



## 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 fulfill 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?

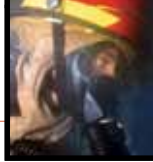
The successful use of most munitions depends on the controlled and predictable release of stored chemical energy. Substances and mixtures of substances that are employed for their energetic properties can be found in the explosives in warheads, propellants, and a variety of devices that use propellants 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.

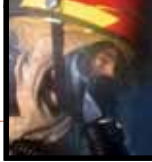
The MIL-STD-882 analysis sequence is designed to provide the safety engineer with a structured approach to discovering, documenting, and developing mitigations for the hazards inherent in a system. However, when focusing on the explosive component of the system, special consideration must be given to 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.

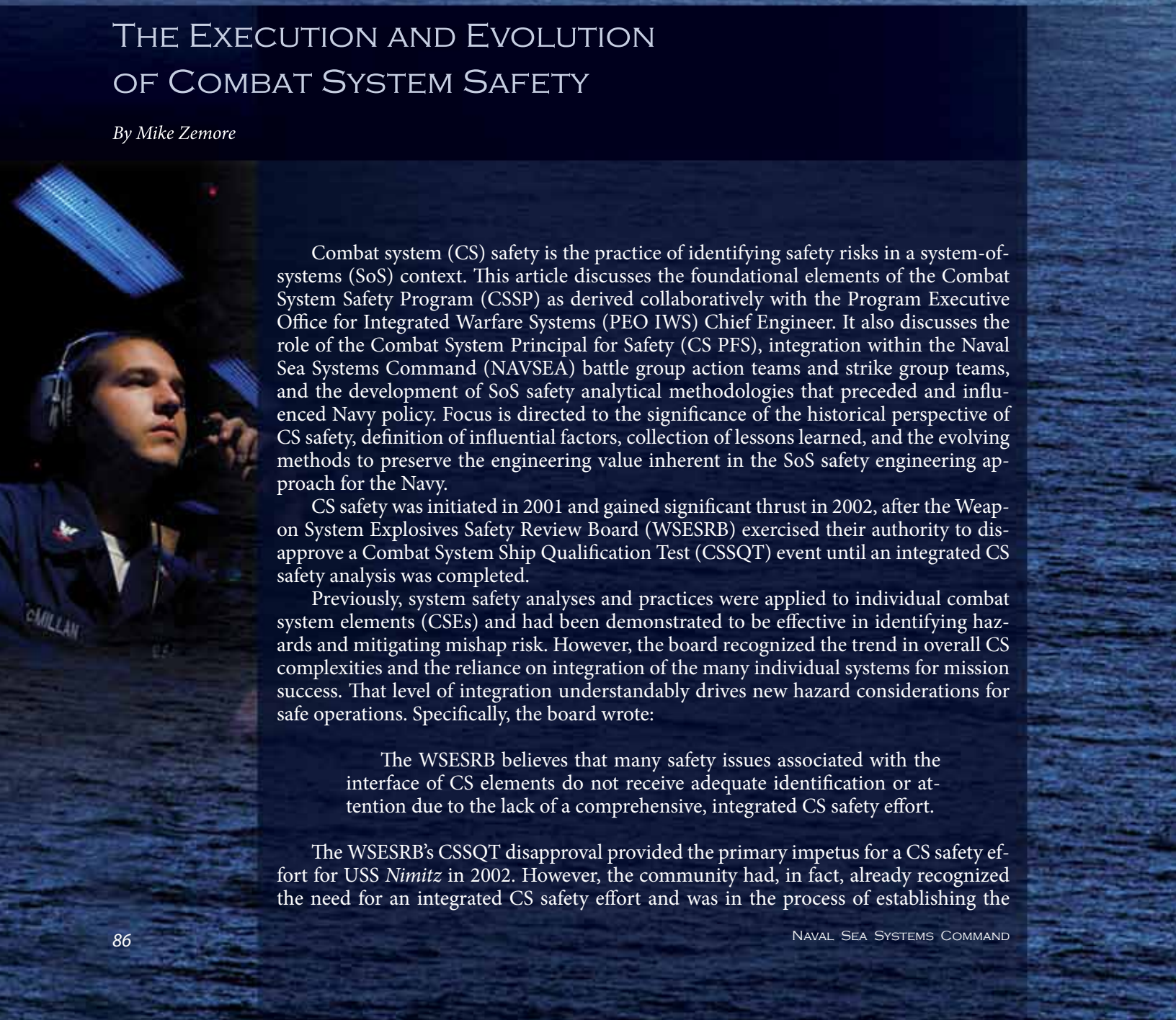







## THE EXECUTION AND EVOLUTION OF COMBAT SYSTEM SAFETY

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)

