SSSTRP conducts informal technical assistance meetings, which are not official meetings and need not be reported out to the WSESRB. This is an opportunity for the program office to obtain guidance and advice at key points in time within the acquisition cycle. There are no minutes taken, findings assigned, or letter generated as a result of the meeting. The WSESRB considers technical assistance meetings an informal information exchange to assist the program office in understanding WSESRB interpretation of safety regulations, instructions, and policy. These meetings are not intended to discuss concurrence with program office design, development, or acquisition goals.

Since its inception, the SSSTRP has reviewed numerous programs in its role as the software arm of the WSESRB. It has provided for these systems a detailed review of their software safety programs and has provided technical assistance and recommendations for improving the depth and quality of their software safety analysis. In this way, the SSSTRP continues to provide valuable oversight for the safety of the warfighter utilizing modern, software-intensive systems.



U.S. Navy Fuze and Initiation System Technical Review Panel (FISTRP): Duties, Responsibilities, and Processes

By Jack Waller

Introduction

The Navy's Fuze and Initiation System Technical Review Panel (FISTRP)—which is a subpanel of the Navy's Weapon System Explosives Safety Review Board (WSESRB)—reviews the designs of fuzes and initiation systems to assure that they are safe for their intended use in munitions. Fuzes and initiation systems are devices that control the safety of the munition during manufacture, handling, logistic deployment and use. The FISTRP is tasked with reviewing fuze and initiation system designs during development and providing an assessment of the compliance of these systems with safety requirements; FISTRP is a vital arm of the Navy's independent safety review program.

Purpose and Membership

Technical review panels (TRPs), functioning as subpanels to the Navy's WSESRB, were implemented in the early 1990s to add a focused safety review capability to the overall WSESRB review function. The operational processes for TRPs were developed by the WSESRB. The FISTRP is one of these regularly meeting subpanels of the WSESRB.

The purpose of the FISTRP is to provide expert technical safety review of the design of safety and arming devices/fuzes, ignition safety devices, and related safety devices used in Navy weapon systems. The FISTRP reviews system designs against established Department of Defense (DoD) or international safety design requirements, including North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs) and U.S. Military Standards. Safety criteria utilized for a review by the FISTRP include, but are not limited to:

NATO STANAGs:

- 4187—*Fuzing Systems Safety Design Requirements*
- 4368—*Electric and Laser Ignition Systems for Rockets and Guided Missile Motors Safety Design Requirements*
- 4497—*Hand-Emplaced Munitions (HEM), Principles of Safe Design*

Military Standards:

- 1316—*Fuze Design, Safety Criteria for*
- 1901—*DoD Design Criteria Standard, Munition Rocket and Missile Motor Administration System Design* and
- 1911—*Hand-Emplaced Ordnance Design, Safety Criteria f*or

The *WSESRB Technical Manual on Electronic Safety and Arming Devices with Non-Interrupted Explosive Trains* is also used as a resource for following safety criteria.

By ensuring adherence to the principles espoused in these guidelines, the FISTRP is able to address the multitude of areas where safety risk is inherent in these critical systems. For example, STANAG 4187 provides detailed safety design criteria for warhead safety and arming devices and fuzes. A FISTRP review results in an assessment of the safety design and recommendations for the program and the WSESRB. This assessment is documented in a summary report and includes justifications for the recommendations made.

The WSESRB chairperson designates the chairperson for the FISTRP. The remainder of the panel is composed of technical experts drawn from a variety of areas across the Navy and can include subject matter experts from other services, as necessary. In addition, due to the multiservice utilization of many modern munitions, the Navy FISTRP often acts in concert with other services to hold joint service reviews. The FISTRP interfaces directly with the Army's Fuze Safety Review Board and members of the U.S. Air Force's Nonnuclear Safety Board on fuze and initiation system programs of mutual interest. Members are selected for their expertise in:

- Fuze design
- Ignition safety device design
- Explosives safety
- Logic systems
- System safety
- Fuze development
- Individual weapon systems design and development

Members are rotated, as required, to ensure that they do not have conflicting interests in the program being reviewed. Members of the FISTRP also actively participate in DoD's Fuze Engineering Standardization Working Group (FESWG), which develops and maintains fuze and initiation safety design requirements for DoD and keeps the WSESRB abreast of the FESWG activities.

Scope

The scope of a FISTRP will vary depending upon the needs of the program. FISTRP reviews generally fall into one of three categories: a full FISTRP meeting, a letter data package review, or a technical assistance meeting. A full FISTRP meeting involves a formal safety review of the design of safety and arming device/fuze, ignition safety device, or related safety device, and requires a complete technical data package before the FISTRP will be scheduled. The program then follows with an in-person presentation to the panel. FISTRP recommendations and action items are

coordinated with and documented by the WSESRB. When limited or narrowly focused issues are in question, or when closing out previous action items, a letter data package review may be sufficient in lieu of a full FISTRP meeting. In this instance, the program representatives do not need to appear before the panel to present their data; they simply provide the necessary data in writing, accompanied by a letter explaining their purpose for submission. The results of letter data package reviews are also coordinated with and documented by the WSESRB. Technical Assistance, or Tech Assist, meetings are informal reviews of issues or concepts where no formal recommendations are provided to the program. These are provided primarily to aid the program in addressing specific issues and defining a way forward.

While all requirements in the design safety area are important and are assessed during a FISTRP review, the following areas normally receive particular attention during a FISTRP:

- Identification/description of independent safety features in safety devices, complex logic devices, or firmware used in the safety logic
- Cut sets and numerical analysis associated with fault tree analysis
- Safety and environmental test programs
- Qualification of explosive devices

The Review Process

The program will recommend the appropriate level of review and coordinate the review type and review date with the FISTRP chairperson and the appropriate WSESRB point of contact (POC) for the program. Typically, FISTRPs will be held 15 to 30 days in advance of a regularly scheduled WSESRB. The Chairperson of the FISTRP is responsible for contacting the other members and making arrangements for their attendance. The length of the meetings will generally be 1 day or less. A typical 1-day FISTRP review will consist of no more than 5 hours of review/discussions with the program representatives and up to 3 hours for panel members to caucus and draft findings and recommendations.

Lessons Learned

Over time, and as the FISTRP process continues to be employed, a number of lessons learned and observations arising from the FISTRP process are worth noting:

Lesson 1: Recent acquisition policy, along with technology advancements, has resulted in a widening of initiation safety system design responsibility. Evolution of safety design requirements can be seen in the requirements for in-line ignition systems for safety and arming devices and rocket motor ignition systems, programmable logic devices, and built-in test features. These factors have expanded the design safety requirements and their application—increasing the potential for unfamiliarity and misunderstanding—and have resulted in an increased need for design safety evaluation provided by forums such as the FISTRP.

Lesson 2: Design safety evaluations early in the development process are essential to arriving at the most effective design approaches, while minimizing the impact to the programs involved. Unfortunately, program costs and schedules have been impacted as the result of lack of compliance with design safety requirements. Technology advancements also impact safety design criteria. This is particularly true in the rapidly advancing capabilities of logic devices and their associated tools and implementation. The safety community is examining these impacts and applying lessons learned to the existing safety design criteria documents.

Lesson 3: Arming decisions for military munitions are generally, though not always, based on the existence of some very simple conditions and environments. In these cases, it is strongly preferred that the complexity of the safety features validating these conditions and enabling arming be minimized to preclude inadvertent subversion via unexpected or unrecognized paths.

Lesson 4: Not every design can be evaluated solely by analysis. Comprehensive test plans often expose safety and reliability issues that are not caught during paper evaluations.

Lesson 5: As joint efforts increase both within DoD and within NATO, the coordination of safety design requirements for fuze and initiation systems may be impacted. Similarly, as technology progresses, the safety requirements tend to evolve to address issues that did not previously exist. Evidence of this can be seen in the move away from U.S. Military Standards to STANAGs, as well as the rapid progression of electronic logic devices and the movement to all-electronic safety devices. The NATO and DoD communities are adapting to these conditions through the updating of design safety criteria.

Summary

The FISTRP provides a detailed review forum for the safety design aspects of fuze and initiation systems in support of the WSESRB. The FISTRP is tasked with reviewing fuze and initiation system designs against safety design criteria established both nationally and internationally in STANAGs and U.S. Military Standards. These reviews normally take place prior to major milestone decisions; however, experience has shown that earlier safety assessment of designs is the most effective. The FISTRP membership provides a broad spectrum of experience and expertise during the review process. This includes participation of U.S. Army and Air Force representatives when available and appropriate. The overall goal of the WSESRB FISTRP is to enhance the safety of fuze and initiation system designs via an independent assessment so that the systems comply with applicable safety requirements.

Joint Service Weapon Safety Review Processes

By Robert Gmitter

Background

The challenges to designing, procuring, and fielding safe joint service weapon and laser systems for the warfighter include: weapon/environment interoperability, service-unique design requirements, service-unique testing requirements and processes, and differences in service's safety and laser review processes. There has been no single joint service safety review board or authority to address these challenges in a coordinated manner. Weapon system and laser safety releases, approvals, or certifications were required from each of the multiple service safety review boards as shown in Figure 1. Each of these individual service safety review boards utilizes unique processes designed to meet their specific requirements. The downside of these service-unique reviews for program managers (PMs) is that it is often expensive, redundant, and time-consuming; it also has the potential to result in conflicting safety requirements or actions.

This is an inherent problem for United States Special Operations Command (USSOCOM) weapon and laser system acquisition programs since USSOCOM is composed of elements from all four branches of the U.S. armed forces (see Figure 2). The USSOCOM Acquisition Executive determined, therefore, that all weapons, munitions, ordnance, laser systems, or related devices developed or procured for USSOCOM use would be considered ***joint use systems*** since they would be available for use by all service components of USSOCOM.

USSOCOM Joint Weapon Safety Review Process

In July 2005, as the result of a request from USSOCOM, the Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force (TF) chartered a Joint Weapon Safety Working Group (JWSWG) to begin developing a collaborative joint service safety review process for USSOCOM weapon, ordnance, and laser systems in order to eliminate the inefficiencies inherent in the safety review process. The JWSWG consisted of safety and laser experts from USSOCOM, the Army, the Navy, the Marine Corps, the Air Force, the Department of Defense Explosives Safety Board (DDESB), and the Office of the Under Secretary of Defense (OUSD) for Acquisition, Technology, and Logistics (AT&L). The JWSWG used, and is continuing to use, the following approach to develop the collaborative USSOCOM Joint Safety Review Process:

- Requests candidate USSOCOM programs to validate the process
- Modifies the process as necessary

Figure 1. List of U.S. Services' Safety Review Boards and Organizations

Figure 2. USSOCOM Organizations

- Proceeds with full implementation
- Continues modifications to process, based on lessons learned

The USSOCOM Joint Safety Review Process is shown in Figure 3 and is designed to deliver safe weapon systems to the USSOCOM warfighter through the coordinated and collaborative efforts of the individual service's safety review authorities. Classified joint safety reviews are currently not part of this process.

The USSOCOM Joint Weapon Safety Review process consists of seven main elements:

1. Collaborative planning & consolidation of requirements
2. Adjudication of requirements (if necessary)
3. Execution of testing and analysis for system/product
4. Collaborative reviews of testing and analysis results
5. Adjudication of results (if necessary)
6. Identification and documentation of residual risks (if necessary)
7. Acquisition community acceptance of residual risk(s). User representative must provide formal concurrence prior to all ***high*** and ***serious*** risk acceptance decisions.

There are three major participants in the USSOCOM Joint Weapon Safety Review Process: System Safety Lead (SSL), Service Safety Review Coordinator (SSRC), and the Lead Service Safety Review Coordinator (LSSRC).

The SSL is the acquisition PM's system safety representative and is usually the Principal For Safety (PFS) for U.S. Navy and Marine Corps programs. The SSL's responsibilities include leading the Safety Integrated Product Team (IPT) or System Safety Working Group (SSWG), as well as executing the System Safety Program (SSP) and System Safety Program Plan (SSPP). The SSL is appointed by the acquisition PM.

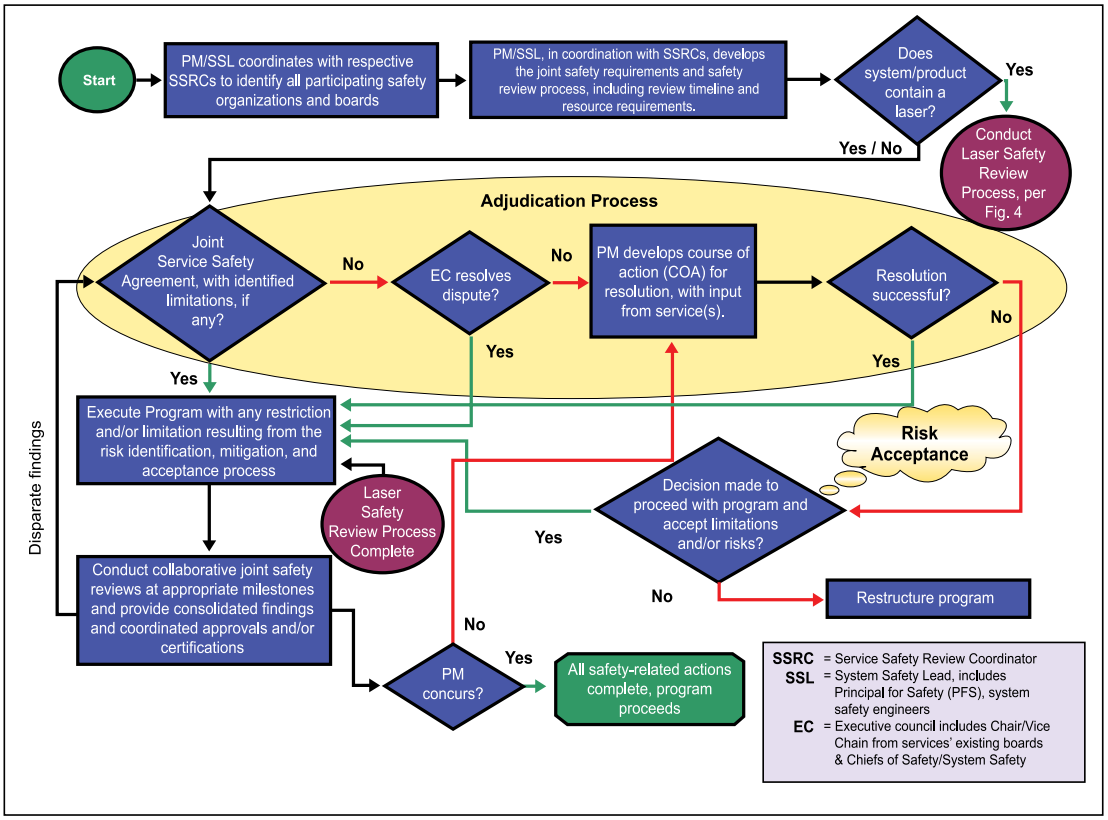


Figure 3. Joint Weapon Safety Review Process

Each SSRC is selected by a service's safety review authority or USSOCOM. The SSRC serves as the primary point of contact to assist the SSL and work with the LSSRC to help facilitate collaborative joint safety reviews of USSOCOM weapon systems, ordnance, and laser systems. An SSRC may designate a technical representative to assist and serve as the SSRC's technical POC.

The acquiring service or USSOCOM provides the LSSRC, who coordinates with the other SSRCs and the SSL for:

- Safety technical data package (TDP) content
- Joint review of the TDP
- Conduct of the Joint Boards' review, if required
- Drafting of letter and coordinating final signatures
- Monitoring closure of Joint Boards' findings
- Drafting and coordinating signatures on final letter from the joint services' safety organizations providing safety verification to support fielding/operational use

The leadership role in the USSOCOM Joint Weapon Safety Review Process is provided by the Executive Council (EC), which comprises the Chair/Vice Chair from the existing individual weapon system safety boards and the designated U.S. Army Chiefs of Safety/System Safety. The purpose of the EC is to resolve disparities among the services regarding weapon safety requirements and findings from the boards. The EC does not resolve laser safety requirements or findings.

USSOCOM Joint Laser Safety Review Process

Similar to the USSOCOM Joint Safety Review Process depicted in Figure 3 is the USSOCOM Joint Laser System Safety Review Process. This process, shown in Figure 4, was designed to deliver safe laser systems to the USSOCOM warfighter through the coordinated and collaborative efforts of the individual service's laser safety authorities.

There are two major participants in the USSOCOM Joint Laser System Safety Review Process: the Service Laser Safety Review Coordinator (SLSRC) and the Lead Service Laser Safety Review Coordinator (LSLSRC).

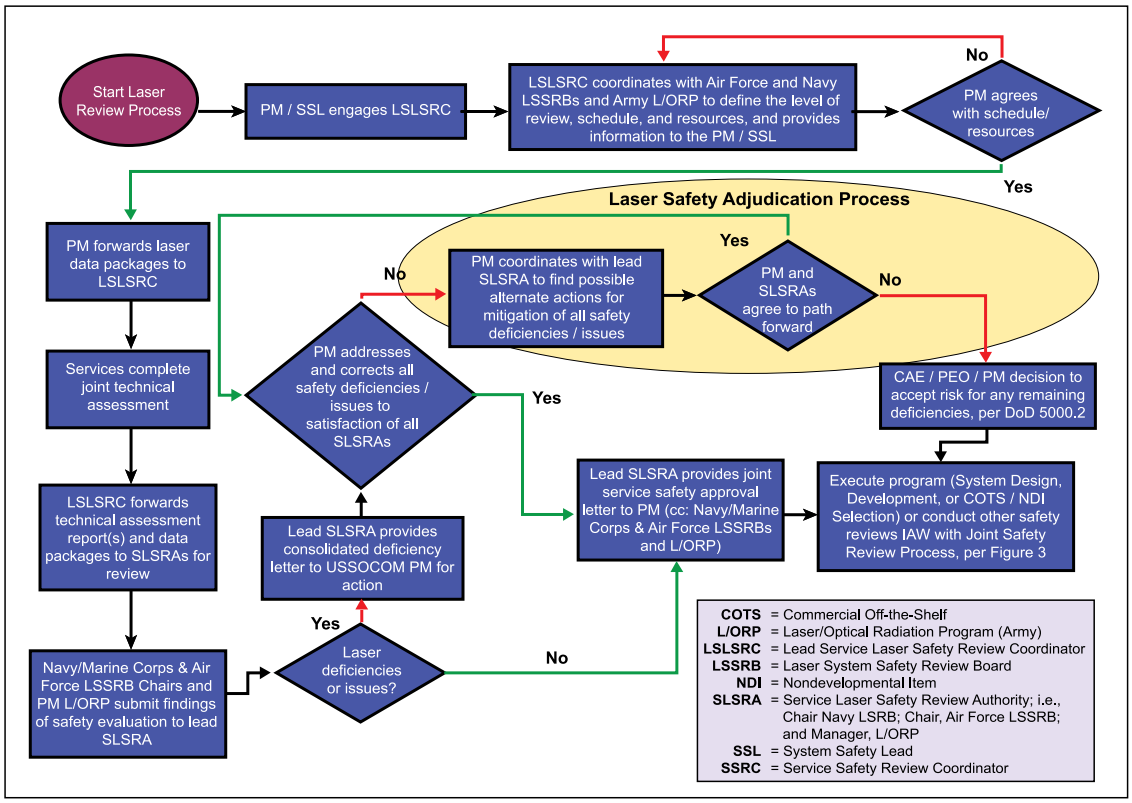


Figure 4. Joint Laser Safety Review Process

The SLSRC is the point of contact identified by a service to be the initial lead for coordinating the review of a laser system. The SLSRC can be from the Air Force Laser System Safety Review Board (LSSRB), the Navy Laser Safety Review Board (LSRB), or the U.S. Army Center for Health Promotion and Preventative Medicine (USACHPPM) Laser/Optical Radiation Program (L/ORP).

The service assigned the lead for the acquisition effort will provide the LSLSRC. The LSLSRC coordinates with the other SLSRCs and the SSL for:

- Laser safety TDP content
- Joint laser safety review of the TDP
- Conduct of the joint laser safety review, if required
- Drafting of letter and coordination of final signatures
- Monitoring closure of joint laser safety findings
- Drafting and coordination of signatures on final letter

For laser systems, if any service has identified a laser safety deficiency, this system cannot be approved for joint service use until all deficiencies are satisfactorily resolved by the PM and SLSRAs.

USSOCOM Joint Weapon Safety and Laser Safety Review Summary

The Office of the Secretary of Defense (OSD) joint weapon and laser safety guide, *Joint Systems Safety Review Guide for USSOCOM Programs*, Version 1.1, dated 12 October 2007, provides contact information for SSRCs and SLSRCs, along with guidance on review criteria expectations for TDP submissions in support of weapon and laser safety reviews. The Service Acquisition Executives signed the Memorandum of Agreement implementing the USSOCOM Joint Weapon Safety and Laser Safety Review Processes in October 2007. More than 15 acquisition programs are presently in, or have completed, the USSOCOM Joint Weapon Safety and Laser Safety Review Process as part of their validation. While no cost or time-savings metrics have been compiled to date, anecdotal data indicates significant savings are being realized for USSOCOM programs via this process.

Department of Defense (DoD) Joint Service Weapon and Laser Safety Review Process

The DSOC ATP TF tasked the JWSWG to expand the USSOCOM joint weapon and laser safety review processes to include all DoD joint weapon and laser system acquisitions and fielding decisions. The JWSWG is using the same collaborative approach as that used for the USSOCOM Joint Safety Review Process. The DoD Joint Weapon and Laser Safety Review Process consists of the same seven main elements as the USSOCOM process; therefore, the process charts in Figures 3 and 4 still

apply. Also, the weapon and laser safety process participant (i.e., SSL, SSRC, SLSRC, etc.) descriptions and responsibilities still apply. The JWSWG is developing a new DoD Instruction implementing the *Joint Service Weapon Safety Review (JSWSR) Guide* that will closely resemble the *Joint Systems Safety Review Guide for USSOCOM Programs*.

The JSWSR process is facilitated by a joint meeting of the service's safety review authorities or Army's designated Chief of Safety/System Safety. Such joint meetings are referred to as a "meeting of the Joint Boards" or "Joint Boards" and are co-chaired by the Chairpersons or Vice Chairpersons from the service boards in attendance and by the Chief of Safety from the appropriate Army major command. The Chairperson or Chief of Safety from the service that is lead for the weapon acquisition effort hosts meetings of the Joint Boards.

A written statement by the Joint Boards verifying that the weapon or laser system provides adequate design safety and meets each service's safety requirements will constitute a ***Joint Weapon Safety Certification***. If the weapon system fails to meet any of the services' safety requirements, the statement will verify that the weapon system PM has accurately identified the risk of this noncompliance or has accepted the risk at the appropriate level, per DoDI 5000.2, *Operation of the Defense Acquisition System*. The JSWSR process has been validated on numerous occasions, including twice for the joint Mine Resistant Ambush Protected (MRAP) Vehicle Program.

Summary

In the past, there has been no single, joint service safety review board or authority for USSOCOM programs that are joint by nature. Weapon system and laser safety releases, approvals, or certifications were required from each of the unique service safety review boards, with the potential programmatic downside of added expense, redundancy, schedule slippage, and conflicting safety requirements or actions.

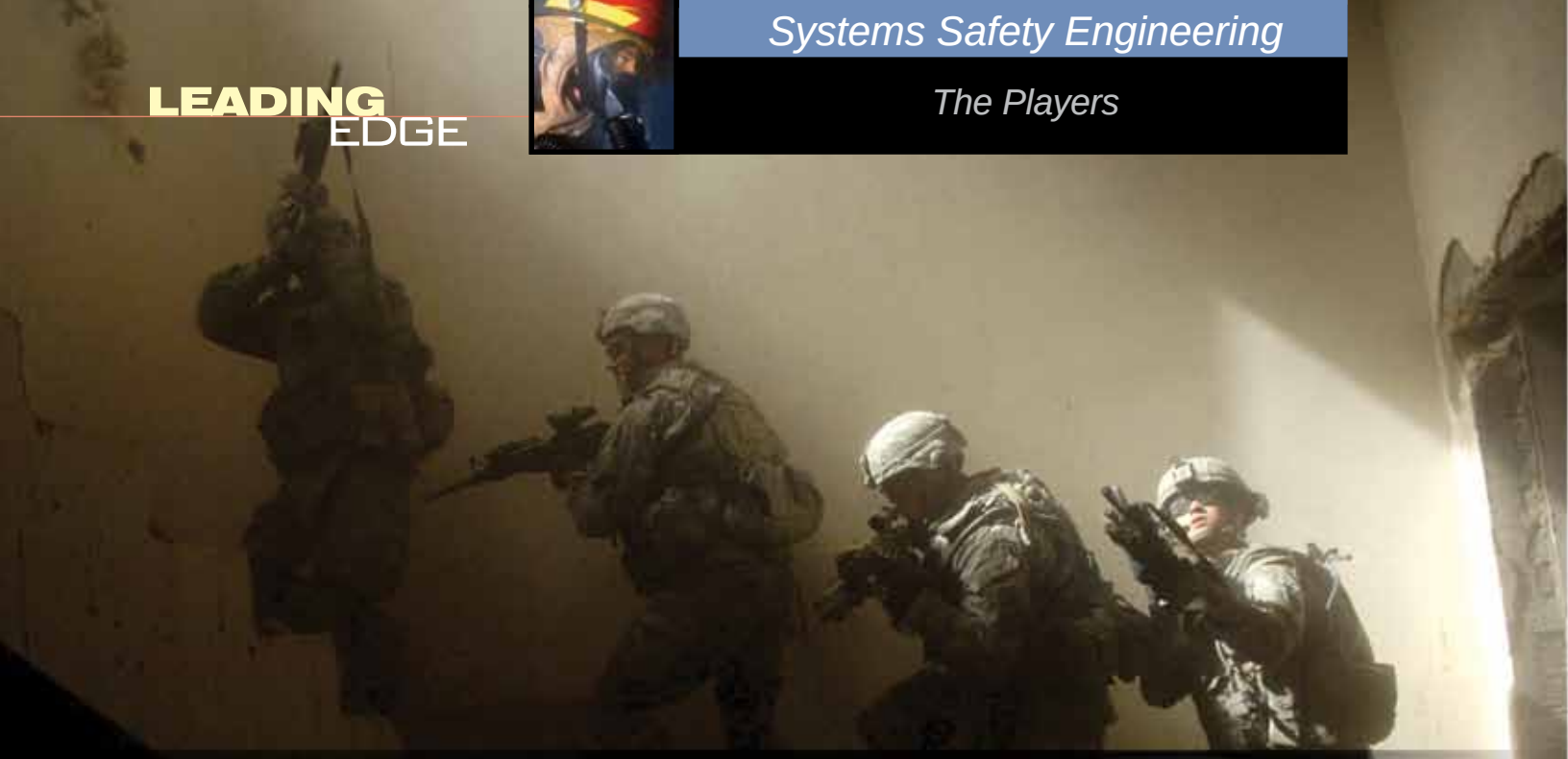
The joint weapon and laser safety review processes in support of USSOCOM are now finalized and documented in an OSD guide titled, *Joint Systems Safety Review Guide for USSOCOM Programs*, Version 1.1, dated 12 October 2007. More than 15 acquisition programs are presently in, or have completed, the USSOCOM Joint Weapon Safety and Laser Safety Review Process.

The DoD Joint Weapon and Laser Safety Review process consists of the same seven main elements as the USSOCOM process but will apply to non-USSOCOM Joint programs. A new DoD instruction implementing the JSWSR Guide that will closely resemble the *Joint Systems Safety Review Guide for USSOCOM Programs* is currently being developed and validated.

Bibliography

Demmick, Michael H., *Integrated System Safety Across the DoD Services: Why, When, & How; a.k.a. Joint Service Weapon Safety Review Process*, Naval Ordnance Safety and Security Activity (NOSSA).

Kratovil, Edward W., SAIC, 25 June 2008.



United States Special Operations Command System Safety

By Cathi Crabtree

Introduction

Acquisition system safety for United States Special Operations Command (USSOCOM) is the practice of controlling system and technical hazards throughout the system life cycle. Through the process of first identifying and then mitigating or eliminating hazards early in the system design process, the overall system performance can be optimized. This practice is one of the key elements of the systems engineering discipline and methodology. It integrates hazard identification with the associated hazard management and mitigation for the system within the constraints of the program. The objective is to design out risks early in the acquisition process so that an item or system, by virtue of its design or safety-specific design features, prevents or minimizes safety-related problems throughout its life cycle.

This general description should sound pretty familiar to most who deal with system safety. Where USSOCOM begins to diverge from much of the Department of Defense can be summed up in the following statement:

> Special Operations-peculiar systems shall always be designed and evaluated for safety of use, handling, storage, and transportation in the ***joint warfighting environment***.

Because Special Operations Forces (SOF) comprise components from each service, work side-by-side with regular forces from each service, and have their gear transported by elements of each service, it is essential that their weapons, munitions, and lasers meet the safety requirements of all services.

Background

In October 2007, the USSOCOM Acquisition Executive designated all USSOCOM acquisition programs as joint use, and the Department of Defense established the Joint Systems Safety Review Process for USSOCOM programs. This process was developed to prevent the consecutive processing of USSOCOM weapons, munitions, and lasers through the various services' safety processes; instead, the processes start at once so they can concurrently proceed; see Figure 1.

Key to the success of this joint review is the involvement of the Service Safety Review Coordinators (SSRCs), the gatekeepers to each service's system safety process. These SSRCs (one per service) collaborate throughout the concurrent review process to ensure that the program manager (PM) and the System Safety Lead do not become disparate and to avoid the possibility of conflicting guidance on their system safety program.

Numerous weapons, munitions, and laser systems are working through the joint process, and there have been challenges. However, new insight is being gained daily, and the process is working more smoothly and more quickly than at its implementation.

Way Ahead

Now that the process has been in existence for approximately 2 years, lessons learned are being reviewed, and input is being gathered from the various stakeholders including, but not limited to, the logistics community, the safety community, the technology and engineering (T&E) community, and the PM community.

The complete Joint Systems Safety Review Guide for USSOCOM programs and the Memorandum of Agreement implementing it can be found at the Acquisition and Technology Programs Task Force (ATP TF) Web site at http://www.acq.osd.mil/atptf/

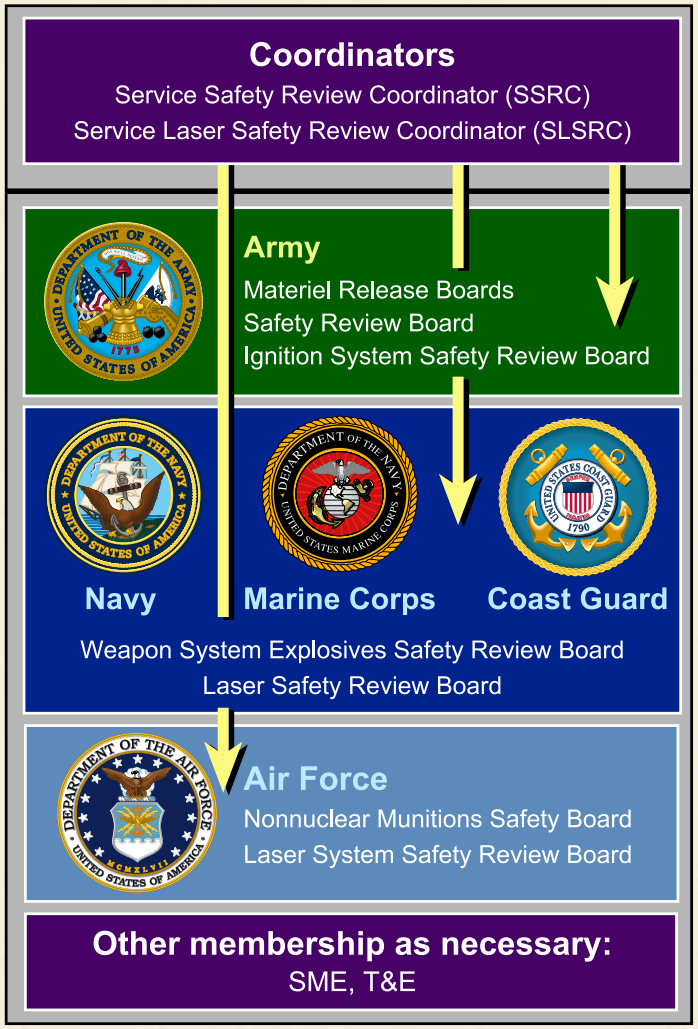
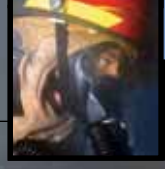


Figure 1. Joint Service Coordination



Explosive Ordnance Safety

By Bill Hammer

Introduction

The term ***ordnance*** is defined as military materiel, including combat weapons of all kinds, with ammunition and explosives (A&E), and equipment required for their use. Ordnance includes all the things that make up a ship's or aircraft's armament; i.e., guns, A&E, and all equipment needed to control, operate, and support the weapons. This article discusses the necessity and methodology for performing safety analysis to ensure that the explosive components in the ordnance we provide to the warfighter fulfills their intended purpose, while maintaining a margin of safety for the users and noncombatants.

It is the nature of weapons that they are inherently dangerous. They are, after all, designed to destroy personnel, equipment, and infrastructure. Central to this purpose is the presence of an energetic component, for which safety must be a primary consideration. While not all weapon systems contain explosives, such as electromagnetic or directed energy-based systems, most modern weapons still contain some explosive element either in a warhead, a propulsion system, or both. While the former are still dangerous systems for which safety review is necessary, it is to the latter—and specifically, to the explosive component therein—that our attention is directed in this discussion.

The weapons discussed above that contain explosives are part of a larger system that combines the mechanical, electrical, and computational components to effectively launch the weapon safely, in the right direction, and at the right time. Regardless of whether the weapon is employed from land, ship, or aircraft, it must be noted that safety of explosives is typically only part of the overall safety effort, and that issues regarding safe employment are bigger than the safety issues of just the explosive components. A complete and effective system safety program is essential to protect Navy and Marine Corps assets, and to maintain a warfighting capability. Note that a "system" in this context can vary from a Sailor manning a 25mm gun providing force protection, to the automated Aegis system with sensors to monitor positions of ships and aircraft, computers to track and identify targets, missile launchers and gun systems to engage targets, and personnel to operate the whole system.

Why is Ordnance Dangerous?

The successful use of most munitions depends on the controlled and predictable release of stored chemical energy. Substances and mixtures of substances that are employed for their energetic properties can be found in the explosives in warheads, propellants, and a variety of devices that use propellants or pyrotechnic materials to generate gas, heat, light, or smoke. The rate at which the energy is released in the chemical reactions that are characteristic of the material and the nature of the products that are generated in the reactions determine the applications for which any given energetic material will be suitable.

Although the overriding concern in the selection of an energetic material is whether it will perform adequately for the application of interest, the underlying question of safety is always present and needs to be factored into the decision-making process. The history of explosives use has demonstrated repeatedly that mishaps can and do happen, and that the consequences of accidents involving explosives can be catastrophic. Therefore, the characterization of an energetic material for military use must involve not only a determination of its energy output under the conditions of intended use but also its response to unplanned stimuli. The regulations governing the qualification of explosives for military use prescribe tests that determine the sensitivity of energetic materials to such stimuli as impact, friction, electrostatic discharge, shock, and heat. These tests are intended to simulate the hazards to which an explosive might be exposed during storage, transportation, and handling, as well as during hostile action. Additionally, recent developments in warheads technology are now presenting scenarios in which explosives must survive very harsh environments in the normal course of their functioning. The best known case of this type is probably hard target penetration, wherein the explosive must survive the stress of penetrating a hardened target and still be able to function on demand in the interior of the target.

Nature of Energetics

Explosives safety is the element of system safety practiced to prevent premature, unintentional, or unauthorized initiation of explosives and devices containing explosives, and to minimize the effects of explosions, combustion, toxicity, and any other deleterious effects. Explosives safety includes all mechanical, chemical, biological, electrical, and environmental hazards associated with explosives or electromagnetic environmental effects. Equipment, systems, or procedures and processes whose malfunction would cause unacceptable mishap

risk to manufacturing, handling, transportation, maintenance, storage, testing, delivery, or disposal of explosives are also included.

Explosives Safety Program Goals

All acquisition programs that include or support A&E items must comply with the Department of Defense (DoD) explosives safety requirements. The program manager (PM) for a Navy or Marine Corps system is responsible for implementing a safety program that covers all aspects of explosives safety and meets all Department of the Navy (DON) explosives safety policies and requirements, as well as federal, state, and local regulations. The PM is responsible for design requirements, management, engineering, and hazard controls for conventional A&E, and conventional components of nonnuclear weapons systems, such as warheads, rocket motors, separation charges, igniters, and initiators. A complete explosives safety program for A&E items requires an integrated effort involving several different disciplines, as well as application of independent oversight. For the Navy, this oversight is provided by the Weapon System Explosives Safety Review Board (WSESRB) and the Naval Ordnance Safety and Security Activity (NOSSA).

As a minimum, an explosives safety program should provide for identifying and assessing hazards inherent to the explosive item and operations associated with it. To that end, the program should focus on the following:

- Assurance of compliance with all explosives policies, procedures, standards, regulations, and laws
- Assessment of system designs incorporating explosives for hazards and mishap risk
- Application of design mitigation measures to reduce mishap risk to an acceptable level
- Review of the design and design mishap risk by appropriate safety review boards
- Documentation, communication, and acceptance of residual system mishap risks
- Establishment of Explosives Safety Quantity-Distance (ESQD) requirements for storage of A&E
- Facility site approvals for storage of A&E
- Explosives hazard classifications for transportation of A&E
- A Hazards of Electromagnetic Radiation to Ordnance (HERO) program
- An Insensitive Munitions (IM) assessment and test program
- A fuze safety program to ensure compliance with fuze design guidelines and standards

Typical Explosive Ordnance Safety Program

An explosive ordnance safety program follows a prevention-focused process based on:

- Reducing the probability of an explosives mishap from occurring
- Reducing the consequences of an explosives mishap, should it occur
- Continually informing and educating personnel on explosives mishap risks

There are many elements to an explosive ordnance safety program. Explosives safety is a joint effort involving many disciplines, such as weapon design, fuze design, explosives design, testing, IM safety, environmental safety, and system safety. For this reason, it is difficult to explicitly identify all tasks related to an explosives safety effort.

Appropriate MIL-STD-882 Hazard Analyses

Many contracts for development of a weapon system within the Navy or Marine Corps have only vague discussion of the need and extent of a system safety program. Often, they specify that the program initiate a system safety program in accordance with MIL-STD-882, with no other guidance. Although there may sometimes be references to some specific area of the discipline, such as electrical safety requirements or human factors considerations, the rigor of the system safety program is often left up to the system design agent (DA). DAs have a responsibility to develop a safe system but have no responsibility to deliver documentation of this safety program to the government unless required under the contract. Without this documentation and frequent interaction with the contractor during conduct of the system safety program, the government program office and the WSESRB have no basis for judging the overall safety of the weapon system. If we can assume that the proper level of documentation of the system safety program has been requested in the weapon system development contract, what then constitutes a good systems safety program for a Navy or Marine Corps weapon system?

A variety of sources discuss the nature of a system safety program: Naval Sea Systems Command (NAVSEA) SW020-AH-SAF-010, *Weapon System Safety Guidelines Handbook* (Formerly OD 44942); MIL-STD-882D, *Standard Practice for System Safety*; and the *System Safety Society Handbook* are some examples that speak in terms of six basic system safety hazard analyses that should be performed for every program. These are:

1. Preliminary Hazard List (PHL)
2. Preliminary Hazard Analysis (PHA)
3. Safety Requirements/Criteria Analysis (SR/CA)
4. Subsystem Hazard Analysis (SSHA)
5. System Hazard Analysis (SHA)
6. Operating and Support Hazard Analysis (O&SHA)

When safety is involved from the beginning of a program, each of these analyses provides specific benefits. However it's sometimes the case that safety becomes involved later in the program. In these instances, the safety engineer must make value judgments on the utility of the various analyses, depending on the extent to which he/she feels the design can reasonably be affected should a safety risk be identified. If the design has been frozen, it makes sense to tailor the safety effort to focus efforts on identifying hazards for which mitigations that do not entail design changes are appropriate. In the performance of these analyses, it is also important to note that a number of other hazard analysis tools are available to the safety engineer to aid in discovery and development of hazards. A Fault Tree Analysis (FTA) is often used to validate the likelihood of a hazard identified by an SSHA or an SHA. A Failure Mode, Effects, and Criticality Analysis (FMECA) is often used for similar purposes. Other analyses—such as Bent Pin, Barrier, and Common Cause Analyses—can be used to examine very specific causes of a given hazard and will augment the basic analyses listed.

The MIL-STD-882 analysis sequence is designed to provide the safety engineer with a structured approach to discovering, documenting, and developing mitigations for the hazards inherent in a system. However, when focusing on the explosive component of the system, special consideration must be given to evaluating the characteristics of the energetic materials themselves. For this reason, a number of explosives-specific tests, analyses, and reviews are necessary in an explosives safety study. These studies complement the MIL-STD-882 sequence and aid the safety engineer in developing the data specific to explosives hazards. This list includes, but is not limited to, the following:

- Energetic Qualification
- Programmatic Environment, Safety, and Health Evaluation (PESHE)
- IM and Hazard Classification Testing
- Electromagnetic and Electrical Testing
- Packaging and Replenishment
- Explosive Ordnance Disposal
- Firefighting
- Quality Evaluation
- Demilitarization and Disposal

Energetic Qualification

To a large extent, explosives and other energetics are not interchangeable in their uses. For example, a good booster explosive is likely to be too sensitive to be used as a main charge explosive, whereas a main charge explosive would likely not function when struck by a stab detonator in a fuze. To preserve both safety and performance, each type of explosive must be used in an application for which it is capable. This involves a qualification program to evaluate the properties of each explosive and verify that it is useable and safe for its stated purpose. Qualification is a two-step process. First, an explosive is "qualified" to perform an explosive function—such as primary explosive, booster explosive, propellant, etc.—based on the results of a series of tests of the raw explosive. Second, once an explosive has been qualified for a function, it can be utilized for that function in a specific application and tested in that design to become qualified in that application, known as Final (Type) Qualification. NOSSA, Code N8 maintains the list of all Qualified and Final (Type) Qualified explosives in the Navy and is the point of contact for establishing these qualifications.

Programmatic Environment, Safety, and Health Evaluation (PESHE)

Significant environmental issues often arise during the development, production, and test of a new weapon or system. The use of hazardous materials and the desired minimization of these materials, environmental impacts of storage or testing, and effects on endangered species or marine mammals all have to be addressed by the program. This is usually captured in the PESHE.

Noise, toxicity, and other health issues that potentially could be induced by a program are of interest, as is compliance with the National Environmental Protection Act (NEPA), environmental impact and assessments, and other pertinent laws and executive orders. The PESHE is a living document, usually started early in a program and updated periodically to support specific program milestones. Its final version should be sufficiently detailed to support a request for fielding of an explosive ordnance item. When conducting a safety assessment of an explosive item, the safety engineer should ensure a basic relationship with their local environmental experts.

Insensitive Munitions and Hazard Classification Testing

Key to any explosive's safety is how the explosive responds to potentially hazardous external stimuli. Insensitive munitions and hazard classification testing are utilized to characterize the response of munitions to stimuli such as heat, flame, and external object impact, as well as their response to the functioning of other ordnance in close proximity, known as sympathetic reaction. The results of this testing aid the safety engineer in determining necessary mitigations for exposure to hazardous external stimuli throughout the life cycle of the explosive item. NOSSA N8 also manages the Navy IM program. All issues related to the choice and qualification of explosives must be coordinated with NOSSA N8 in accordance with the appropriate series of NAVSEA Instructions (NAVSEAINSTs):

- 8020.3—*Department of Defense Explosive Hazard Classification Procedures*
- 8020.5, *Qualification and Final (Type) Qualification Procedures for Navy Explosives (High Explosives, Propellants, Pyrotechnics, and Blasting Agents)*
- 8020.8—*Department of Defense Ammunition and Explosives Hazard Classification Procedures*
- 8010.5—*Navy Weapon System Safety*

Electromagnetic and Electrical Testing

Modern shipboard and battlefield environments are alive with unseen electromagnetic energy. The numerous radars and communications devices aboard ship and in the field can couple with ordnance items and control systems, inducing voltage and current in firing and control circuits that can create hazards described as HERO. In addition, proximity to potential electrostatic discharge may induce similar hazards. Design techniques must be considered to minimize the effects of these environments. Testing and analysis is necessary to determine the vulnerability of an explosive item and to demonstrate the degree of effectiveness of design mitigations in mitigating potential hazards. In the case where safety from these effects is not designed into the system, this testing helps the safety engineer to determine procedural mitigations for protecting ordnance from these invisible threats.