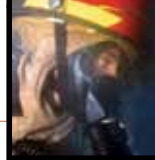
foundational elements for that evolution. By 2001, the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) had begun working with Program Executive Office for Expeditionary Warfare (PEO EXW) and PEO carriers to establish an overarching system safety role for aircraft carriers and amphibious assault 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, NSWCCD 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:

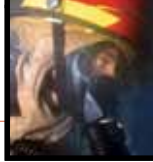
- Provide safety leadership for the Combat System Safety Integrated Product Team (IPT) for Strike Groups/Action teams
- Provide a CS Safety point of contact (POC) with NAVSEA 06 concerning the safety of CS configurations certification

- 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

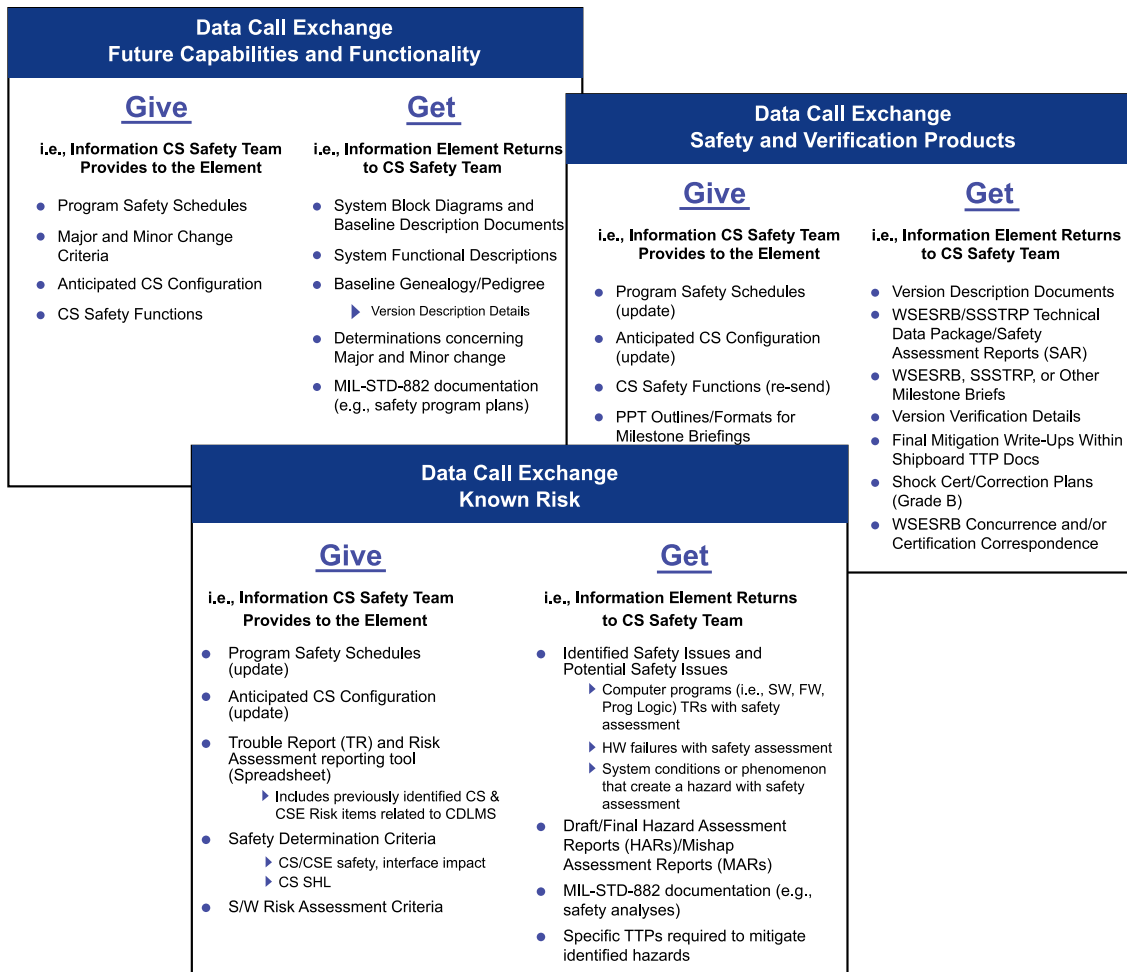


Figure 1. Combat System Safety Data Call Exchange



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

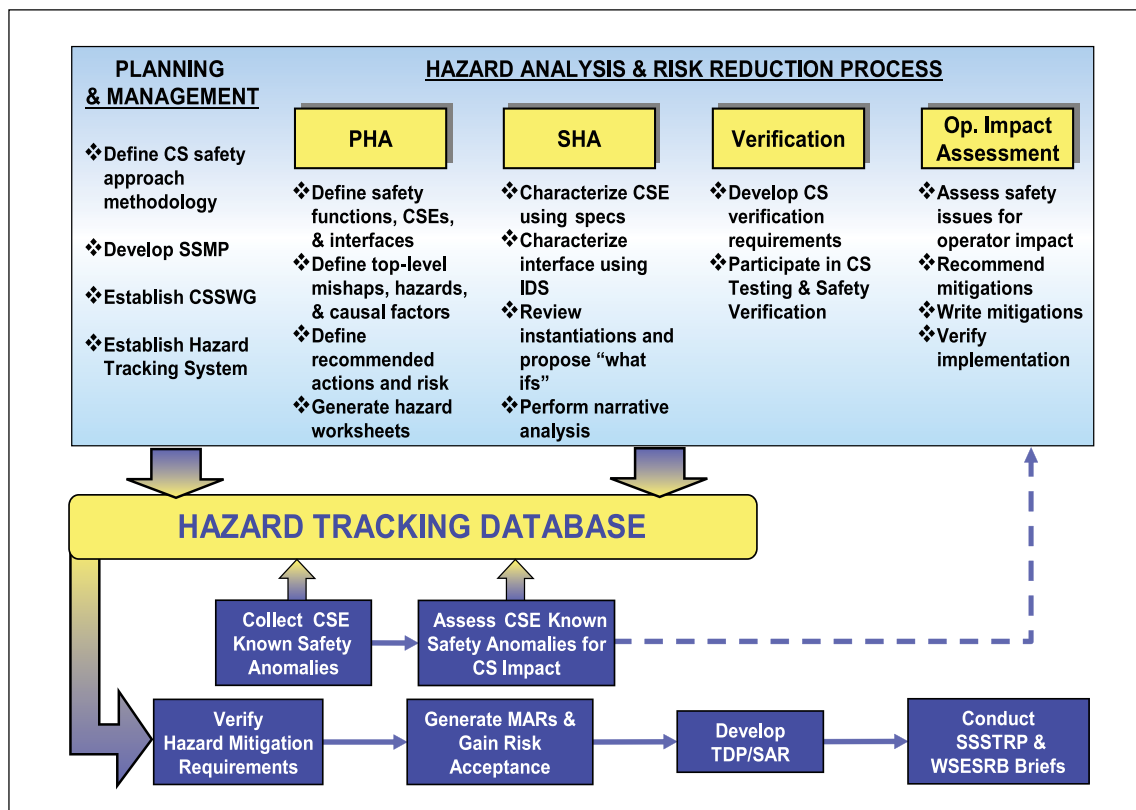


Figure 1. Combat System Safety Process



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

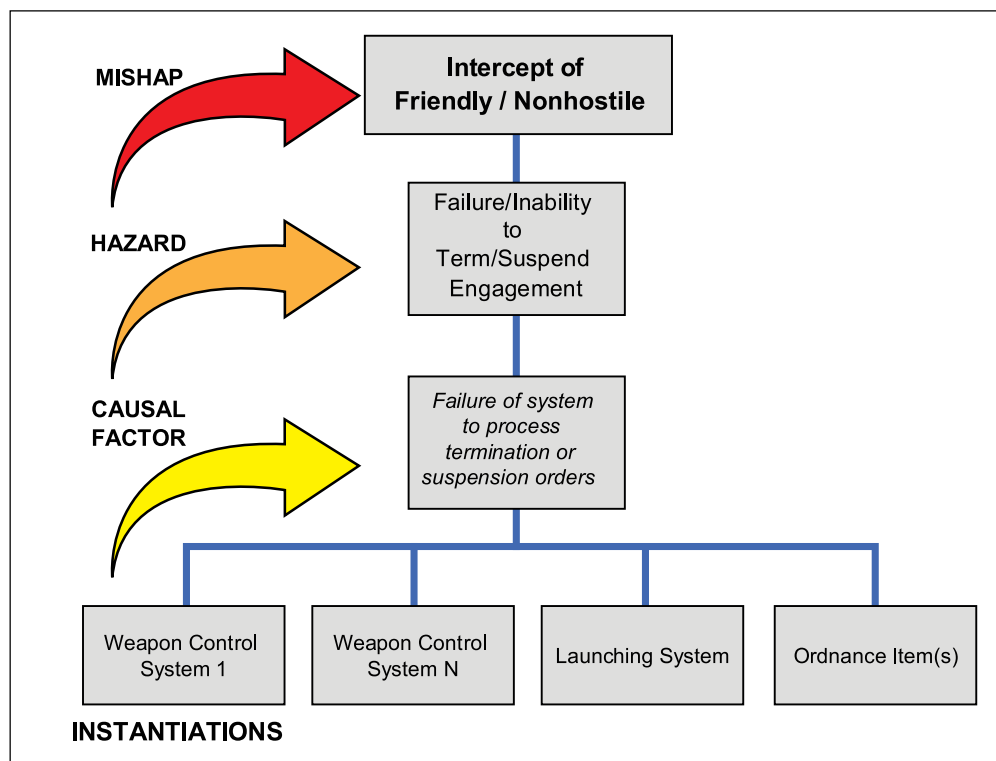
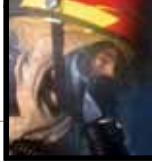


Figure 2. Concept Diagram of System Hazard Analysis



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
<b>HIGH</b>	<ul style="list-style-type: none"> <li>– <b>A software implementation or software design defect that:</b> <ul style="list-style-type: none"> <li>• Leads directly to a catastrophic or critical mishap, or</li> <li>• Subjects the system to a single point (1) failure that would lead to a catastrophic or critical mishap</li> </ul> </li> </ul>
<b>SERIOUS</b>	<ul style="list-style-type: none"> <li>– <b>A software implementation or software design defect that:</b> <ul style="list-style-type: none"> <li>• Influences a catastrophic or critical mishap, but where two (2) independent functioning interlocks or human actions remain, or</li> <li>• Leads directly to a marginal or negligible mishap</li> </ul> </li> </ul>
<b>MEDIUM</b>	<ul style="list-style-type: none"> <li>– <b>A software implementation or software design defect that:</b> <ul style="list-style-type: none"> <li>• Influences a catastrophic or critical mishap, but where three (3) independent functioning interlocks or human actions remain, or</li> <li>• Influences a marginal or negligible mishap, reducing the system to a single point (1) failure</li> </ul> </li> </ul>
<b>LOW</b>	<ul style="list-style-type: none"> <li>– <b>A software implementation or software design defect that:</b> <ul style="list-style-type: none"> <li>• Influences a catastrophic or critical mishap, but four (4) or more independent functioning interlocks or human actions remain</li> <li>• Would be a causal factor for a marginal or negligible mishap, but two (2) independent functioning interlocks or human actions remain</li> </ul> </li> <li>– <b>A software degradation of a safety-critical function that is not categorized as high, serious, or medium safety risk</b></li> <li>– <b>A requirement that, if implemented, would negatively impact safety, however code is implemented safely</b></li> </ul>