Packaging and Replenishment

The sensitivity of explosive materials and the ability to restrict the potential impact of external stimuli during transportation and storage is a vital element for consideration in an explosives safety analysis. For this reason, how the item is packaged for the various logistical phases of its life cycle is paramount to safety. The Department of Transportation (DOT) manages the certification of packages intended to pack weapons and other ordnance. DOT has delegated this authority to the services for their individual items. The Naval Packaging, Handling, Support, and Transportation (PHS&T) Center at the Naval Weapons Station, Earle, New Jersey, is the Navy's center of expertise for all PHS&T issues. Certification of a package involves a discrete series of tests to demonstrate the survivability of the package under real-life conditions and the ability of a package to withstand these conditions. The PHS&T Center can design and certify a package or can examine developed packaging and test to verify it meets DOT standards.

Explosive Ordnance Disposal

One of the more important configurations for packaging is the development of the fleet issue unit load (FIUL). This describes how smaller boxes are arranged on a standard pallet, such that the pallet of ordnance can be transferred from ship to ship during connected replenishment (CONREP) or by helicopter during vertical replenishment (VERTREP). Certifying a FIUL for CONREP involves passing the original packaging tests, as well as

demonstrating compliance to HERO and electrostatic discharge (25 kV) requirements. Certifying a FIUL for VERTREP involves an extra step managed by the U.S. Army.

The desire to protect not just friendly forces but also noncombatants is a high priority in modern ordnance development. Thus, the ability to "sterilize" the area after testing or hostilities in order to protect the innocent is a driving force behind the attention paid to unexploded explosive ordnance (UXO). All explosive ordnance items entering the Navy or Marine Corps inventory are required to have validated procedures for rendering them safe by an explosive ordnance disposal (EOD) team. Items under development or in use may experience malfunctions, leaving behind UXO that must be rendered safe by a trained EOD team. Testing of ordnance items is necessary for the development of the procedures and data required by the EOD team in order for them to maintain the knowledge and information on any item being stored, handled, tested, or used, so that they can safely manage these malfunctioned items.

Firefighting

The addition of any new explosive item to existing inventory mandates a review of firefighting procedures. New energetic mixes in weapons being developed may contain materials that, when ignited, are not responsive to existing firefighting methods. Shipboard firefighting capabilities are usually considered outside of the purview of the safety community except when the addition of a new weapon system or a change in an existing system adversely affects the existing firefighting system. New explosive items may require the development of new fire-suppression methodologies. While the approval of those methodologies is the responsibility of a dedicated office in NAVSEA, Code 05P4, that office will often ask the safety engineer and the WSESRB for inputs on the overall effects of safety to the system and the ship, as these issues are considerations in the hazard analysis performed on the item.

Quality Evaluation

Ordnance safety in the fleet depends both on the initial safety and quality of a weapon when it enters the fleet and its retained quality after experiencing the rigors of fleet use and stowage. Age and exposure to various environmental factors—such as heat, cold, and humidity—may contribute to destabilization of explosives over time. Development of a Quality Evaluation Plan for ordnance is essential to ensuring that explosives maintain safe characteristics over the lifetime of their service use. All weapon programs are required to establish a quality evaluation program to monitor the quality of a weapon as it ages in the fleet. NOSSA N8 oversees this process for the Navy and aids by maintaining controlled samples of all propellants used in the fleet and schedules for periodic re-examination of other ordnance items.

Demilitarization and Disposal

As with any production item, the likelihood is that not all ordnance produced will be needed. At some point, an explosive item must be disposed of when using it is no longer safe or productive. Each program is required to have a plan to demilitarize or dispose of all items safely at the end of their lifetime; requirements for disposal differ depending on the materials present in the item. Guidance for developing an appropriate plan for demilitarization and disposal may be found in NAVSEAINST 8027.2 (Series), *Demilitarization Disposal Requirements Relating to the Design of the New Modification of Ammunition Items.*

While this article presents a number of considerations in conducting a safety study on explosive ordnance items, it is not meant as a comprehensive primer in explosives safety. An explosive ordnance safety program comprises many elements—a number of analyses and extensive review and approval. While the process may be extensive and laborious, it is critical to ensure that weapons meet their design objectives and are safe in the hands of those who use them.

The Execution and Evolution of Combat System Safety

By Mike Zemore

Combat system (CS) safety is the practice of identifying safety risks in a system-of-systems (SoS) context. This article discusses the foundational elements of the Combat System Safety Program (CSSP) as derived collaboratively with the Program Executive Office for Integrated Warfare Systems (PEO IWS) Chief Engineer. It also discusses the role of the Combat System Principal for Safety (CS PFS), integration within the Naval Sea Systems Command (NAVSEA) battle group action teams and strike group teams, and the development of SoS safety analytical methodologies that preceded and influenced Navy policy. Focus is directed to the significance of the historical perspective of CS safety, definition of influential factors, collection of lessons learned, and the evolving methods to preserve the engineering value inherent in the SoS safety engineering approach for the Navy.

CS safety was initiated in 2001 and gained significant thrust in 2002, after the Weapon System Explosives Safety Review Board (WSESRB) exercised their authority to disapprove a Combat System Ship Qualification Test (CSSQT) event until an integrated CS safety analysis was completed.

Previously, system safety analyses and practices were applied to individual combat system elements (CSEs) and had been demonstrated to be effective in identifying hazards and mitigating mishap risk. However, the board recognized the trend in overall CS complexities and the reliance on integration of the many individual systems for mission success. That level of integration understandably drives new hazard considerations for safe operations. Specifically, the board wrote:

> The WSESRB believes that many safety issues associated with the interface of CS elements do not receive adequate identification or attention due to the lack of a comprehensive, integrated CS safety effort.

The WSESRB's CSSQT disapproval provided the primary impetus for a CS safety effort for USS *Nimitz* in 2002. However, the community had, in fact, already recognized the need for an integrated CS safety effort and was in the process of establishing the

A RIM-7P NATO Sea Sparrow Missile launches from Mount Four aboard the *Nimitz*-class aircraft carrier USS *Abraham Lincoln* (CVN 72) during a stream raid shoot exercise. *Lincoln*'s self-defense systems fired four Sea Sparrow missiles, engaging and destroying two BQM-74E turbojet-powered drone aircraft, and a High-Speed Maneuvering Surface Threat (HSMST) remote-controlled Rigid Hulled Inflatable Boat (RHIB) during the event. *Lincoln* and embarked Carrier Air Wing (CVW) 2 are underway off the coast of Southern California conducting Tailored Ship's Training Availability (TSTA).

U.S. Navy photo by Mass Communication Specialist 2nd Class M. Jeremie Yoder (RELEASED)

foundational elements for that evolution. By 2001, the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) had begun working with Program Executive Office for Expeditionary Warfare (PEO EXW) and PEO carriers to establish an overarching system safety role for aircraft carriers and amphibious assault ships. Focusing a safety effort at this level of integration was a tremendous opportunity to advance systems safety engineering methodologies and collaborative efforts to influence the CS safety posture to eliminate potential accidents. Also in 2001, NSWCDD was working with PEO ships to execute a CS safety effort for the new construction of the amphibious transport dock (LPD)-class ship. Thus, the integrated SoS safety methodologies and techniques were at that time in their formative stages, but had not gelled into a cohesive SoS safety engineering process.

The WSESRB disapproval, therefore, forced the established framework for CS safety to be fully developed and exercised in order to gain concurrence for USS *Nimitz* CSSQT and deployment. This action thrust the safety community and the CS safety role to new heights. Almost instantly, NAVSEA 06 and program offices aligned to address the WSESRB finding. USS *Nimitz* was a special case, in that the *Nimitz* Battle Group Action Team (NIMBGAT), previously established as a risk mitigation strategy, employed cross-organizational coordination to support successful deployment of USS *Nimitz*. At the time, the Deployment–30 months (D-30) certification process was applicable, and close coordination was required between the NIMBGAT and NAVSEA 06 as the certification activity. The NIMBGAT accepted the CS PFS as a team member and designated the CS PFS as the Safety Lead for USS *Nimitz*.

With the importance of USS *Nimitz* and its projected deployment timeline, NSWCDD worked directly with the PEO IWS (formerly known as the PEO for Theater Surface Combatants (TSC)) Chief Engineer, the NIMBGAT, the WSESRB, and the many stakeholders to establish and execute the CSSP. This was no ordinary safety effort given that most of the SoS safety methodologies needed definition and refinement to accomplish value-added safety analytical work. USS *Nimitz*, only weeks from a CSSQT and follow-on deployment, required detailed safety analyses performed on the integrated CS in order to support these important milestones. It was a daunting task, but it was also a great challenge and great opportunity for many dedicated individuals to serve this nation and our fleet. Beneficial to this endeavor was that the NIMBGAT was an extraordinary group. They were exceptional in their knowledge, leadership, planning and execution in preparing USS *Nimitz* for deployment. Likewise, the PEO

USS *Nimitz*
Integrated Combat System Capability

USS *Nimitz* Combat System provides:

- **State-of-the-Art Sensor Integration**
- **Quick Reaction Through Automation & Efficient Human / Machine Interface**
- **Coordination of Weapons**

IWS Chief Engineer, a Navy Captain, was exceptional as an innovator, motivator, and leader. The successful initiation and execution of the CSSP for USS *Nimitz* was due to the dedication of these individuals—and many others—to mission success.

The CS Safety approach was carefully crafted utilizing (MIL-STD) 882 series, *Standard Practice for System Safety*. The overall goal was to identify, communicate, and mitigate integration hazards not previously identified through individual CSE safety programs. The approach stressed engineering analyses of the integrated CS while assessing CSE analysis results for potential integration safety risks. The effort was unique given that hazards associated with the integration of multiple CSEs would likely:

- Have multiple CSEs with contributing hazard causal factors, or
- Have multiple CSEs contributing to hazard mitigation strategies, or
- Have multiple risk acceptance authorities providing residual risk acceptance

To ensure consistent development, documentation and execution of the CSSP, NSWCDD developed a Combat System Safety Management Plan. The plan captured the methodologies, techniques, roles, and responsibilities associated with establishing and executing the CSSP. PEO IWS, responsible for the majority of surface warfare CSEs, was the obvious owner of the document. The 2002 draft plan was disseminated throughout PEO IWS for review and disposition and subsequently updated to include lessons learned after the PEO IWS-initiated safety study on integrated training systems for surface ships.

Of particular emphasis in the CS safety approach was the application of analytical methods for hazard identification and detailed risk assessment. The methods included analysis of all possible failure-mode root causes associated with the following:

- Integration of human actions and interactions across numerous systems
- Implementation of CS safety-critical functions and system interactions
- Hardware failures and their impact on CS safety-critical functions and system integrations
- Software deficiencies and their impact on CS safety-critical functions and system integrations

To successfully execute the CS safety approach, the team had to define specific criteria to maintain focus on the safe integration of CSEs. Through the conduct of the Combat System Safety Working Group (CSSWG), the team defined CS-level safety-critical functions and initiated a trace of the safety functions to individual CSEs. The team

also identified CS-level hazards and initiated the assessment of CSEs for causal factor contributors. This led to the realization that safety "scrutiny" of individual CSEs could be guided by defining the terms ***safety critical*** and ***safety related***. Safety-critical CSEs were those that directly controlled weapons and needed the highest level of safety analysis rigor. Safety-related CSEs were those that provided data used in controlling weapons but performed no controlling functions. Safety-related CSEs typically required less safety analysis rigor.

Since the overall SoS effort hinged on successful collaboration with CSE safety leads, it was paramount that the safety analysis criteria and approach be well communicated to CSE Safety Leads in order to enlist their assistance. Collaborative sessions aided in determining CSE relevance to CS safety functions and in applying CSE safety analysis results to determine possible CS-level hazards. Although hazard identification and mitigation were primary goals, there were ancillary responsibilities for the CS PFS. The CS PFS would also:

- Provide safety leadership for the Combat System Safety Integrated Product Team (IPT) for Strike Groups/Action teams
- Provide a CS Safety point of contact (POC) with NAVSEA 06 concerning the safety of CS configurations certification
- Optimize safety costs through coordinated engineering efforts and the Software Systems Safety Technical Review Panel (SSSTRP)/ WSESRB CS reviews

Possibly the most vital aspect in conducting the CSSP was the collection of CSE safety engineering data. To facilitate this, the CS Safety Team initiated a series of "data calls" as a collaboration vehicle. The data calls targeted individual CSE Safety Leads as members of the CSSWG. Response to data calls was essential for conducting the first CS safety analysis—USS *Nimitz* CS Preliminary Hazard Analysis. The data calls were also instrumental in the follow-on analysis—USS *Nimitz* CS System Hazard Analysis. Significantly, tuning of this data call process also prepared the CS Safety Team for safety studies on upcoming CS configurations as the team refined the analytical capabilities and evolved the discipline.

The success of the data call process and collaborative sessions was largely attributable to the community having a focused goal on USS *Nimitz*, with support from the NIMBGAT. The data call process targeted three types of data for assessment at the CS level: future capabilities and functionality, safety and verification products, and known risks. Implementation of the data calls was collaborative in that the CS Safety Team would

"give" information during the call process and would "get" data from the CSE Safety Lead in return (see Figure 1).

The hazard identification and safety verification process also relied heavily on integrating the CS Safety Team into the development and integration testing process. Since integration hazards are not always identifiable through purely analytical studies, the team required requisite system performance knowledge best acquired through actual system operation. For safety verification, the integration test lab, combined with shipboard testing, provided the necessary venue for end-to-end verification of CS safety-critical functions and implemented hazard mitigations.

Although the CSSP was on track for USS *Nimitz*, it was an aggressive engineering venture, where the pending milestones for deployment provided little room for error. As a result, the team decided that a memorandum of agreement (MOA) was necessary to guide the formal review and certification process. The MOA outlined the approach and responsibilities to mitigate programmatic risk, understanding that this was the first ever surface ship CS WSESRB review with follow-on NAVSEA 06 warfare systems certification. The CS Safety Team drafted the MOA with responsible organizations including the WSESRB, NAVSEA 06, PEOs, and the CS PFS. The MOA was never signed as a formal agreement, but all parties acknowledged the content. That acknowledgment was effective in providing the necessary facilitation and coordination for USS *Nimitz* configuration during the formal review and certification process. The content of the draft MOA was later used in the development of the warfare certification instruction NAVSEAINST 9410.2, *Naval Warfare Systems Certification Policy*, and the update to WSESRB instruction NAVSEAINST 8020.6E, *Department of the Navy Weapon System Explosives Safety Review Board*. Each addresses CS safety requirements.

As discussed earlier, the CS safety analysis effort was no ordinary system safety effort, so no ordinary SSSTRP and WSESRB would suffice. The

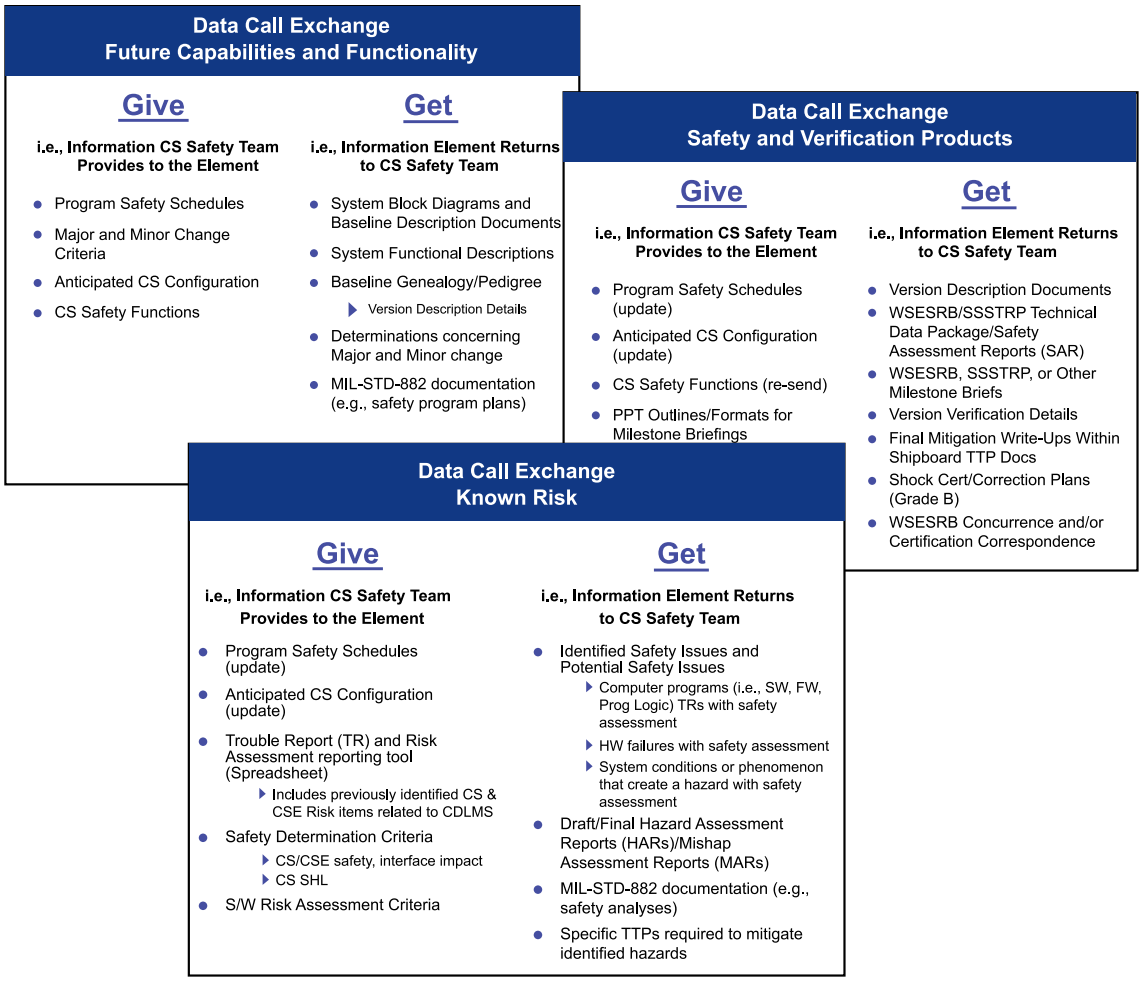


Figure 1. Combat System Safety Data Call Exchange

The aircraft carrier USS *Nimitz* (CVN 68), the guided-missile cruiser USS *Chosin* (CG 65), the guided-missile destroyers USS *Sampson* (DDG 102) and USS *Pinkney* (DDG 91), and the guided-missile frigate USS *Rentz* (FFG 46) operate in formation in the South China Sea. The Nimitz Carrier Strike Group is conducting operations in the U.S. 7th Fleet area of responsibility.

(U.S. Navy photo by Mass Communication Specialist 1st Class David Mercil/Released)

SSSTRP, held in November 2002, was a 2-day session, with detailed review of all software, software safety processes, software configurations, and risk. The CS PFS presented the CS mishap risk assessment methodology and analysis results, where causal factors were evaluated individually and collectively within the context of the integrated system. The review was deemed successful, and the panel concluded with its recommendations being provided to the WSESRB. The WSESRB review followed in December 2002. The importance of having a first-ever CS safety review that covered the integration of numerous CSEs within the context of integrated CS led the board to its first-ever Senior Level WSESRB that is now documented in NAVSEAINST 8020.6E. During the review, the characterization and quantification of mishap risk potential based on the analytical results was communicated within the context of a collective SoS. At the conclusion of the review, the WSESRB wrote in their findings:

> The WSESRB concurs that the process used adequately identifies USS *Nimitz* ship self-defense CS residual risk, and based on that process, the residual risk is at an acceptable level for deployment.

The culmination of USS *Nimitz*'s CS safety analysis and review process was significant in that it:

- Characterized risk for the entire CS
- Established the basis to mitigate risks as a distributed or shared responsibility
- Emphasized the need for integration of the CS Safety Team in all integration test events
- Laid the groundwork for the CS safety involvement in the definition and documentation of safety-related information provided to the ship

USS *Nimitz*'s CS safety effort established the precedent for conducting a CSSP. Although techniques and methods continue to evolve, the WSESRB and certification authorities continue to leverage the scope, methods, techniques, collaborative efforts, and communications defined during this effort as the baseline for integrated safety analyses and review.

Combat System Safety

By Kevin Stottlar

The practice of combat system (CS) safety engineering was established to address CS safety issues by focusing on integrated hazard methodology and integration hazards, which typically fall outside the bounds of individual combat system element (CSE) system safety program efforts. This article describes the processes and methodologies for conducting a CS safety program in an effort to identify and characterize CS integration hazards and provide engineering recommendations to eliminate or mitigate them to an acceptable level.

CSEs have historically been effective executing a system safety program on their system to identify and mitigate risks in the context of their system. When each of these CSEs is integrated to make up a CS however, existing CSE hazards may create a greater risk at the CS or system-of-systems (SoS) level, and/or new safety hazards may be introduced as a result of the integration. The practice of CS safety engineering was established to address these integration hazards. The processes and methodologies utilized to conduct a CS safety program are discussed in this article.

To begin, let us define CS and CSE as utilized in the context of this article:

Combat System (CS)—An integrated set of systems capable of accomplishing the plan, detect, control, and engage functions across all warfighting mission areas.