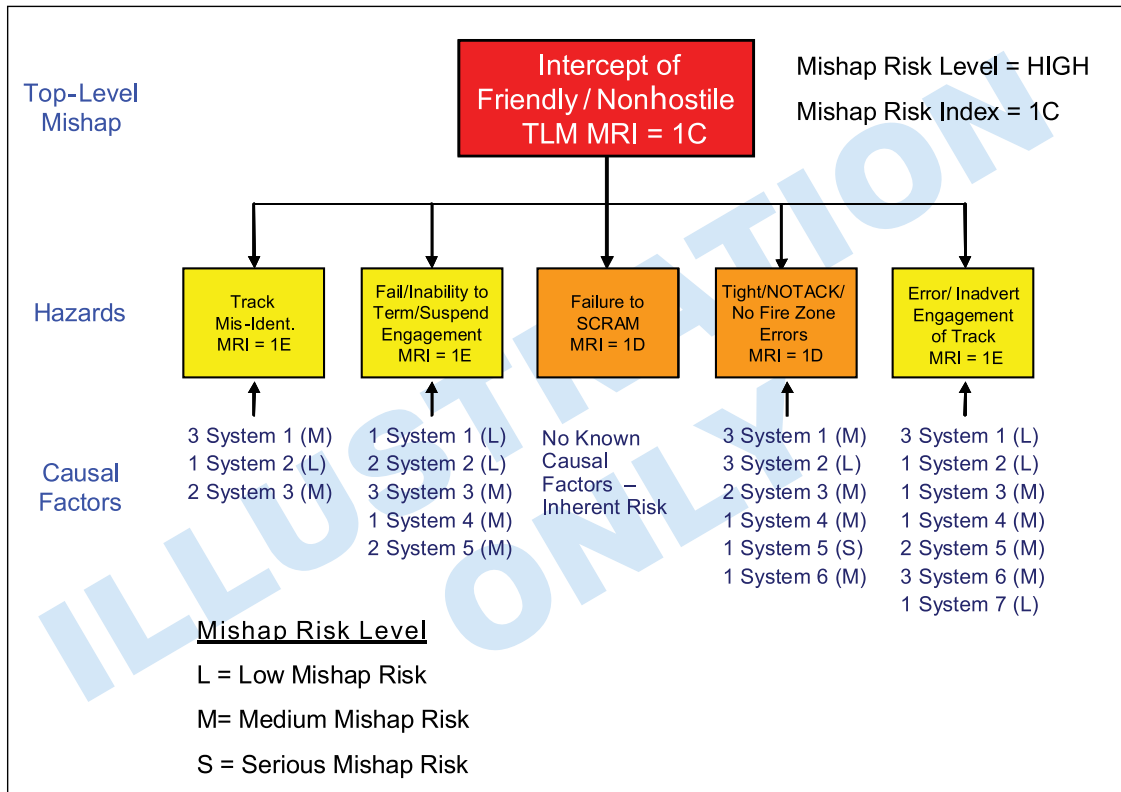
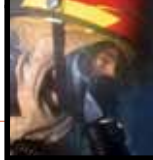


Figure 3. CS Mishap Risk Assessment

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**)
- *Erroneous/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:

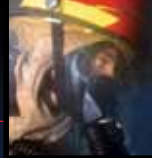
- End-to-end CS safety assessment
- Enhanced technical communication via Navy-wide CSSWG meetings
- Coordinated hazard risk assessments and reporting mechanisms
- Capability for providing insight into CS level issues at Mission Readiness Reviews, Mission Control Panels, CS Certification Panels, and other 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
<b>A</b> FREQUENT		HIGH RISK	HIGH RISK	SERIOUS RISK	MEDIUM RISK
<b>B</b> PROBABLE		HIGH RISK	HIGH RISK	SERIOUS RISK	MEDIUM RISK
<b>C</b> OCCASIONAL		HIGH RISK	SERIOUS RISK	MEDIUM RISK	LOW RISK
<b>D</b> REMOTE		SERIOUS RISK	MEDIUM RISK	MEDIUM RISK	LOW RISK
<b>E</b> 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 NSWCCD'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

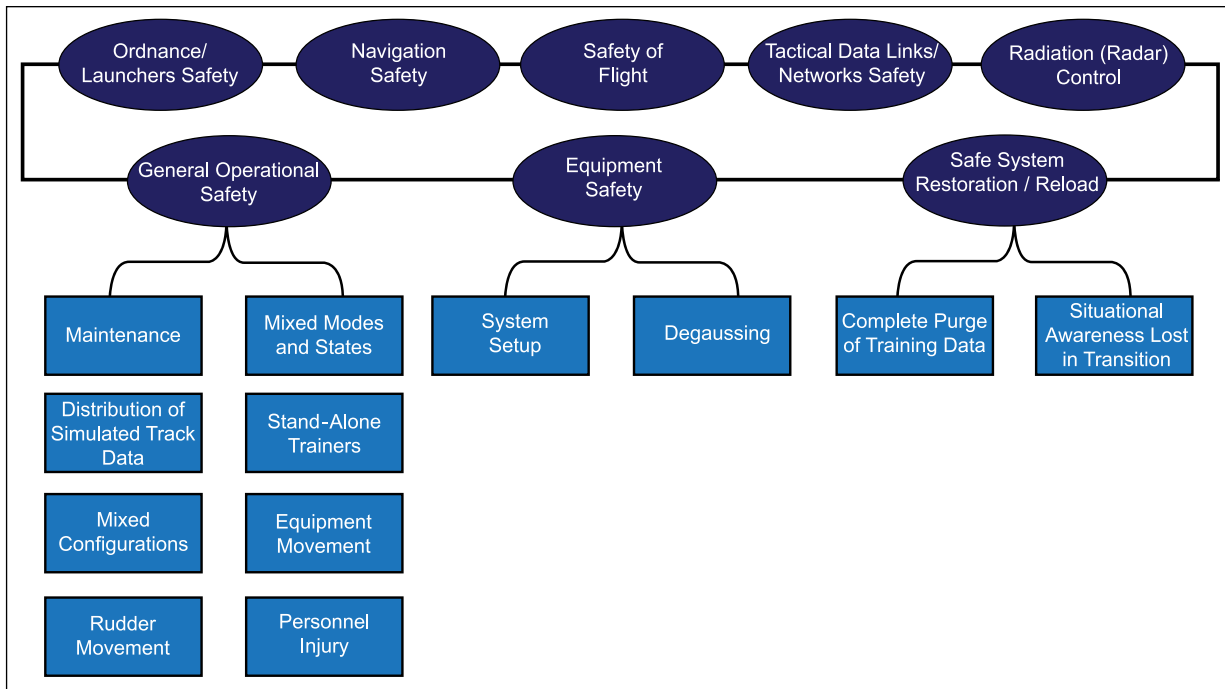
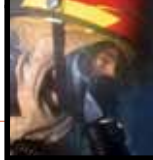


Figure 1. Primary Safety Concerns

- 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 safing 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  $-45^{\circ}\text{F}$ . By comparison, diesel fuel (1-D) has a flash point of  $100^{\circ}\text{F}$ . 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