Combat System Element (**CSE)**—A weapon control system, weapon, or other system/component that is necessary for the completion of one or more of the ship's warfare missions. CSEs exchange information with other CSEs via a digital or analog interface.

CS safety can be broken down into three process phases, though the efforts within each process phase can be executed concurrent with efforts in another process phase:

1. CS safety planning and management
2. Hazard analysis and risk reduction
3. Hazard tracking and CS residual risk determination

CS Safety Planning and Management Process

Before executing a CS safety program, an understanding of the CSEs that make up the CS and determination of their level of criticality is required. CSE criticality determination is important, as this will assist in the prioritization of resources when planning and executing the CS safety program. NAVSEAINST 8020.6E, *Department of the Navy*

Weapon Systems Explosives Safety Review, provides the following definitions in assessing CSE criticality:

- **Safety-Critical CSE**—A CSE that directly or indirectly controls—or has the potential to control—ordnance, or provides information necessary to the safe selection, arming, release, firing, or jettisoning of an ordnance item with respect to a specific event (i.e., missile test firing or deployment).
- **Safety-Related CSE**—A CSE that interfaces to a safety-critical CSE, whose failure would result in the increased risk of an ordnance-related mishap. Determination is made based on engineering judgment utilizing the Combat System Safety Working Group (CSSWG) and the documented CS safety-critical functions and potential CS-related mishaps.

Figure 1 depicts these process phases and the tasks associated with each and will be discussed throughout the remainder of this article.

Execution of a CS safety program requires a vast array of knowledge and understanding of the CSEs making up the CS, and heavy reliance on the CSE safety programs sharing detailed information when hazards are identified as contributing to CS-level hazards. The CSSWG, with representation from each CSE Principal For Safety (PFS) or safety lead—along with representation from organizations associated with the system acquisition program—is the forum in which data sharing and collaborative assessment of technical safety issues occurs. Early establishment of the CSSWG is critical to the successful execution of a CS safety program.

The tool for planning, managing, and communicating when multiple safety efforts are occurring on a CS is called the System Safety Management Plan (SSMP). The SSMP establishes the foundational elements necessary for CSEs to develop their System Safety Program Plans (SSPPs) and provides a common framework in which individual CSEs can work together on a CS safety program while eliminating methodology issues, minimizing communication problems, and avoiding duplication of effort.

Given that engineering development efforts may span years, it is imperative that hazard data be tracked, maintained, and stored electronically

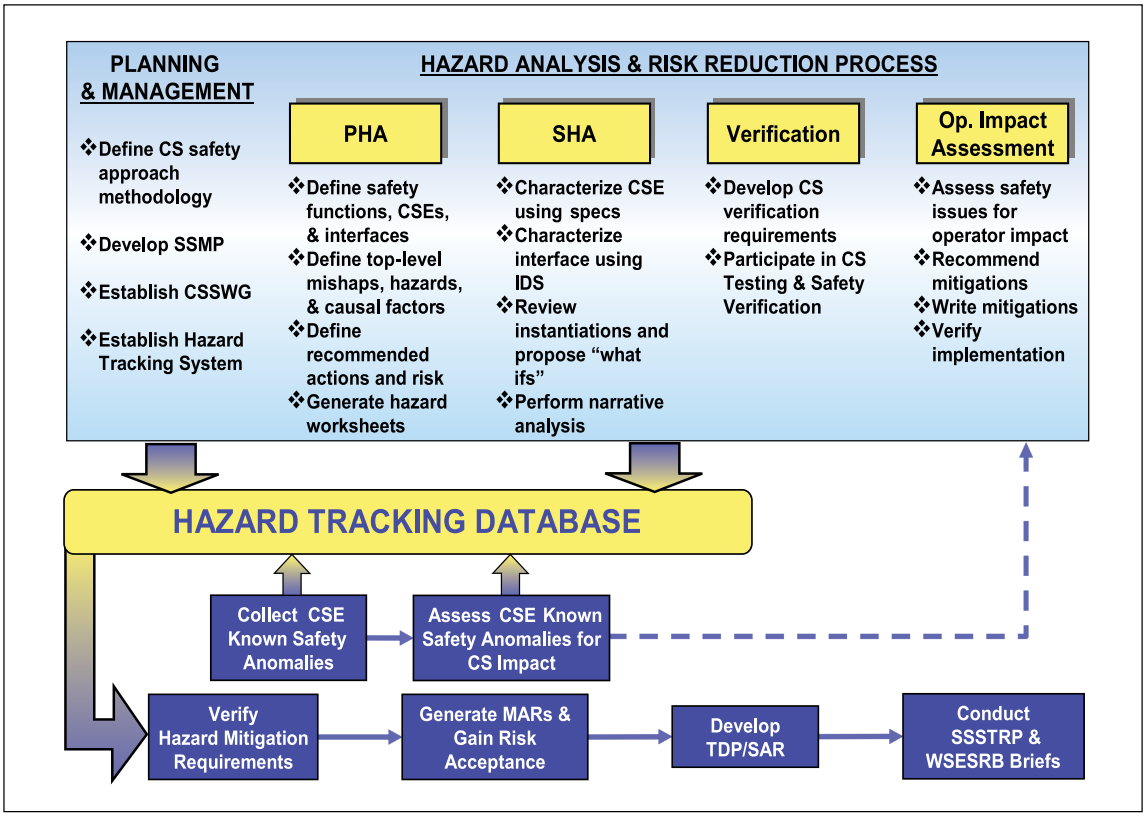


Figure 1. Combat System Safety Process

in a hazard tracking system. The hazard tracking system should be designed to accommodate at a minimum:

- A hazard description
- Any contributing or causal factors to the hazard, as well as the hazard's potential contribution to a mishap
- Mitigations and verification/validation status of mitigations
- Current status of all hazards and any actions assigned

A CS hazard tracking system must also account for real and potential CSE hazards, and an assessment of known CSE causal factors by the CS PFS for their contribution to CS mishaps. This is discussed in greater detail later in the article.

Establishment of a CSSWG, SSMP, and hazard tracking system establishes the foundation necessary to initiate the next CS safety process phase: the Hazard Analysis and Risk-Reduction Process Phase.

Hazard Analysis and Risk-Reduction Process

The Interface Requirements Specification (IRS), the Interface Design Specification (IDS), and CSE hazard analysis data are appropriate and necessary inputs to the CS Preliminary Hazard Analysis (PHA). As part of the CS PHA, safety functions are defined consistent with CS missions. The safety functions are then allocated to applicable CSEs based on the CSEs potential involvement in the safety function.

A PHA can be thought of as a rigorous analytical exercise in which top-level mishaps (TLMs), hazards, and causal factors are hypothesized, given the missions and capabilities of a system. The CS PHA is far more comprehensive, in that it considers TLMs, hazards, and causal factors in concert with CS missions and capabilities from an SoS approach involving all safety-related and safety-critical CSEs. A TLM is defined as an unwanted and unplanned event in which there is a release of energy that will have a detrimental effect on personnel, equipment, or the environment. This unplanned event is induced by one or more hazard, with hazards being understood to mean a real or potential condition that, if realized, could lead to a mishap. In other words, a hazard is a prerequisite to the occurrence of a mishap. Causal factors are elements within the system design, implementation, or operation that can lead to the realization of a hazard, and they fall into one of three categories: human or operator, hardware, and software. The CS PHA

then applies each TLM/hazard/causal factor relationship as instantiations to all applicable CSEs. The following example of a TLM/Hazard/Causal Factor instantiation relationship is provided to illustrate this concept:

For TLM ***Intercept of Friendly/Nonhostile***, one potential hazard that could lead to this mishap would be ***failure/inability to terminate or suspend engagement***. A causal factor that could result in this potential hazard being realized would be ***failure of system to process termination or suspension orders***, which may have a number of instantiations, or CSEs that it may be applicable to. Figure 2 is a generic graphical representation of this concept.

At the conclusion of a CS PHA, there is likely to be an enormous number of hazards, causal factors, and instantiations that will provide the foundation for the start of the CS System Hazard Analysis (SHA). The results of the CS PHA are the foundation for initiation of the CS SHA. The focus of the CS SHA is to:

- Fully analyze and characterize the risk associated with the hazards and causal factors identified in the CS PHA
- Identify previously unidentified hazards associated with CSE interfaces
- Identify existing mitigations for CS hazards and causal factors
- Recommend actions necessary to either eliminate identified CS hazards or identify mitigation strategies to control their risk to an acceptable level

To ensure that appropriate safety analysis rigor and focus is applied to the CS SHA, CSEs and CS interfaces must be characterized. Characterization of CSEs should be done in the context of CS safety functionality. Some key focus areas to identify in characterizing CSEs include: weapons, ordnance and other energy sources, CSEs dependent upon data or information from another CSE to execute CS safety functionality, modes of operation, and safety functions requiring operator involvement. Characterization of CSE interfaces should focus on some key areas involving critical data flow, including timing and other controls to ensure delivery and processing, data integrity, communication protocols, and interface recovery processing. Adequacy of IDS should also be factored into this analytical assessment.

Characterization of CSEs and their interfaces allows for a more targeted approach in performing interface analysis as part of the CS SHA. Those

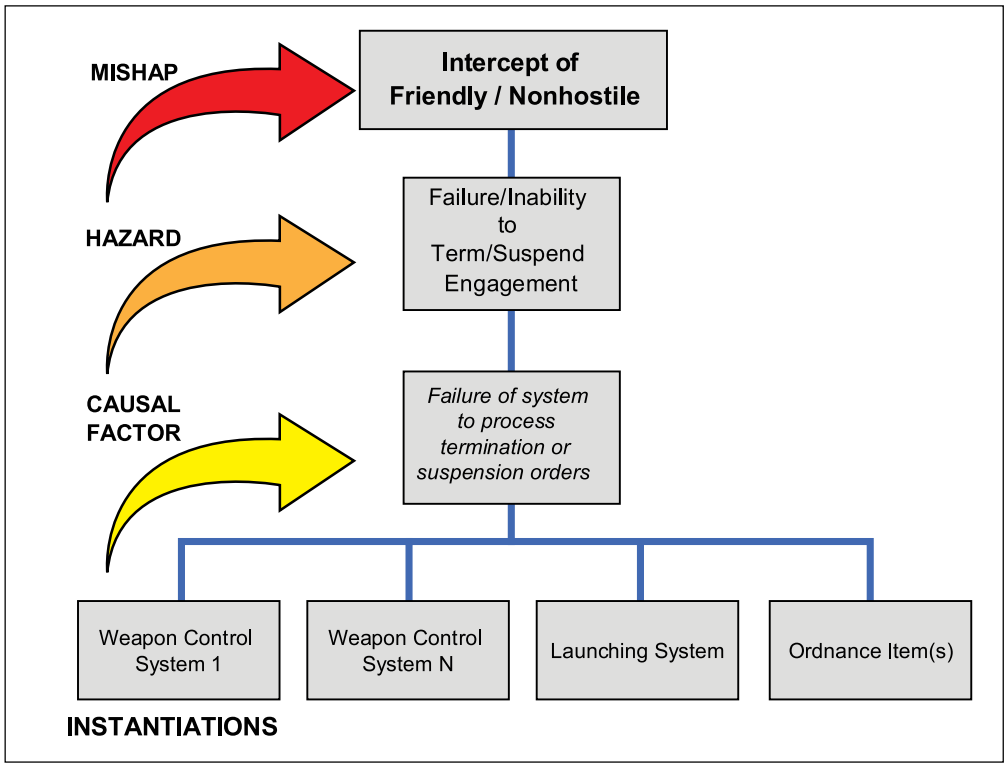


Figure 2. Concept Diagram of System Hazard Analysis

CSEs and CSE interfaces with the most severe potential for a safety mishap should receive the most attention with respect to safety analysis and testing. Potential root causes from all causal factor categories must be considered in this process, including:

- Human actions and interactions involved with integrating multiple operators across multiple CSEs
- Hardware and software failures
- Design defects and their impacts on CS safety functions

Utilizing the instantiations from the CS PHA—uncertainties due to immature design, new CS capabilities or functionality, potential failure conditions, and potential data errors—a series of safety scenarios can be constructed. These safety scenarios can be thought of as "what-if" constructs and are intended to focus safety analysis and testing efforts. Some areas for consideration include:

- Failure of safety interlocks
- Mode mismatches
- Safety data verification errors
- Timing errors involving safety-critical data transfer across CSE interfaces

For each hazard and causal factor identified during the conduct of the CS SHA or carried forward from the CS PHA, existing safety mitigations should be identified and captured in the CS Hazard Tracking Database (CS HTDB). An assessment as to the comprehensiveness of the mitigation should also be made. For those hazards or causal factors deemed insufficiently mitigated, actions necessary to either eliminate the identified CS hazards or identify mitigation strategies to control their risk to an acceptable level should be documented in the CS SHA and captured in the CS HTDB. Additionally, adequacy of the design mitigations relative to CS safety concerns captured in the "what-if" safety constructs should be determined by assessing appropriate IDS, assessing CSE safety hazard analysis artifacts, and/or collaboration with the appropriate CSE safety team or CSE system engineers.

Verification and validation of hazard and causal factor mitigations designed into the CS can be accomplished via interface analysis as the design continues to mature, via system integration testing, or a combination of the two. Integrating CS safety engineers into the developmental and testing processes with an emphasis on CS integration testing is vital in understanding and assessing implementation of safety mitigations to eliminate or reduce CS safety risk. The CS safety team should be directly involved by providing system safety testing input to ensure that appropriate levels of safety function testing are accomplished. The CS safety team's involvement during the conduct of safety testing to ensure full insight and understanding of any test anomalies that occur during system integration testing is important in providing an assessment of risk.

Even after thoroughly analyzing and testing CS interfaces, making risk mitigation recommendations, and verifying and validating the mitigations, at the end of the day there will be residual safety issues that cannot be eliminated or that still require additional procedural workarounds to ensure safety of personnel, equipment, and the environment. The CS safety team must provide an operational impact assessment of these procedural workarounds to ensure that they, in fact, effectively mitigate the risk without introducing additional safety issues or creating a burden for any particular operator. Commonly referred to as tactics, techniques, and procedures (TTP), these workarounds are not the best option for providing mitigation to a known safety risk, but often this is the only option left. Because TTP workarounds are employed by

humans, it becomes imperative that they are written in clear and unambiguous language, and can be easily invoked by the operator when required.

Hazard Tracking and CS Residual Risk Determination

The CS safety program HTDB is populated with hazard data and is continually updated throughout the life of the CS safety program. The HTDB contains data from CS safety analysis and testing efforts but also contains pertinent hazard and causal factor data from CSEs. This is important, as one of the principles of CS safety is an assessment of overall CS mishap risk. This mishap risk assessment comprises hazard analysis by the CS safety team in conjunction with hazard analysis by each CSE safety program for their respective CSE. Potential interface hazards and causal factors are assessed by the CS safety team using the methodologies discussed in this article. In addition to CS and CSE hazard analysis, CSE software causal factors must also be assessed for potential contribution to CS mishap risk. Software causal factors are actual CSE design deficiencies that can lead to the realization of a CSE hazard, which could culminate in a mishap. If the CSE hazard has relevance to a CS safety function, then the CSE software causal factor likely has relevance, and its contribution must be considered when determining CS mishap risk.

In order for a CSE to make an informed determination that their software causal factors may have CS implications, the CS safety program provides the CSEs with CS safety functions, hazards, and causal factors as criteria. CSEs use the criteria to determine hazard and software causal factor applicability in response to CS safety "data calls." Each CSE hazard and software causal factor is assessed to determine and characterize their potential CS mishap risk contribution. For CSE software causal factors, the CS safety team assesses each risk using the criteria in Table 1. Each CS causal factor mishap risk assessment must stand on its own in defining the potential that the particular causal factor could lead to the mishap. Each CS causal factor mishap risk assessment is discussed and arbitrated at the CSSWG.

In addition to CS software causal factor mishap risk assessment, CS hazard mishap risk assessments are performed and must include all associated causal factors in determining the potential that a particular hazard could lead to a CS mishap. The aggregate CS mishap risk for each TLM considers the aggregate of all associated causal

Table 1. Software Causal Factor Risk Criteria

Mishap Risk Level	Description of Safety Criteria
HIGH	– **A software implementation or software design defect that:** • Leads directly to a catastrophic or critical mishap, or • Subjects the system to a single point (1) failure that would lead to a catastrophic or critical mishap
SERIOUS	– **A software implementation or software design defect that:** • Influences a catastrophic or critical mishap, but where two (2) independent functioning interlocks or human actions remain, or • Leads directly to a marginal or negligible mishap
MEDIUM	– **A software implementation or software design defect that:** • Influences a catastrophic or critical mishap, but where three (3) independent functioning interlocks or human actions remain, or • Influences a marginal or negligible mishap, reducing the system to a single point (1) failure
LOW	– **A software implementation or software design defect that:** • Influences a catastrophic or critical mishap, but four (4) or more independent functioning interlocks or human actions remain • Would be a causal factor for a marginal or negligible mishap, but two (2) independent functioning interlocks or human actions remain – **A software degradation of a safety-critical function that is not categorized as high, serious, or medium safety risk** – **A requirement that, if implemented, would negatively impact safety, however code is implemented safely**

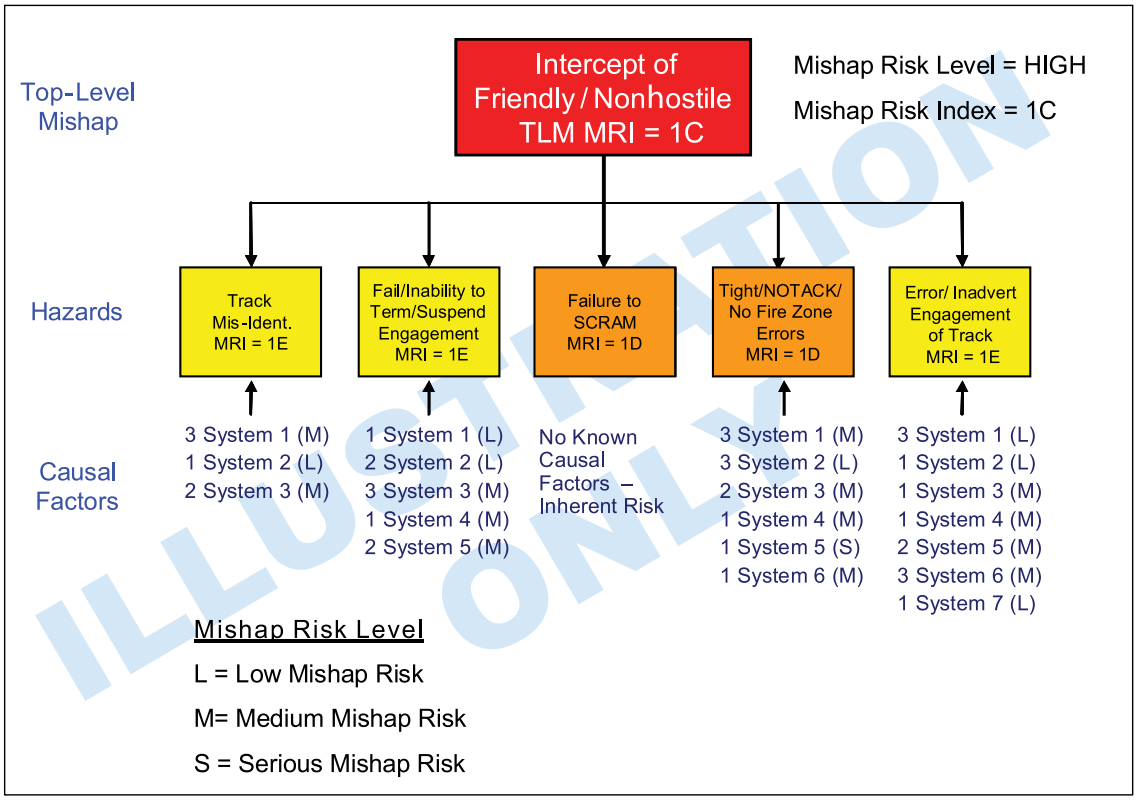


Figure 3. CS Mishap Risk Assessment

factors and hazards, and their collective potential for mishap as illustrated in Figure 3.

The CS TLM assessment is the potential that the mishap will occur based on all associated hazards and causal factors. Using the example depicted in Figure 3, then, each software causal factor mishap risk assessment is performed using the criteria in Table 1, and shows the likelihood that the particular causal factor could lead to the mishap, referred to as the mishap risk level (MRL). So for the Hazard ***Track Mis-ID***, there are five ***Medium Risk*** and one ***Low Risk*** causal factors. These causal factor mishap risk assessments reflect the risk that the mishap of ***Intercept of Friendly/Nonhostile*** will be realized. The mishap risk associated with the hazard ***Track Mis-ID*** reflects the risk based on CS and CSE safety hazard analyses, as well as the mishap risk associated with the causal factor mishap risk assessments. In this case, the mishap risk index (MRI) for the hazard ***Track Mis-ID*** is considered a 1E, or ***Medium Risk***, as defined in the Mishap Risk Assessment Matrix provided in Figure 4.

Determination of CS Mishap risk takes into consideration the aggregate risk of each hazard that could result in the TLM. Following the example in Figure 3 again, it becomes evident that there are five hazards that could lead to the TLM ***Intercept of Friendly/Nonhostile***. In addition to ***Track Mis-ID***, the four other hazards and their MRIs are:

- ***Failure/Inability to Terminate/Suspend an Engagement*** (MRI = 1E ***Medium Risk***)
- ***Failure to SCRAM*** (MRI = 1D ***Serious Risk***)
- ***Tight/NOTACK/No Fire Zone Errors*** (MRI= 1D ***Serious Risk***)
- E***rroneous/Inadvertent Engagement of Track*** (MRI = 1E ***Medium Risk***)

So of the five hazards that can lead to the TLM ***Intercept of Friendly/Nonhostile***, three are assessed as ***Medium Risk***, and two are assessed as ***Serious Risk***. These mishap risk assessments include the results of CS and CSE hazard analysis, as well as causal factor mishap risk assessments. Note that in this hypothetical example, there are no known software causal factors for the hazard ***Failure to SCRAM***, so the hazard mishap risk assessment is based on CS and CSE hazard analysis only. Note, too, that in this example the overall TLM MRI is 1C or ***High Risk***. An explanation for this may be that, in the judgment of the CS PFS, the probability that the TLM will be realized increases based on the two ***Serious*** hazard mishap risk assessments in

concert with the ***Serious Tight/NOTACK/No Fire Zone Errors*** causal factor mishap risk assessment, and the fact that SCRAM processing is likely to be exercised during tactical operations. This example is to be used only to illustrate the relationships between causal factor mishap risk assessments and how they are a part of the hazard mishap risk assessment and that, taken in totality, the aggregate CS TLM risk is assessed.

In summary, it is important to remember that NAVSEAINST 8020.6E states that a CS safety program does not eliminate the need for CSE safety programs and should not be construed as relieving any program manager (PM) of their safety program responsibilities. As shown in this article, CS safety programs are intended to be executed using integrated hazard assessment methodologies, with a focus on identifying and resolving hazards that fall outside of traditional CSE safety program boundaries. Some of the benefits of a well-executed CS safety program include:

- End-to-end CS safety assessment
- Enhanced technical communication via Navy-wide CSSWG meetings
- Coordinated hazard risk assessments and reporting mechanisms
- Capability for providing insight into CS level issues at Mission Readiness Reviews, Mission Control Panels, CS Certification Panels, and other major milestone events
- Consistent CS safety approach for major program managers (MPMs)
- Consistent CS-level Software System Safety Technical Review Panel (SSSTRP) and Weapon System Explosives Safety Review Board (WSESRB) safety reviews

	MISHAP SEVERITY CATEGORY			
MISHAP PROBABILITY	1 CATASTROPHIC	2 CRITICAL	3 MARGINAL	4 NEGLIGIBLE
A FREQUENT	HIGH RISK	HIGH RISK	SERIOUS RISK	MEDIUM RISK
B PROBABLE	HIGH RISK	HIGH RISK	SERIOUS RISK	MEDIUM RISK
C OCCASIONAL	HIGH RISK	SERIOUS RISK	MEDIUM RISK	LOW RISK
D REMOTE	SERIOUS RISK	MEDIUM RISK	MEDIUM RISK	LOW RISK
E IMPROBABLE	MEDIUM RISK	MEDIUM RISK	MEDIUM RISK	LOW RISK

Mishap Risk Level (MRL)	Mishap Risk Indices	Acceptance Authority
High Risk	1A, 1B, 1C, 2A, 2B	Component Acquisition Executive (for Navy programs, this is the Assistant Secretary of the Navy for Research, Development, and Acquisition)
Serious Risk	1D, 2C, 3A, 3B	Program Executive Officer
Medium Risk	1E, 2D, 2E, 3C, 3D, 3E, 4A, 4B	Program Manager
Low Risk	4C, 4D, 4E	

Figure 4. Mishap Risk Assessment Matrix

Shipboard Combat System Training Restoration

By Michael Zemore, Rachael Carroll, and Brian Schwark

In 2004, the Program Executive Office (PEO), Integrated Warfare Systems (IWS) restricted the use of Battle Force Tactical Training (BFTT) at sea and mandated tagout of all weapon delivery systems and tracker illuminators (TIs) in response to safety concerns. In an effort to restore this critical training capability, Naval Surface Warfare Center, Dahlgren Division (NSWCDD) led an extensive safety evaluation to identify the potential hazards associated with the use of the BFTT system and other combat system training capabilities on carriers and amphibious assault ships. This required an assessment of all potential safety impacts to the combat system, ship control systems, air control systems, and shipboard equipment. A team of Dahlgren safety engineers validated the analytical results through shipboard verification testing and collaboration with subject matter experts (SMEs) from the Naval Sea Systems Command, the Naval Air Systems Command, the Afloat Training Group, and the U.S. Fleet Forces Command. The following article recounts the process to successful completion of the training restoration effort and authorization to restore combat system training with BFTT for all ships affected. Also included is a discussion of the lessons learned from the training restoration effort and how this knowledge has evolved to influence both engineering process improvements and future design recommendations.

In the late 1990s, challenged with resource reductions to support fleet training, the U.S. Navy embarked on a program to develop a robust shipboard combat system training capability. The BFTT system was developed to meet these combat system training needs for individual watchstanders, ship's Combat Information Center (CIC) teams, and battle group staffs. The BFTT architecture can support independent, single-ship training as well as multiship battle group training. Battle group training integrates forces by utilizing a common tactical training scenario that is distributed via the Navy Continuous Training Environment (NCTE).

The shipboard subsystem training capabilities are organic and designed to interface with the existing onboard/embedded trainer configurations. Because the BFTT system wraps around the combat system, stimulation/simulation of the combat system is transparent to the trainees. Once safely activated, it provides the essential synthetic data to the numerous shipboard systems required to create the virtual training environment in support of the training scenario objectives. To establish and maintain the virtual training environment, BFTT produces and supplies synthetic navigation data to the ship's

navigation distribution system, synthetic track detection data to the ship's radar, and synthetic electronic warfare emissions data to electronic warfare systems. Collectively, these BFTT capabilities provide a wide spectrum of combat system training support, thereby reducing underway training time and off-ship training service requirements.

But despite the benefits associated with BFTT, subsequent use of BFTT was halted after being linked to two safety incidents that occurred during combat system training. The first shipboard incident was reported in July 2004, when simulated navigation data was distributed to a ship's autopilot, and the safety of ship navigation was compromised. Testing at Wallops Island and shipboard uncovered the second issue, where the fire control radar was unintentionally commanded to radiate during a training exercise. As a result of these incidents, the PEO IWS restricted the use of BFTT at sea and directed ships to tag out missile launchers and fire control radars when conducting BFTT training in port. This restriction impacted training for guided missile cruisers (CGs), guided missile destroyers (DDGs), aircraft carriers (CVs), carrier vessels nuclear (CVNs), amphibious assault ships, general purpose (LHAs), amphibious assault ships, multipurpose (LHDs), and dock landing ships (LSDs). These restrictions were mandated until completion of a safety investigation to ensure that all conditions for potential hazards—both at sea and in port—had been addressed.

The safety investigation, better described as a detailed systems safety engineering analysis, was assigned to safety engineers from NSWCDD's Systems Safety Engineering Division. The primary objective was to restore the safe use of BFTT to the surface fleet for combat system training. It required a focus on the combat system training designs, configurations, and operational procedures to identify potential safety issues with the BFTT/combat system integrated training capabilities. The majority of the investigation and systems safety engineering analyses emphasized the carriers and amphibious assault ships' configurations, since Aegis utilized the Aegis Combat Training System with its embedded safety interlocks.

The analytical effort was expected to be complex, given the numerous BFTT signal injections within the combat systems and ship systems, and the uniqueness of the installations and data distribution networks across individual ships and ship classes. The initial analytical focus was to fully identify all shipboard systems and operations that could potentially be impacted when conducting combat system training. This initial effort helped formulate the path forward for restoration efforts and provided insights for the Red Team—an independent group tasked to perform a safety and programmatic review of the BFTT. The Red Team identified eight primary areas of safety concern related to combat system training as illustrated in Figure 1.

The safety evaluation was extensive and considered all potential hazards associated with the combat system, ship control systems, air control systems, and shipboard equipment. The effort began with data gathering and verification of combat system element (CSE) information for safety evaluation. This included collaboration with SMEs from system commands, fleet commanders, afloat training activities, and design agents to understand and characterize all potential safety issues. Validation of analytical results occurred through shipboard verification testing and collaboration with SMEs. All safety analysis results were documented in matrix format on a per ship basis. This allowed detailed systems safety engineering data and analytical results to be accurately used when implementing mitigations for each impacted ship.

During the initial assessment of intended BFTT operational uses, it was clear that categorizing BFTT utilization as the binary state of either "at sea" or "in port" was not adequate to address all potential hazards. Therefore, the team defined the operating conditions and analytical scope to specifically address the safe use of BFTT while ships operate pierside, at anchor, underway, and during restricted maneuvers. Each environment changed the conditions of the analysis and the resulting mitigations for safe operation.

The analysis encompassed safety assessment of numerous shipboard systems and their functional relationships in various training configurations. These systems were analyzed for training-related hazards associated with detailed design, physical interfaces, system modes, embedded training capabilities, moving parts and energy, power up/down processes, and operator interfaces. The systems analyzed were those associated with identification, engagement control, fire control, navigation, sensor, training, data extract, and communications. In addition, safety devices, verification equipment, monitors, nonstandard configurations, and anything else identified as remotely associated with combat system training was included in the analysis. The causal factors evaluated included:

- Nonparticipating embedded trainer being initiated
- Participating embedded trainer being de-energized

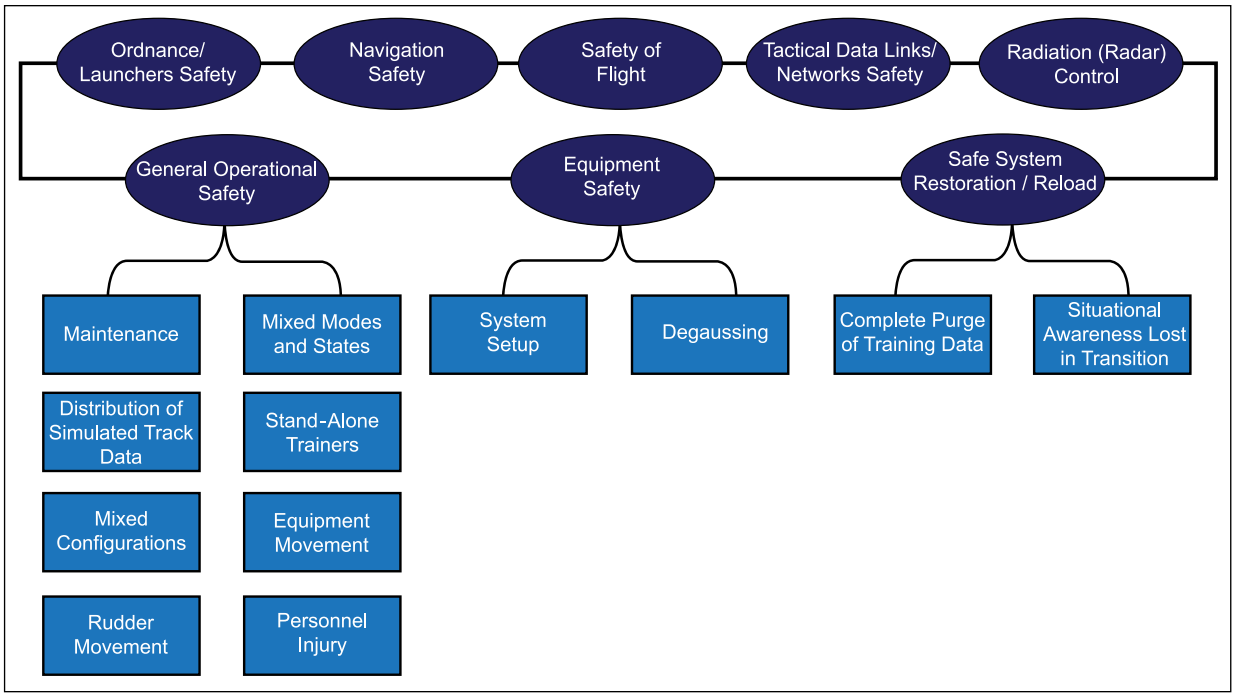


Figure 1. Primary Safety Concerns

- Nonparticipating CSE being energized
- Participating CSE being de-energized
- Mixed CSE modes
- Maintenance procedures being conducted during training
- Incomplete training documentation
- Mixed tagging of tracks (training/tactical)

The culmination of the analysis effort and the process for implementing mitigations to restore the use of BFTT required a detailed review of the safety analyses and mitigations by the Weapon System Explosives Safety Review Board (WSESRB). Chartered by the Chief of Naval Operations (CNO) to provide independent oversight of the Department of the Navy (DON) weapon program's safety efforts, the WSESRB also provides safety-related guidance and recommendations regarding safety engineering analyses, hardware/software/system designs, and hazard mitigation strategies for DON weapon-related systems. Given the complexity of the analyses and volume of systems safety engineering data, multiple WSESRB review sessions, collaborations, and interactions were required to incrementally gain approvals to restore surface ship BFTT training capability.

The mitigations, implemented as mandated procedures, lowered the risk of possible mishap during combat system training. Lifting the weapon delivery system and TI tagouts allowed all necessary components to be included for end-to-end combat system training exercises. The procedural mandates were written as supplements to existing Combat System Operational Sequencing System (CSOSS) guidance. This documentation clearly delineated necessary setup procedures, restrictions, cautions and warnings, and post-training saf-ing procedures to maintain shipboard and weapon system safety for all aspects of BFTT integrated and stand-alone training events. The effort culminated with the authorization to regain use of the BFTT and stand-alone trainers while lifting weapon delivery system and TI tagout restrictions for all ships. This authorization was predicated on the implementation of hull-specific hazard mitigations as derived from the safety analyses. Realistic combat system training is inherently dangerous when conducted shipboard with actual weapon systems. Restoration of the safe combat system training capability allows for improved competencies and mission readiness of our warfighters.

This safety study underscored the necessity for programs to dedicate resources to execute system safety activities with a system-of-systems perspective. Or consider—this safety study underscored the reason why dedicated resources are necessary to execute system safety activities with a system-of-systems perspective. Significant process improvements initiated as a result of this effort continue to reap benefits today. For training systems, as with tactical systems, programs must integrate systems safety engineers with the other functional areas and working groups. It is also

critical that safety programs for individual CSEs are well integrated with the overall combat system safety programs, and are active in system safety working groups. These relationships and forums help ensure that integrated combat system training safety concerns are identified early, discussed among the SMEs, and tracked through resolution.

At the heart of systems safety engineering is the objective to positively influence system design to minimize reliance on human actions for safe operation. The combat system training restoration safety team noted design concerns throughout the analysis and documented recommended architectural considerations for future training capabilities in the Navy's *Training Safety Precepts and Design Requirements*. The publication, developed by NSWCDD in partnership with the Naval Ordnance Safety and Security Activity, should give the guiding principles for every organization that will provide a system or embedded capability to support combat system training. A high-level summary of some key points detailed in the *Training Safety Precepts and Design Requirements* follows:

- Future training capabilities should be engineered to be reconfigurable, predictable, controllable, scalable, and interoperable.
- It is important to have safety in layers: embed, automated safety interlocks for mode transitions in each participating system, with verification processing across all interfaces.
- Simplify and automate training transitions through safe operating modes to reduce potential safety risks of sharing mixed-mode data.
- Localize and automate positive control and monitoring of the training configuration for all participating ship systems.
- Design integrated systems to ensure that tactical operations can be safely maintained when training events are being conducted.
- Eliminate mixed-mode operation; ensure that all training data is properly tagged, and that all systems with the potential to accept training data are designed to process the training tags.
- Display a positive visual indication of training mode on all consoles, including all system displays associated with training/simulated data.
- Design the entire integrated training capability to fleet requirements via a system-of-systems approach. Simply engineering a "box" that interfaces with an existing design is not adequate.

The significant lesson learned during the 3-year effort to restore full BFTT training capability to the fleet was the recognition that introducing new or enhanced shipboard training functionality or capabilities requires the same, or greater, engineering rigor as that expended for changes to shipboard tactical systems. This lesson learned must be embraced and acted upon by all of the fleet training stakeholder activities—technical and operational—to ensure that the necessary engineering requirements, including safety, are accomplished across the complex system-of-systems enterprise that compose a ship's combat system training capability.

Assessment for the Use of Motor Gasoline on Navy Combatant as an Example of Total Ship Safety

By Eric Weissman, Jon Frederick, and Joe Janney

This article is an examination of total ship safety discussing the combination of dangerous substance handling and storage, fire prevention and fighting, and electromagnetic environmental effects (E3). The authors use an assessment of motor gasoline (MOGAS) handling and storage on a Navy combatant as an example of the coordinated efforts of system safety with various technical warrant holders (TWHs) in order to provide a safe system to the U.S. Navy, with known risks identified and assessed.

Total ship safety is an approach that provides a ship acquisition program manager with an understanding of the comprehensive safety risk inherent in the ship and associated systems—from bow to stern—and from the top of the mast to the keel. Throughout the development of the ship, the safety engineer is continuously performing analyses to assess the safety of design and identify potential hazards and design mitigations, as well as communicating safety risk status to the program office. Many times the ship safety assessments focus on specific operations to determine safety risk inherent in those operations, as was the case in a recent safety assessment for MOGAS stowage on an L-class ship.

The use of MOGAS has led to incidents involving fatalities aboard Navy ships in the past; thus, the Navy has minimized the use of MOGAS at sea due to the inherent safety risks. However, although many systems use fuels that are less sensitive to ignition, such as diesel marine and JP-5 jet fuel, MOGAS is still required for certain equipment that supports special operations forces, deployed Marines, and certain shipboard systems.

MOGAS has a flash point, which is the lowest temperature where enough fluid can evaporate to form a combustible concentration of gas, of -45°F. By comparison, diesel fuel (1-D) has a flash point of 100°F. The U.S. Navy has implemented a program to eliminate the need for MOGAS by modifying systems, such as aircraft using aviation gasoline (AVGAS) and the P250 submersible pump, to operate with JP-5. However, there remains a need to provide MOGAS for support operation of equipment deployed with embarked forces. In 1993, the Commandant of the Marine Corps, via CMC letter 5000 EPB-12 of 29 July 1993, endorsed a minimum MOGAS stowage requirement of 10,000

gallons for embarked Marine expeditionary units (MEUs). To date, this requirement to transport and deploy MOGAS remains.

The Systems Safety Engineering Division of the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) recently completed a safety assessment of MOGAS stowage for an L-class ship. The ship had a requirement to provide stowage for 3,000 gallons of MOGAS for internal storage and fuel transfer. The Naval Sea Systems Command (NAVSEA) design community met on the ship to inspect the internal fuel stowage and fuel transfer spaces, and to discuss the issues with internal stowage/fuel transfer and its potential safety risk. As a result of their discussion, several changes were implemented to reduce the risk of MOGAS aboard ship, including:

- Reduce the total onboard stowage of MOGAS from 3,000 gallons to 330 gallons
- Abandon all internal stowage of MOGAS, including both the MOGAS Stowage Room and MOGAS Transfer Room
- Remove the external 1,500-gallon bladder stowage rack and replace with modified low-sulfur diesel (LSD) MOGAS racks (55-gallon drum type)
- Install modified LSD-type MOGAS jettison locker for small bladders and jerry cans
- Install aqueous firefighting foam (AFFF) fixed sprinkling to the external MOGAS stowage area
- Modify and issue an instruction to reflect ship material and operational requirements affected by this change

The MOGAS stowage system for the six 55-gallon drums is a relatively simple "strap-on" system that was determined to be adequate for this ship. The system consists of rack-system hardware, including two jettison racks located amid ship, on the 01 level on the port side deck edge. One rack holds six 55-gallon drums and the other, a MOGAS stowage locker that is adjacent to the drum rack and used to store equipment and containers, including fuel bladders and jerry cans. The locker stores equipment and used fuel bladders and containers, which may be partially filled or empty and are considered hazardous; see Figures 1 and 2.

The system is designed for manual emergency jettison of the six 55-gallon drums and the storage locker in the event of a fire. When the jettison system is activated, restraining bolts are released, and the drums and locker roll overboard. The drum system and locker have separate activation levers.

A safety assessment was conducted to determine the associated safety risk of shipboard MOGAS stowage. NSWCDD Platform Safety Branch personnel conducting the safety assessment were part of the ship inspection team and developed the safety assessment after discussions with the ship designers, ship's crew, and applicable Navy TWHs. The ship areas and equipment pertinent to this assessment included the flight deck, vehicle deck, well deck, and boat crane.

MOGAS is prepared for deployment for the MEU by transferring fuel from the 55-gallon drums to fuel bladders or jerry cans. These containers are moved to the deployment vehicles via a transport route that traverses topside areas, a cargo elevator, the vehicle deck, and then either the well deck or the flight deck for embarkation by the MEU. MOGAS may also be transferred to boats alongside the ship using the boat crane. The drums may be transferred to boats only by using the boat crane; they are not allowed to be moved internally through the ship. All the equipment used to transfer fuel is kept in the locker, including the tools. The upper three drums in the jettison rack are for storage only. If MOGAS is required from them, they must

Figure 1. Shipboard MOGAS Rack Storage System

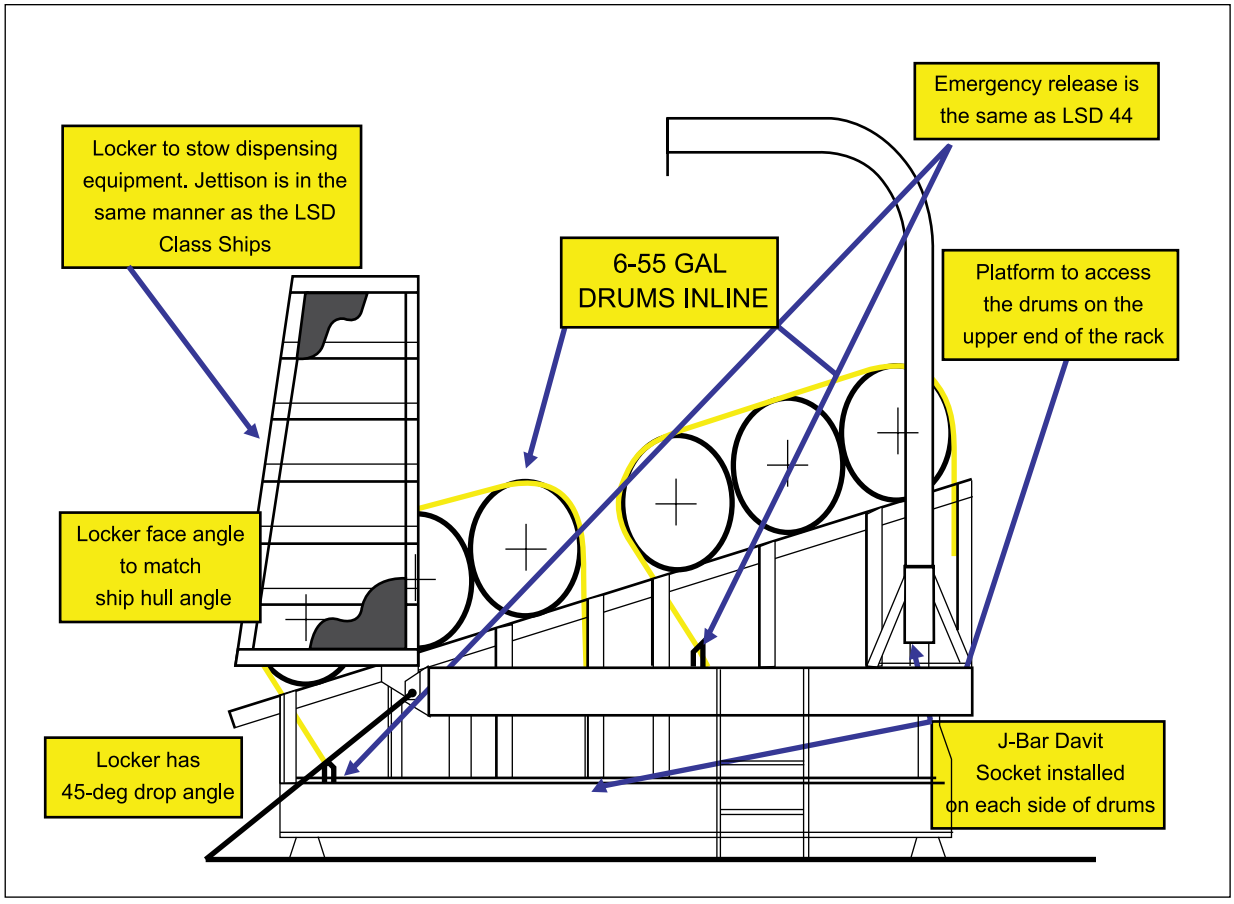


Figure 2. Shipboard MOGAS Storage System Diagram

be swapped out with the lower three drums, using the provided J-davits.

The drums and the stowage locker may be manually jettisoned during a fire, and a manually operated AFFF fire-suppression system activated to provide onboard fire protection for the MOGAS storage area. In the event of a fire in the storage area, personnel would need to manually jettison both the drums and lockers, and activate the AFFF system. The activation mechanisms are located in the boat valley.

Use of MOGAS on Navy ships presents the potential hazard of a shipboard fire, exposure of personnel to hazardous chemicals and vapors, and may impact the environment. The safety assessment for use of MOGAS on the L-class ship addressed each of these areas for each potential mishap. Because a fire requires only fuel, oxidizer, and an ignition source to burn, the safety assessment focused on the ignition source and fuel in assessing mishap potential during operations.

The assessment considered potential ignition sources such as hot work, sparks, smoking, pyrotechnic devices, weather conditions, and radiation hazards. Control of ignition sources during ship operations can be addressed by isolating hot work from the fuel sources, preventing smoking adjacent to potential fuel sources, controlling the use of pyrotechnic devices, ensuring proper grounding in the event of inclement weather, and identifying and controlling sources of ignition from ship's radars and antennas. Directly related to the threat of mishap during MOGAS operations are the tools that are used during those operations. Safety engineering personnel noted that the use of non-sparking tools eliminates an ignition source during

MOGAS operations of fuel transfer from a drum to a bladder or jerry can. The potential for an ignition source due to ship's radars and antennas also required a survey to determine the radiation hazards. A credible radiation hazard from this assessment is the existence of radiating emitters that create hazardous contact currents on the boat crane hook. In addition, the assessment considered other ignition sources, such as nonexplosion-proof light and electrical fixtures.

Aside from combustion, two other possible mishaps are exposure of personnel to toxic vapors and impact to the environment resulting from a spill. Mitigations are divided into hazard mitigations and mishap mitigations. Hazard mitigations are designed to prevent hazards from developing into mishaps. Mishap mitigations reduce the effect of a mishap once an event has been initiated. The hazard mitigations for the MOGAS system include minimizing the quantity of MOGAS stored and handled, transfer of MOGAS bladders and jerry cans in Tri-Wall containers, the use of nonsparking tools, and the use of approved containers, such as 55-gallon drums, 6-gallon bladders, 18-gallon bladders, and jerry cans.

Mitigations to mishaps from MOGAS storage, handling, and transport were assessed to determine their impact to the ship personnel, ship equipment, and the environment. Mishap mitigations include the following:

- The use of AFFF in the storage area to provide fire suppression
- Readily available hazardous material spill kits in the storage areas and along the transport routes
- Use of personal protective equipment (PPE) during fuel handling operations
- Installation of explosion-proof lights and fans in the storage areas and fuel transport routes
- Proper training for ship damage control
- Use of Tri-Wall containers for transport of bladders and jerry cans internal to the ship and jettison of MOGAS drums and stowage locker when the storage area is threatened by fire

From these analyses, the system safety team determined that the highest risk operation to the ship was transferring bladders and jerry cans within the interior of the ship. Fuel spills that occur during transfer will present explosive vapors and severe fire hazards. It was noted that, along the transfer route, there are nonexplosion-proof fixtures and outlets. It was also noted that the ventilation systems in the vehicle deck and well-deck areas are designed to vent JP-5 fumes. It was not known, however, if the current system configuration would be effective for MOGAS vapors. MOGAS fumes are heavier than air and may settle in lower decks away from the spill area. All these areas should have explosion-proof fixtures. The ship procedures clearly state that no transfer of 55-gallon drums (either full or empty) are allowed in the interior of the ship, thus reducing the likelihood of a large internal spill due to a catastrophic drum failure.

Several factors were identified in the assessment that would mitigate the associated safety hazards from MOGAS storage, transfer, and movement about the ship. Minimizing the amount of MOGAS involved during transfer is essential. The use of Tri-Wall containers to transport fuel bladders and jerry cans, while forbidding the transport of 55-gallon drums interior to the ship, mitigates potential risk from large, uncontained fuel spills. Identifying potential ignition sources—such as antennas/emitters, explosion-proof electrical outlets and light fixtures, using nonsparking tools, and implementing proper controls—all help to mitigate the potential for initiating a fire.

The location of the storage racks and the ability to remotely jettison them are two means of removing the fuel source in the event of an adjacent fire. The storage area is also provided with AFFF fire suppression. Mishaps resulting in contamination of personnel and the environment were assessed, and the threat was considered negligible due to the relatively small amount of MOGAS that may leak. Personnel must be equipped with the proper PPE to mitigate the potential for severe injury. Because transfer of MOGAS from the drums to fuel bladders is conducted in an unconfined, open area, the personnel exposure to hazardous vapors is considered minimal. Residual spillage during these operations should be insignificant and result in a minimal environmental impact. When the lower three drums are empty, they are swapped out with the upper three drums using two J-davits. Operations that require moving fuel containers from the storage location to boats alongside the ship should, therefore, be low risk to the platform, since the ship's boat crane will be used.

While stowage and transportation of this highly combustible and inherently dangerous substance aboard U.S. Navy ships has been minimized, it cannot at this point be eliminated. The application of focused analysis utilizing system safety principles, however, allows a reduction in mishap risk to a level at which the benefit to the warfighter is commensurate or greater than the risk itself.

Implementation of Pointing and Firing Cutout Zones

By David Morgan and Greg Sellers

Properly designed and implemented pointing and firing cutout (P&FCO) zones—also known as no point/no fire (NPNF) zones—are essential for the safe use of trainable guns and missile launchers aboard U.S. Navy ships. P&FCO zones protect a ship's structure from damage due to the use of weapon systems, while also providing the weapon systems with the maximum coverage possible. P&FCO zones are designed for missile systems and major-caliber guns by the Naval Surface Warfare Center, Dahlgren Division (NSWCDD), in accordance with NAVSEAINST 9700.2, *Integrated Topside Safety and Certification Program for Surface Ships*, September 1998. This article will discuss the various ways P&FCO zones can be implemented and the positive and negative characteristics associated with each implementation strategy.

In the days of gun ports, P&FCO zones were unnecessary because the barrel of the cannon was outboard of the ship, and the cannon could not be turned enough such that it ever pointed at a ship's structure. Furthermore, the sailor would look out the port and not fire the cannon until the target lined up with it; that situation no longer exists. Weapon systems can be landed anywhere on a ship's topside, and given their flexibility in pointing, they have ample potential to fire into a ship's structure. To make matters worse, they are aimed at targets by computers that are tracking the selected targets but not the interfering aspects of a ship's structure. Hence, the concept of P&FCO zones was born.

The simplest implementation of P&FCO zones that is used today is for machine guns along deck edges. Physical hard stops prevent the guns from pointing too far to either side (train or bearing) or down (elevation), and the amount of travel allowed is dictated by an adjacent ship's structure. If you cannot point at it, you cannot shoot into it. Old-style train hard stops are machined and then bolted into place. Newer train hard stops and the elevation hard stop are adjusted by turning a bolt. This style of P&FCO zone gives the weapon a rectangle within which it can operate.

If a weapon system is not on the deck edge, or if firing over a low ship structure at one point without losing a lower elevation firing angle at another point is required, a simple rectangular P&FCO zone is unacceptable. What is needed is the ability to implement a contoured P&FCO zone. In a world where cost is no object, this contoured zone boundary would be a free-form curve that the weapon system would follow as it barely cleared all ship structure. In practice today, however, contours are made up of horizontal and vertical line segments.

For many years, the accepted method of implementing P&FCO zones was through the use of two stacks of mechanical cams: one stack controlling train and another controlling elevation. (Some readers may remember that in the past, the P&FCO design function was performed by the NSWCDD Cams Group.) The train stack rotates with the weapon in train, and the elevation stack turns as the weapon moves up and down. These stacks of cams are paired with roller switches that rest against their outside surface. The outside surfaces of the cams themselves are machined so that they have a lobe along a certain length of arc. As the weapon moves, the cams move under the roller switches, and as the roller switches go on and off the lobes, firing circuits are enabled/disabled.

The only remaining systems in the U.S. Navy using a cam system are the 5-inch/54-caliber gun aboard older guided missile destroyers (DDGs) and most guided missile cruisers (CGs), and the 76mm gun aboard guided missile frigates (FFGs). The 5-inch/54-caliber gun has four elevation cams: one controlling the upper and lower firing limits and the other three allowing for three intermediate elevation limits. The elevation cams are paired off with train cams that define the extent of each intermediate elevation limit. Actually, two lobes can be machined onto each train cam, so that firing cutout (FCO) zone design can have two separate areas at the three different heights. The bottom line is that all of the structure has to fit under these three elevation limits, which makes designing zones an exercise in trade-offs. Pointing limits define a simple rectangle, and are implemented by adjusting electric pots. A 5-inch/54 cam with one lobe is shown in Figure 1 and a typical 5-inch/54 FCO zone design in Figure 2. This particular design was implemented with three one-lobe train cams.

Figure 1. MK 45 Gun FCO Cam

The 76mm gun system is similar, but it allows four elevation limits. A fifth elevation cam is used to define where the elevation motor will shut down, effectively serving as a backup pointing limit. The primary elevation pointing limits are adjusted by using different value resistors. This gun has no train pointing limits; it can rotate 360°. A 76mm gun P&FCO cam with two lobes is shown in Figure 3, and a typical P&FCO zone design is shown in Figure 4. This zone was implemented with single-lobed cams.

The other remaining mechanical FCO system found in the U.S. Navy is used by the Phalanx Close-In Weapon System (CIWS). CIWS incorporates stacks of microswitches, two each for train and elevation. Each stack contains four microswitches. The enable and disable points for each microswitch can be adjusted using an Allen wrench. Each elevation

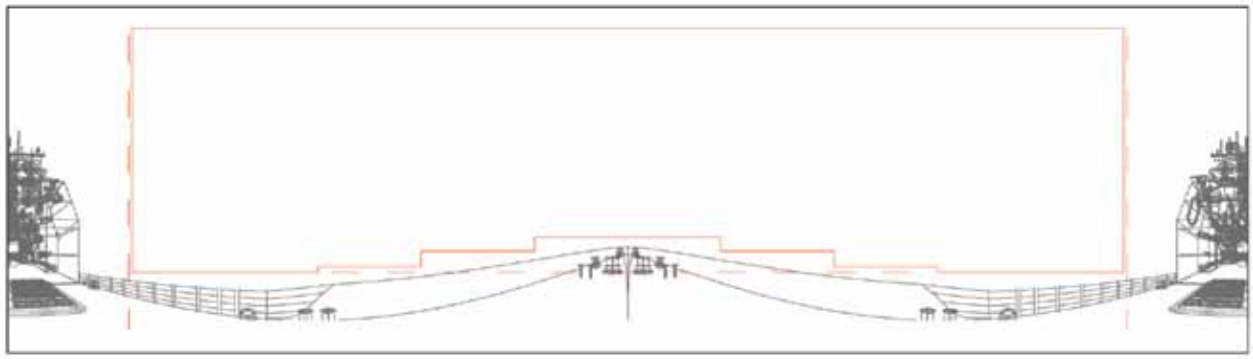


Figure 2. Typical 5-inch/54 Gun FCO Zone

switch is paired with a train switch, and each pair defines a rectangle. Seven of these rectangles define an area where firing is allowed; their overlay defines the overall firing zone. The remaining rectangle defines an area where firing is not allowed and its activation results in an FCO "pop-up" over moveable equipment. CIWS pointing limits are defined by hard stops and are not adjustable. A switch stack is shown in Figure 5. A typical CIWS FCO zone is shown in Figure 6, and its corresponding sector diagram (excluding Sector 8) is shown in Figure 7.

As one might expect, over time, mechanical cutout systems can drift outside specifications; parts wear down, loosen, or become out of adjustment. Given the large number of mechanical parts these systems employ, the maintenance requirements are significant

Figure 3. 76mm Gun FCO Cam

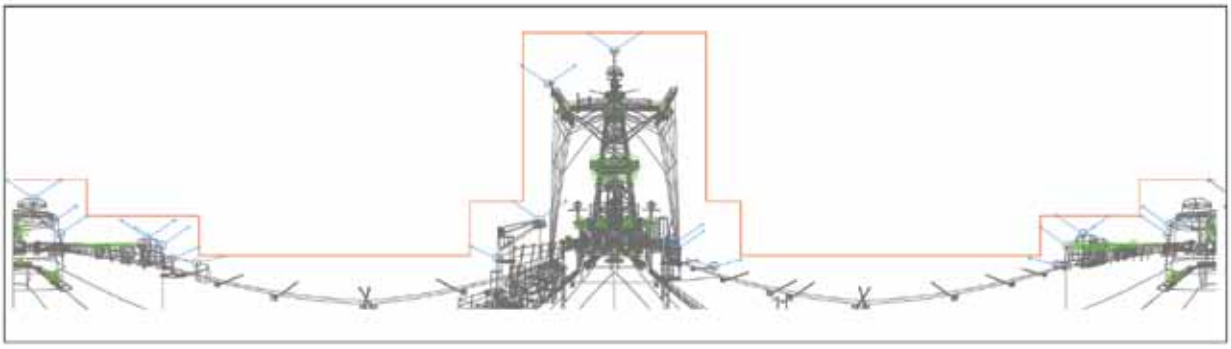


Figure 4. Typical 76mm Gun FCO Zone

and require personnel with the appropriate expertise and skill set to bring the components back into compliance with specifications. The use of circuit boards containing information programmed onto a chip on a circuit card to implement P&FCO zones was the logical progression to alleviate the maintenance burden of mechanical parts. This approach is well represented by the North Atlantic Treaty Organization (NATO) Seasparrow Missile System (NSSMS). This system is a digital implementation of the analog systems in the 5-inch/54- and 76-mm guns, where just four elevation values are allowed in the FCO zone design. A digital twist is that the pointing cutout values are derived from the FCO values. Although the maintenance issues associated with the mechanical FCO systems are eliminated, flexibility in zone design is not improved at all. Additionally, there is a logistical issue introduced; if the card goes bad, there is nothing that can be repaired. The circuit card must be replaced. To alleviate this issue for deployed ships, spares containing the same information are provided to ships. A minor step forward for NSSMS was achieved with NSSMS Mod 12 and 13 systems, where the P&FCO information is now written to the same media as used for digital cameras. An NSSMS P&FCO board is shown in Figure 8, and a typical NSSMS FCO zone is shown in Figure 9.

A major step forward in P&FCO zone implementation was achieved in the Rolling Airframe Missile (RAM) launcher. While this system also uses a programmed circuit board, the input file is a table of 256 elevation values in 1.4° train steps. While in earlier systems the number of steps in the FCO zone design was limited by the FCO zone mechanism, this limitation does not exist in

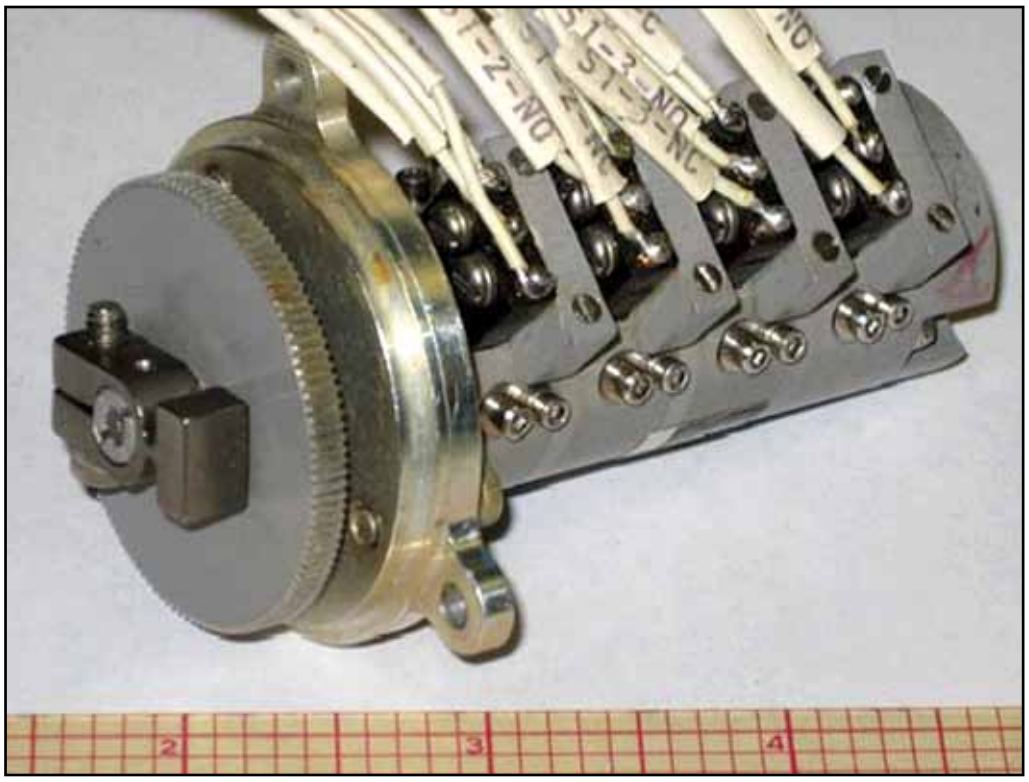


Figure 5. CIWS Switch Stack

Figure 6. Typical CIWS FCO Zone

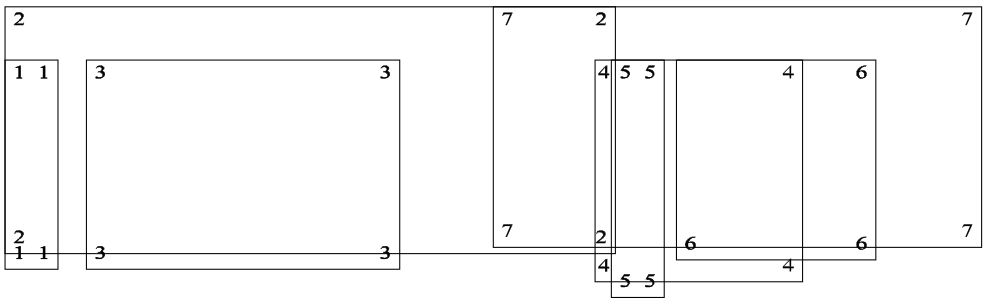


Figure 7. Sectors Defining CIWS FCO Zone

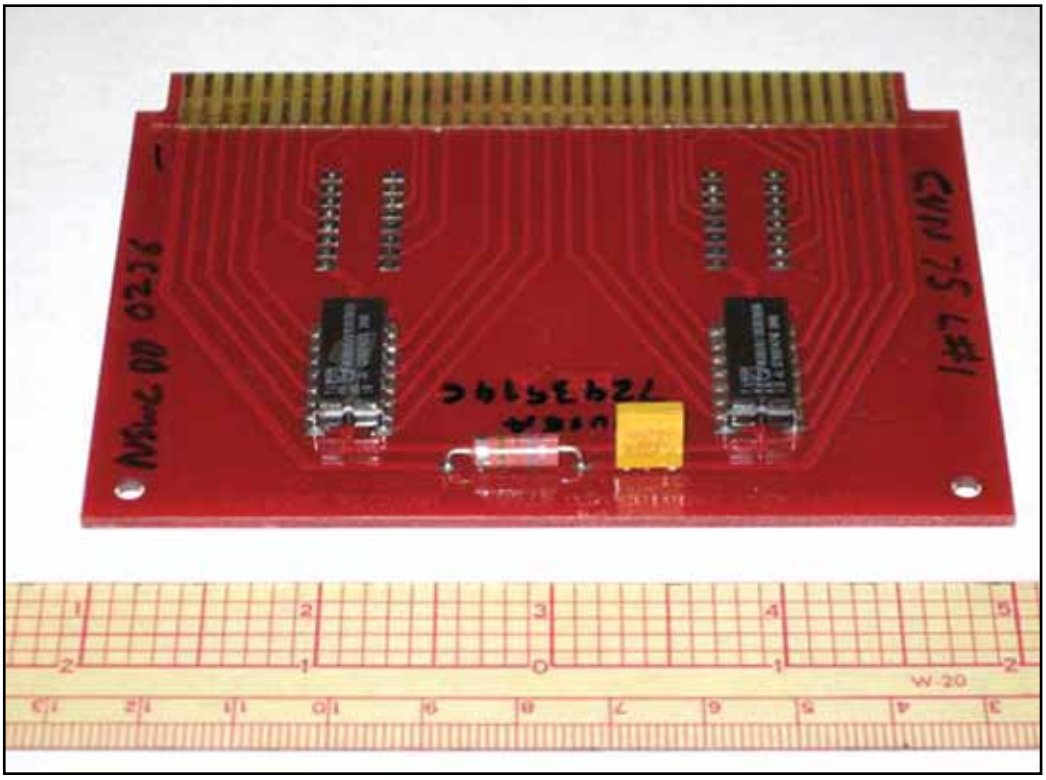


Figure 8. NSSMS FCO Circuit Card

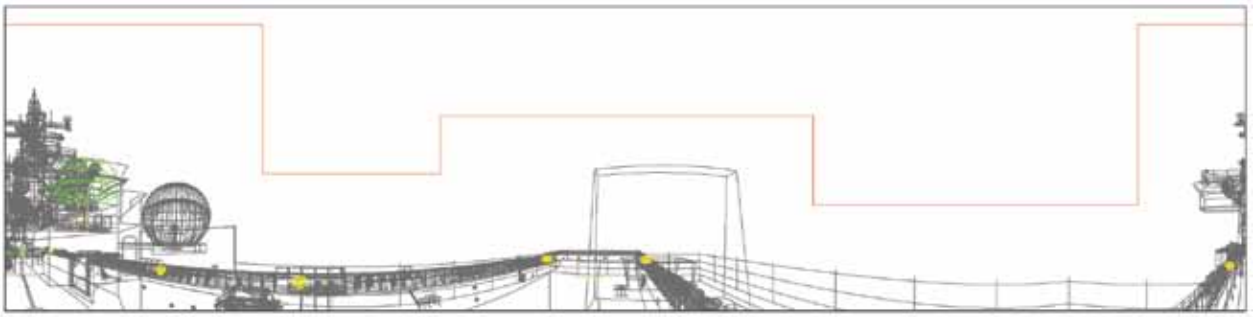


Figure 9. Typical NSSMS FCO Zone

RAM. In fact, the mechanics of launcher motion is the limiting factor in zone design, and steps as small as 5.6° are allowed. As a result, many more steps are possible, as well as much more flexibility. The only negative to this approach is that occasions arise where one would like to implement a step value that does not correspond to a multiple of 1.4°. The RAM card contains separate files for pointing and firing limits, and while the files are generally identical, they do not have to be. The RAM system also allows for implementation of a less restrictive variant of the base FCO design, effectively allowing for a "pop-up" zone. Presently, this feature is used aboard certain amphibious ships to reflect the presence or absence of parked helicopters. A RAM P&FCO circuit board is shown in Figure 10, and a typical RAM P&FCO zone is shown in Figure 11.

The 5-inch/62-caliber gun also implements P&FCO zones with a programmed circuit board. However, in this case, the table consists of over 8,000 values, meaning that the zone designer has basically no limitation as to the zone value to be implemented. FCO design limitation comes from the fact that only 30 corners can be specified in the zone. The pointing zone for 5-inch/62 guns aboard DDGs still consists of a rectangle, but the

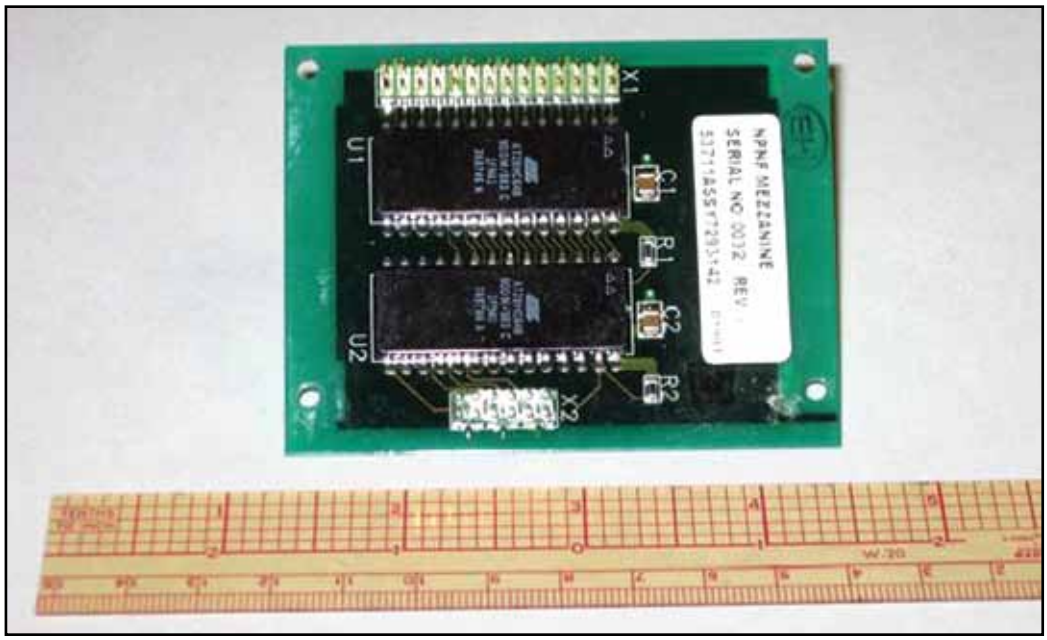


Figure 10. RAM P&FCO Card

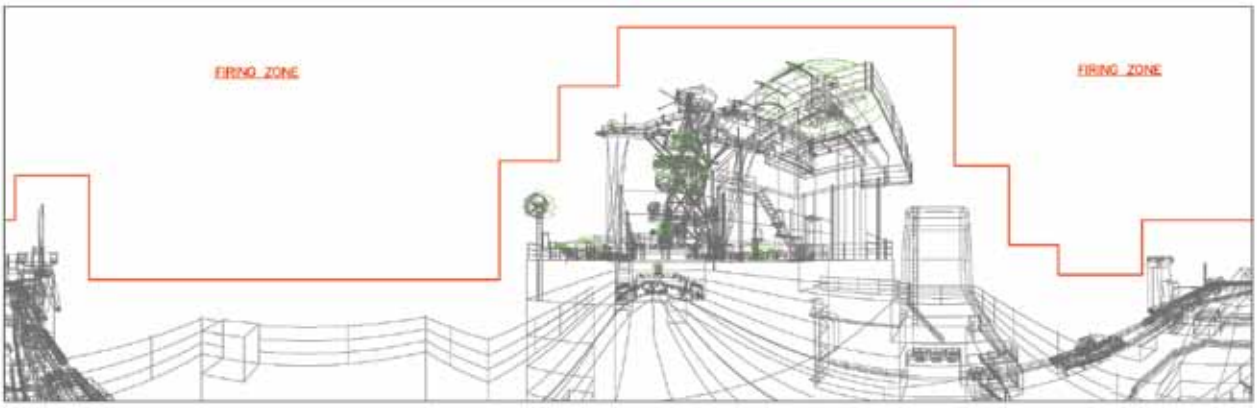


Figure 11. Typical RAM P&FCO Zone

gun variant being back-fitted on CGs will allow a contoured pointing zone to be implemented. A 5-inch/62 gun FCO computer chip is shown in Figure 12, and a typical 5-inch/62 gun FCO zone is shown in Figure 13.

One issue that does not exist with mechanical systems is obsolescence. As long as drawings of the part to be replaced are available, a replacement part can be manufactured—not so for systems using circuit cards. For instance, the chips needed for NSSMS boards are becoming increasingly difficult to find. The logical progression is to bypass the need for an externally programmed circuit board and to upload the necessary files directly into the system. The first system to go this route was the Mk 46 30mm gun aboard the LPD 17 class. Unfortunately, the decision was made to incorporate the cutout information in the compiled portion of the gun control system (GCS) software. The effective result is that if cutouts need to be revised due to topside changes, the entire GCS software package needs to be certified and approved by the Weapon System Explosives Safety Review Board (WSESRB), adding considerable cost to the program. Ideally, the same software load would then be applied to all the guns

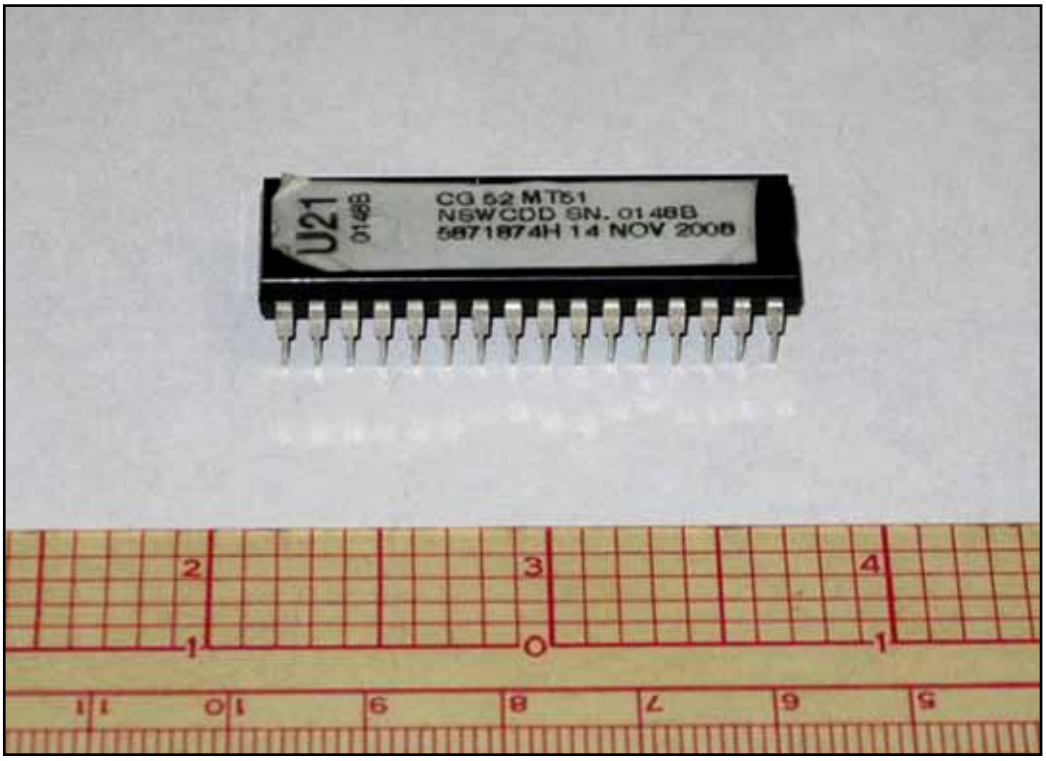


Figure 12. Computer Chip for Implementing 5-inch/62 Gun FCO Zone

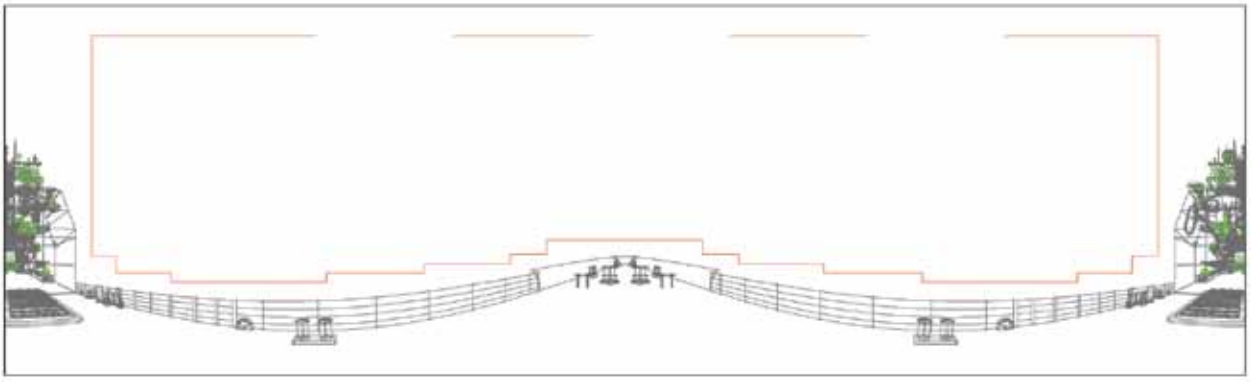


Figure 13. Typical 5-inch/62 Gun FCO Zone

across the ship class, but this goal conflicts with the staggered implementation of topside changes. Experience shows that FCO design needs to be hull-specific. Indications are that software changes are being contemplated that would keep FCO zone information separate from the compiled portion of the GCS software. A typical Mk 46 Gun FCO zone is shown in Figure 14.

An example of a more flexible approach is provided by the Mk 110 57mm gun, found on the Littoral Combat Ship (LCS)-class ships and the WMSL 750-class Coast Guard cutter. The P&FCO zone information for this gun is uploaded as adaptation data to the GCS using a dedicated laptop and connector. The P&FCO zone contour can have elevation steps as small as 0.5° and as many as 100 corners. Pointing and firing contours can be independent of each other. While one may quibble over the necessity of an actual laptop to perform this information transfer, this basic approach seems to be the way of the future. A typical Mk 110 gun FCO zone is shown in Figure 15.

As can be seen, P&FCO zones can be implemented in numerous ways, and each approach has positive and negative characteristics. Ideally, as new methods are investigated, the robustness of the system, flexibility of zone design, and ease of zone revision will all be considered. NSWCDD will continue to work within the constraints of each P&FCO system to give our ships as much protection as possible.

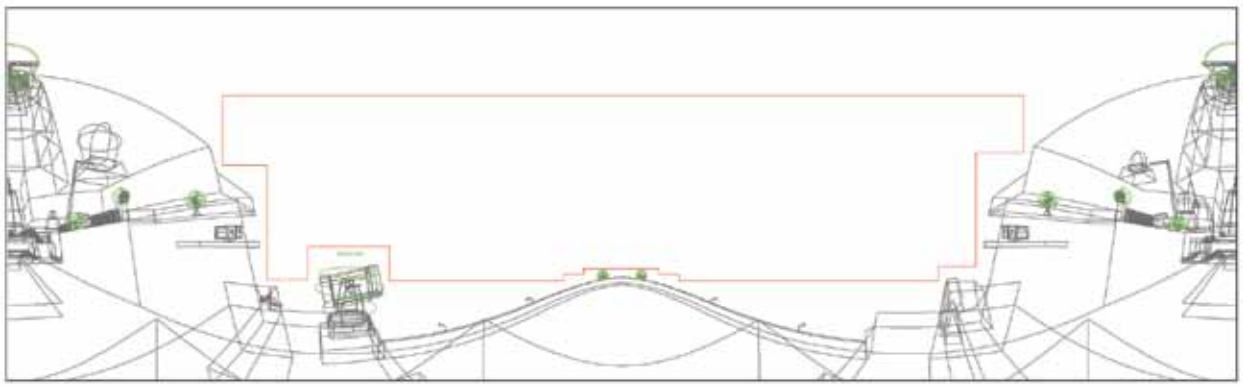


Figure 14. Typical MK 46 Gun FCO Zone

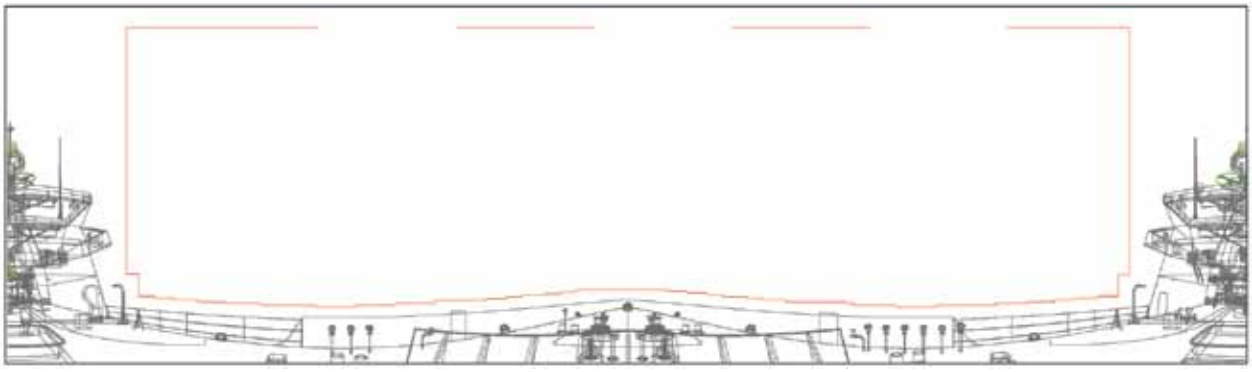


Figure 15. Typical MK 110 Gun FCO Zone

System Safety for Rapid Integration Projects

By Carolyn Blakelock

Rapid integration projects are capability demonstration efforts that take existing, fielded technologies or mature developmental technologies and integrate them onto vehicles to create a system of systems. Current projects include Gunslinger, the Full Spectrum Effects Platform (FSEP), and Wolfpack. These projects have focused on integrating technologies onto military ground vehicles to provide the warfighter with better situational awareness, communications, and cooperative engagement capabilities. As their name implies, these are fast-paced programs, typically lasting 12–24 months.

These programs offer many challenges from a safety perspective. They are fast moving and do not follow the typical acquisition cycle. Formal requirements documents may not exist. Any requirements are typically in the form of desired capabilities, and these tend to be very high level. Schedule and budget constraints also limit the amount and types of testing that can be performed. Yet the program goals require that a system safety program be performed that will enable uniformed personnel to utilize the system in a warfighter assessment, as well as possible deployment. This article examines the unique challenges of these projects and strategies for meeting them.

Since 2004, the Platform Integration Division at the Naval Surface Warfare Center in Dahlgren, Virginia, has been engaged in rapid integration projects. As previously stated, these projects take existing, fielded technologies or mature developmental technologies (Technology Readiness Level (TRL) 6 and above), install them onto military vehicles, and create the software that enables the systems to work together, thus creating a system of systems. In order to ensure that the systems being developed are useful and effective, uniformed personnel are brought in as early in the development process as possible. Such involvement can range from evaluation of the functionality and layout of the graphical user interface to using the vehicle(s) in a training exercise. The ultimate evaluation is an operational evaluation via actual deployment to theater.

The first such project undertaken by the Division is Gunslinger. Gunslinger focused on developing a multispectral, on-the-move hostile fire detection and counterfire system that provides mobile ground forces in operational environments with real time and precise location of hostile direct fire, as well as the ability to engage the source of

the hostile fire in near real time. The primary components of the system include an electro-optical infrared shot detection system, an acoustic shot detection system, a stabilized gun mount, and a situational awareness (SA) video system. These sensors and weapon system have also been integrated with navigation and communication systems to track event detections while "on-the-move" and to relay information about those events using either satellite or wireless local area network (WLAN) communications. Gunslinger was integrated onto a High Mobility Multipurpose Wheeled Vehicle (HMMWV) and an International Military Extreme Truck – Military Version (MXT-MV), as shown in Figure 1.

Managed by the Office of Naval Research (ONR), Code 30, Maneuver Thrust Area, Gunslinger is a joint project among the Army, Navy, and United States Marine Corps (USMC), along with several government laboratories and industry partners. Gunslinger has recently completed a 6-month tour in Iraq, where it participated in over 100 missions and was used to provide overwatch surveillance at Al Asad and street patrols in Fallujah.

The second rapid integration project undertaken is the FSEP, which was initiated in response to a time-critical Joint Urgent Operational Needs Statement (JUONS). The JUONS called for a progressive escalation of force capability in order to engage neutral and hostile crowds using nonlethal, scalable effects and solutions to overcome technology gaps to counter the threats of rocket-propelled grenades (RPG), improvised explosive devices (IED), and snipers. The base vehicle for the FSEP efforts is a Stryker Infantry Carrier Vehicle (ICV), shown in Figure 2.

FSEP takes the Gunslinger capability (minus the electro-optical infrared shot detection system) and combines it with a suite of nonlethal technologies—including a Long-Range Acoustic Device (LRAD), bright white lights (BWL), and a Green Beam Designator (GBD) IIIC laser—to provide an escalation of force capability. Three Stryker ICVs were equipped with the Spiral 1 FSEP technology and deployed to Iraq for operational evaluation for over 18 months. While two of the vehicles are still in theater, the third was hit by an IED and was returned to the United States for repair. That vehicle was then used for development of Spiral 2, which adds nonlethal shove capability in the form of a 12-GA shotgun using nonlethal rounds (sting balls and rubber buckshot) and 66mm grenade launcher (firing smoke and nonlethal grenades).

There have been many funding sources for FSEP. Initiated by the Office of the Secretary of Defense (OSD) and originally funded by the Office of Force Transformation, FSEP was later transferred to the Joint Rapid Action Cell (JRAC). Current

Figure 1. Gunslinger Spiral 2 (MXT-MV)

Figure 2. FSEP Spiral 3 (Stryker)

sponsors are the Army Training and Doctrine Command (TRADOC), the Army Capabilities Integration Center (ARCIC), and the OSD. The program is managed by the Army Project Manager for Close Combat Systems (PM CCS) with the Project Manager, Stryker Brigade Combat Team (PM SBCT). The Joint Product Manager for Reconnaissance and Platform Integration (JPM-RPI) at the U.S. Army Edgewood Chemical Biological Center (ECBC) funded the development and manufacture of the 66mm articulating grenade launcher systems installed on the remote weapon system.

The final rapid integration project for discussion herein is known as Wolfpack, shown in Figures 3 through 5. Wolfpack builds upon the capabilities and technology of FSEP and adds communications capability, enabling cooperative engagement and shared situational awareness between vehicles and between dismounts and vehicles. Wolfpack equipped three vehicles:

- A Cougar Mine Resistant Assault Protected (MRAP) 4x4
- An International MXT-MV
- An Oshkosh Medium Tactical Vehicle Replacement (MTVR)

Wolfpack is sponsored by the Office of the Under Secretary of Defense (OUSD), Acquisition, Technology, and Logistics (AT&L) Rapid Reaction Technology Office (RRTO).

The Platform System Safety Branch of the Naval Surface Warfare Center Dahlgren, Virginia, performs system safety for all three of these projects. Gunslinger and Wolfpack are both USMC projects and follow the Navy's system safety processes. FSEP is an Army project, and system safety testing for safety confirmation is performed by the Aberdeen Test Center (ATC) in Maryland.

Gunslinger laid the groundwork for system safety for rapid integration projects. Their primary sponsor, ONR, worked with the Dahlgren Principal for Safety (PFS) and the Navy's Weapon System Explosives Safety Review Board (WSESRB) to create a System Safety Management Plan for Science and Technology (S&T) programs. Gunslinger was

Figure 3. Wolfpack Spiral 1 (Cougar)

Figure 4. Wolfpack Spiral 1 (MXT-MV)

Figure 5. Wolfpack Spiral 1 (MTVR)

revolutionary, in that it was the first time an S&T program fully embraced a formal system safety program.

Table 6 of Appendix A of MIL-STD-882C provides guidance for system safety activities based upon level of risk or dollar amount. Small-dollar or low-risk programs perform the fewest safety tasks, while high-risk or high-dollar programs perform the most safety tasks. The following tasks from Table 6 were identified as being appropriate to the program goals of deployment for operational evaluation, while still meeting the budget and schedule constraints of a rapid integration prototype effort:

- Task 101: System Safety Program
- Task 102: System Safety Program Plan (SSPP)
- Task 106: Hazard Tracking
- Task 201: Preliminary Hazard List (PHL)
- Task 202: Preliminary Hazard Analysis (PHA)
- Task 204: Subsystem Hazard Analysis (SSHA)
- Task 205: System Hazard Analysis (SHA)
- Task 206: Operating and Support Hazard Analysis (O&SHA)
- Task 207: Health Hazard Assessment (HHA)
- Task 301: Safety Assessment

Tasks 101, 102, 201, 202, 205, and 301 are safety activities identified by MIL-STD-882C as being appropriate for a low-risk or small-dollar program. Tasks 106, 204, 206, and 207 are 4 of the 12 safety activities identified as being appropriate for average risk or medium dollar programs. By contrast, a high-risk or large-dollar program has 18 recommended safety activities.

Because the goal of the program was to deploy a system to Operation Iraqi Freedom for operational evaluation, the program had to go before the WSESRB. Even though the end-user for Gunslinger is the USMC, the sponsor is the Navy; therefore, two separate risk acceptance authorities were identified. For the Navy, the risk acceptance authorities were:

- Maneuver Thrust Manager, ONR Code 30 (low risks)
- Director of Applications, ONR Code 30 (medium and serious risks)
- Deputy CNR, ONR Code 30 (high risks)

For the USMC, the risk acceptance authorities were:

- Commanding Officer, MWS-373 (low and medium risks)
- Commanding Officer, MWSG-37 (serious risks)
- Commanding General, 3rd MAW (high risks)

All of the residual risks for the Gunslinger Spiral 2 Program were low or medium, except for one serious risk related to the Mk 45 gun mount that was previously accepted at the appropriate level for the High Speed Vessel application. Prior to deployment, Marines from the Marine Wing Support Squadron (MWSS) 373 utilized the Gunslinger system in an exercise at the Marine Corps Ground Air Combat Center (MCGACC) at 29 Palms, California. The result of this exercise was a Safe and Ready report. After this event, there was a change in deployment plans, and Marines from MWSS 371 utilized the Gunslinger system in Desert Talon at Yuma, Arizona. Desert Talon is a predeployment exercise.

As an Army project, FSEP follows a different path than Gunslinger. The Dahlgren PFS performs the same basic safety tasks as for Gunslinger, but the documentation delivered to the Army is condensed into a Safety Assessment Report and a report of the hazards from the Hazard Tracking Database. Once these documents and the vehicle(s) have been delivered to Aberdeen, the primary responsibility for the safety testing of the vehicle(s), risk acceptance, and the Safety Confirmation is taken over by the Army and the test and safety engineers of the Aberdeen Proving Ground. Safety testing can include:

- Software testing
- Functional safety testing
- Electrical safety
- Egress safety
- Vehicle stability
- Hazards of electromagnetic radiation to personnel, fuel, or ordnance, etc.

Aberdeen Proving Ground is responsible for issuing the Safety Confirmation. It should be noted, however, that even though the Army provides the Safety Confirmation and performs the official safety testing, the safety work performed by the Dahlgren PFS was done according to the standards and expectations of the WSESRB.

Spiral 0 of FSEP went through safety testing at ATC to obtain a safety release for Limited Utility Assessment (LUA) at Fort Benning, Georgia. The LUA was completed, and feedback was incorporated into FSEP Spiral 1. FSEP Spiral 1 went through safety testing at ATC to obtain a Safety Confirmation for deployment to Operation Iraqi Freedom. FSEP Spiral 2 is currently undergoing safety testing at ATC to obtain a Safety Confirmation for deployment to Operation Iraqi Freedom.

As a USMC project, Wolfpack follows in Gunslinger's footsteps, with Dahlgren responsible for the system safety program. There is, however, one significant difference between Gunslinger and Project Wolfpack. In Project Wolfpack, experimentation exercises with Marines were planned

as part of the development effort. When the project began in February 2007, an introductory meeting was held with the WSESRB Chair and the Marine Corps Systems Command (MCSC) Safety Director. During that meeting, it was suggested that the Wolfpack sponsor put a memorandum of agreement (MOA) in place with the Safety Office of MCSC, designating MCSC the authority to provide safety releases for the experimentation exercises. This effort was initiated, and the MOA was signed among the OUSD, the AT&L Director, the RRTO, and the Commander, MCSC.

The safety data sent to MCSC for review consisted of a Safety Assessment Report that combined the results of the various safety analyses and a copy of the Hazard Tracking Database. Additional documentation included safety information on existing systems, test reports from effects of electromagnetic energy testing (performed by the Electromagnetic and Sensor Systems Department, Advanced Science and Technology Branch at Dahlgren), and vehicle stability test reports from the National Automotive Test Center (NATC) in Nevada. The risk acceptance authority for all risks was the commanding officer of the unit participating in the experimentation exercise and the project sponsor. The Safety Assessment Report was also submitted to the risk acceptance authorities along with a risk acceptance document summarizing the residual risks. The risk acceptance document was then signed by the risk acceptance authorities and submitted as part of the safety package that was prepared for review by MCSC.

To date, Project Wolfpack has held three experimentation exercises. The MCSC Safety Director provided a limited safety release for each of these events. The first took place in August 2007 at a live fire range at the Marine Corps Base in Quantico, Virginia; the second and third exercises took place in February and August 2008 at MCGACC at 29 Palms, California. The first two safety releases came directly from MCSC; but when it was time to obtain the third safety release, the new safety director required the safety case for Project Wolfpack to be reviewed by the Laser Safety Review Board (LSRB), the WSESRB, and the Software System Safety Technical Review Panel (SSSTRP). Thanks to the cooperation of all three boards, the tight schedule of the project was accommodated, and a safety release for the August 2008 event was obtained.

These three projects are revolutionary in several ways. First, they set a precedent by incorporating a formal system safety program into an S&T rapid integration effort. System safety was integrated into these efforts from their initiation. Next, ONR's investment of time and money into the development of a System Safety Management Plan for S&T programs was particularly crucial. Without the system safety success of Gunslinger, FSEP and Wolfpack would have had a far more difficult way forward. FSEP laid the groundwork for collaboration between the Army and the Navy with regard to system safety and has created a positive system safety relationship between Dahlgren and Aberdeen. Project Wolfpack has established a mechanism for obtaining safety releases for USMC participation in experimentation exercises.

These efforts set another precedent by involving the end-user in the development effort as early as possible. This approach of prototyping, combined with experimentation exercises, provides a model for acquisition as new technologies can be exercised and vetted with the end-user, resulting in better requirements for formal acquisition programs. In addition, by involving the user in the development effort, especially with regard to hardware and software user interfaces, these projects are taking a more human-centered approach to system design. A human-centered design approach results in interfaces that are more intuitive and easier to use, which reduces the risk of operator error and increases the overall awareness of the state of the system.

As these projects transition to programs of record, the system safety work that has already been performed reinforces the value and necessity of early integration of system safety into the overall development effort. The cross-service nature of these projects also helps to reinforce the joint system safety process that is currently being established.

Acknowledgments

I would like to thank Frank Lagano, the project lead for Gunslinger, for sharing his expertise on the Gunslinger development effort and for providing me with the Gunslinger system safety documentation. I would also like to thank the members of the LSRB, the SSSTRP, the WSESRB, and the Safety Directorate at the MCSC for their guidance, assistance, and system safety support.

NSWCDD's Role as the Lead Navy Technical Laboratory (LNTL) for Laser Safety Within the Department of the Navy (DON)

By Sheldon Zimmerman, Robert Aldrich, and Thomas Fraser

Since the 1960s, various military organizations have provided Laser Radiation Health Standards criteria and established medical surveillance programs. However, prior to 1979 no lead agency existed to ensure uniform application of these criteria to military systems. Laser health hazards prevention was left almost entirely to the individual system developers and users.

In March 1979, the Chief of Naval Materiel designated the Naval Electronic Systems Command (now designated as the Space and Naval Warfare Systems Command (SPAWAR)) as its lead agency for the Navy Laser Hazards Prevention Program. SPAWAR surrendered its role as the central point of contact for Laser Safety in the mid-1990s.

Since then, the Secretary of the Navy through SECNAVINST 5100.14, *Military Exempt Lasers*, series has designated the Bureau of Medicine and Surgery (BUMED) as the Administrative Lead Agency (ALA) and the Naval Sea Systems Command (NAVSEA) as the Technical Lead Agent (TLA) for the Navy and Marine Corps. Subsequently, OPNAVINST 5100.27B/MCO 5104.1C, *Navy Laser Hazards Control Program*, describes the entire program in its current state.

Department of the Navy (DON) policy is to identify and control laser radiation hazards early during design and development as a matter of military necessity. It is also the policy of the DON to ensure that personnel are not exposed to laser radiation in excess of the Maximum Permissible Exposure (MPE) limit throughout the life cycle of a laser system, which includes:

- Research
- Design
- Testing
- Development
- Evaluation
- Acquisition
- Deployment
- Operation
- Support
- Maintenance
- Demilitarization
- Disposal

By mandate, policy, and principle, the DON provides personnel safety oversight for the use of all military lasers in its inventory. The heart of this oversight is realized by a required safety review conducted by the Navy Laser Safety Review Board (LSRB). The LSRB comprises representatives from all the System Commands, the Naval Safety Center, Marine Corps Headquarters, BUMED, and the Lead Navy Technical Laboratory (LNTL) for Navy and Marine Corps Laser Safety.

The Naval Surface Warfare Center, Dahlgren Division (NSWCDD), Code G73 has maintained the technical lead for DON Laser Safety for almost 30 years and has been designated by NAVSEA as the LNTL. The LNTL provides the expertise required to independently evaluate and verify the technical aspects of safety-related design and application criteria for lasers and laser systems within both the inventory and acquisition processes of the DON, including those used for joint service and interagency applications and missions. The joint laser safety review process is shown in Figure 1.

To this specialized expertise, the LNTL at NSWCDD maintains a group of laser safety specialists holding leadership positions on government, national, and international laser safety standards committees. For example, members of the LNTL hold chairmanships on the American National Standards Institute (ANSI) Committee for the Safe Use of Lasers Outdoors, and the ANSI and International Electrotechnical Commission groups on Laser Safety Measurements. The LNTL performs advanced laser parameter verification measurements and determines applicable laser safety recommendations as the technical evaluators for the LSRB. These measurements are performed either in the local laser safety laboratory maintained at Dahlgren or at other government or manufacturer facilities using National Institute of Standards and Technology (NIST) traceable measurement equipment. An example laser system under evaluation is shown in Figure 2.

One of the primary roles the LNTL fills is providing technical support to the Navy in utilizing existing and emerging laser technology in the development of weapons and weapon-related systems. For example, Navy maritime forces and the Marine Corps recently identified a capability gap in their operations, which they intended to fill through the use of a dazzling laser system for the purpose of hailing and warning suspected threats. After an analysis of alternatives and execution of

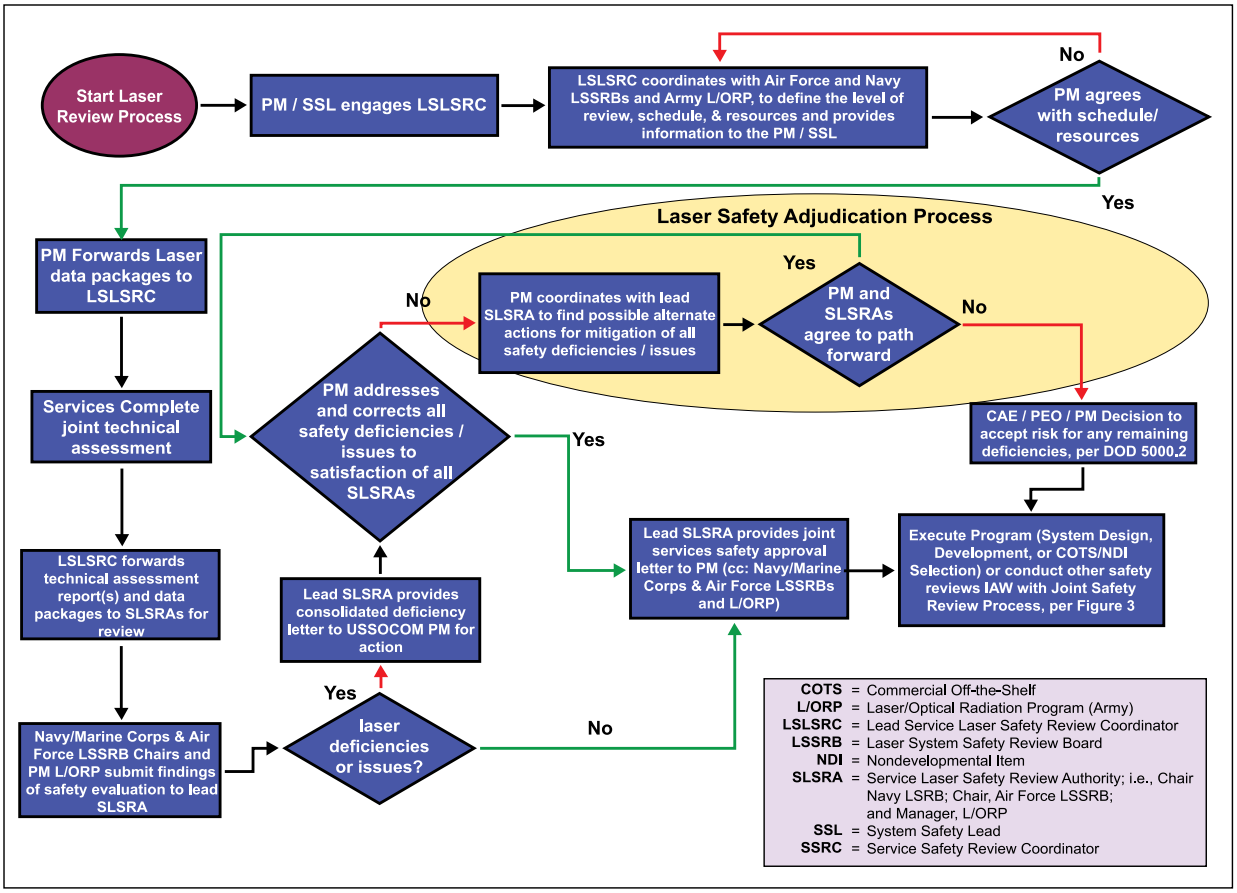


Figure 1. Joint Laser System Safety Review Process

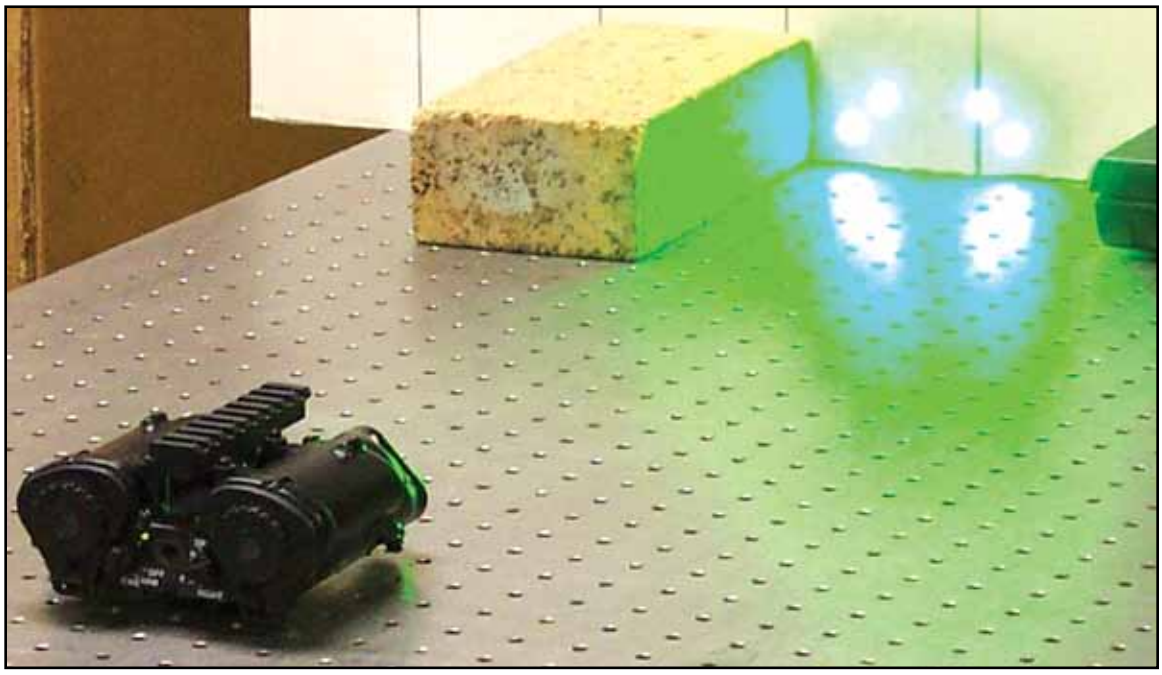


Figure 2. Ghost Laser System Under Evaluation

a source-selection process, a device was selected, and a preproduction unit was submitted to the LNTL and LSRB for review and approval for use. The original preproduction Green Beam Designator-III Custom (GBD-IIIC) system, shown in Figure 3, had a nominal hazard distance to the naked eye of about 114 m for a 10-second exposure. The refined production version of the GBD-IIIC that was fielded had a nominal hazard distance to the naked eye of only about 63 m for a 10-second exposure. Both of these system options were inherently dangerous, as permanent eye damage was possible within the hazard distance to those exposed to the laser beam. Acting on recommendations and requirements from the LSRB and LNTL, the Marine Corps undertook a system improvement effort to produce a dazzling laser system that could maintain the desired functionality, while simultaneously maintaining a high degree of safety. The result of that collaborative effort was the current system entering the fielding cycle, which is known as the LA-9/Portable, or LA-9/P. The LA-9/P uses a Class 1 laser rangefinder retrofitted to the GBD-IIIC to determine the distance between the laser and the target, and implements a Safety Control Module (SCM) that switches off the dangerous beam if the target is within the hazard distance of the laser. This design virtually eliminates the possibility of a laser injury. While currently an interim solution, it is nonetheless one that moves the program down the road toward creating an inherently safe dazzling laser.

In addition to providing laser-related engineering support to programs, the LNTL team also provides advanced laser safety training to Navy and Marine Corps personnel. Two of the four DON laser safety certifications are provided by this group through the courses taught at NSWCDD, which include the Technical Laser Safety Officer (TLSO) and Laser Safety Specialist (LSS) classes. Achieving TLSO certification qualifies the certificate holder to be designated as a command Laser System Safety Officer in order to run a base or facility-level laser hazard control program, or to be a Range Laser Safety Officer. LSS certification equips the course graduate with the knowledge to perform a laser hazard evaluation. At the request of PMS 480, the LNTL conducted the TLSO course at NSWCDD (see Figure 4) during the LA-9/P development effort, in support of fielding the LA-9/P green laser

Figure 3. GBD-IIIC Dazzling Laser System Under Evaluation

Figure 4. Navy uniformed members and civilian workforce members sitting for the TLSO examination in the lobby conference room of building 1470

devices to Navy Maritime forces. Immediately following the TLSO exam for that class, the students were given a demonstration and hands-on introduction to the LA-9/P on the abandoned airstrip (see Figures 5 and 6).

The basic philosophy of the LNTL is, whenever possible, "do what makes sense" with regard to laser safety. Strict, but necessary, laser regulations add both structure and rigor to the task, but a reasonable approach to merging the regulations with the complex principles of laser system safety typically generates satisfactory results. Aiding users, operators, and laser safety officers in understanding why a requirement exists is generally helpful in ensuring that they adhere to it, and adopting a common sense attitude toward laser safety facilitates this.

Figure 5. Navy uniformed members and civilian workforce members receiving a demonstration of the LA 9/P mounted on a modified "rifle" stock from the device manufacturer

Figure 6. Navy uniformed members and civilian workforce members conducting a hands-on introduction to the LA 9/P mounted on a modified "rifle" stock

LEADING EDGE

COMBAT

ENGAGEMENT

PLATFORM

Systems Safety

ENGINEERING

LEADING EDGE
Volume 7, Issue No. 3

Systems Safety Engineering

"Our men and women in uniform are putting their lives on the line every day in defense of our freedoms and way of life. Hence, we all have an inescapable duty and responsibility to equip them with the absolutely best capabilities possible, with safety as a primary and enduring factor. System safety is not nice to have; it is an integral and essential part of the systems engineering process."

Mr. Tom Rollow
Deputy Assistant Secretary of the Navy (Safety)

LEADING EDGE
Volume 7, Issue No. 3

Fallen Warriors

Here we honor those who died while serving their country

NAVSEA WARFARE CENTERS DAHLGREN

NSWCDD/MP-09/33

Statement A: Approved for public release; distribution is unlimited