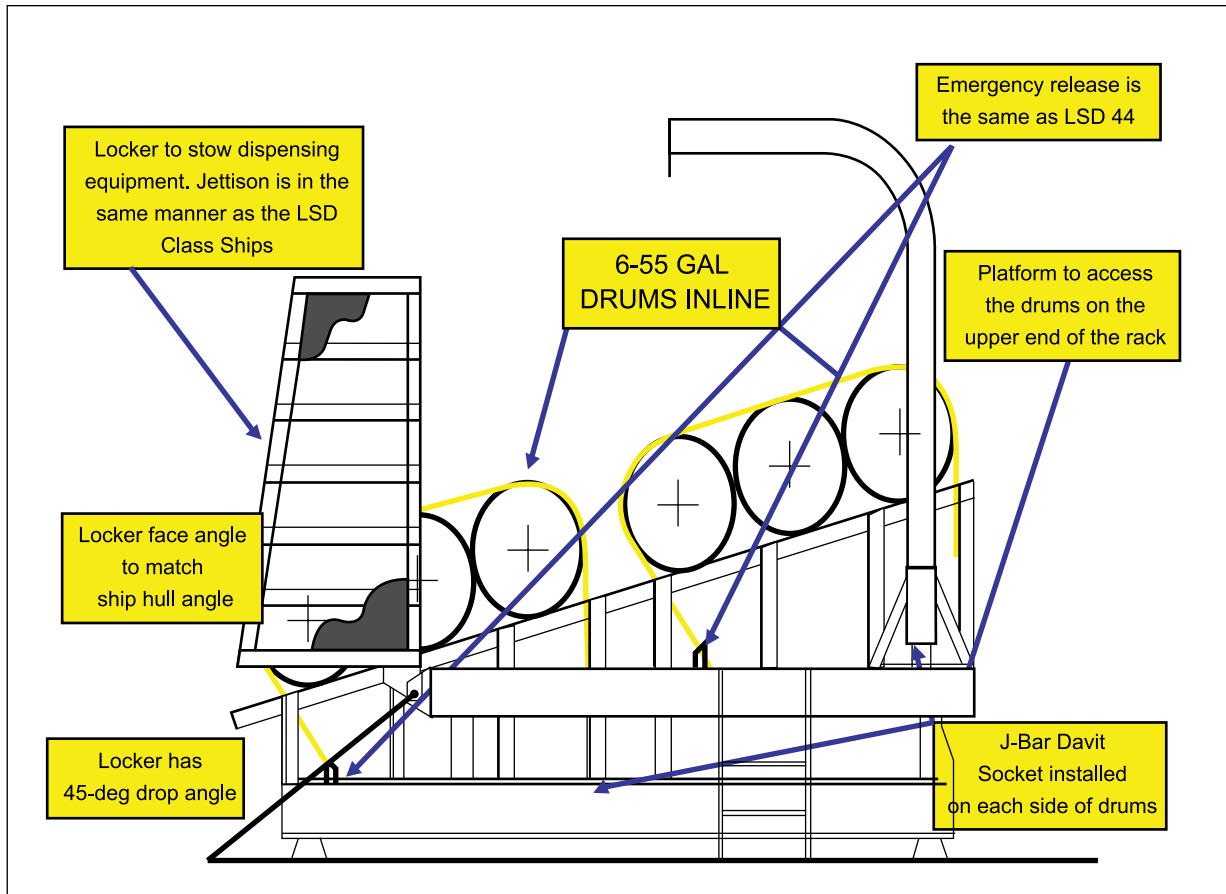
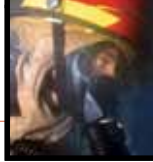


Figure 2. Shipboard MOGAS Storage System Diagram

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

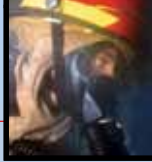
From these analyses, the system safety team determined that the highest risk operation to the ship was transferring bladders and jerry cans within the interior of the ship. Fuel spills that occur during transfer will present explosive vapors and severe fire hazards. It was noted that, along the transfer 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 NSWCCD 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.

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 1. MK 45 Gun FCO Cam

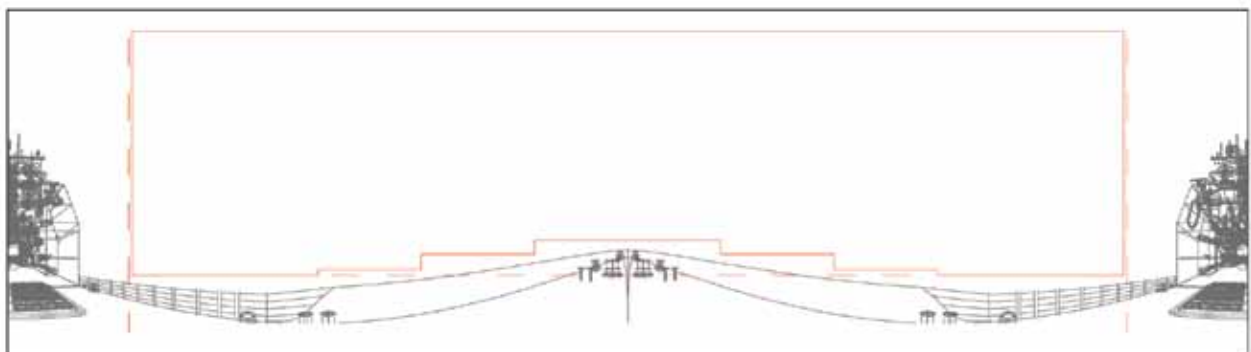
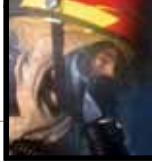


Figure 2. Typical 5-inch/54 Gun FCO Zone

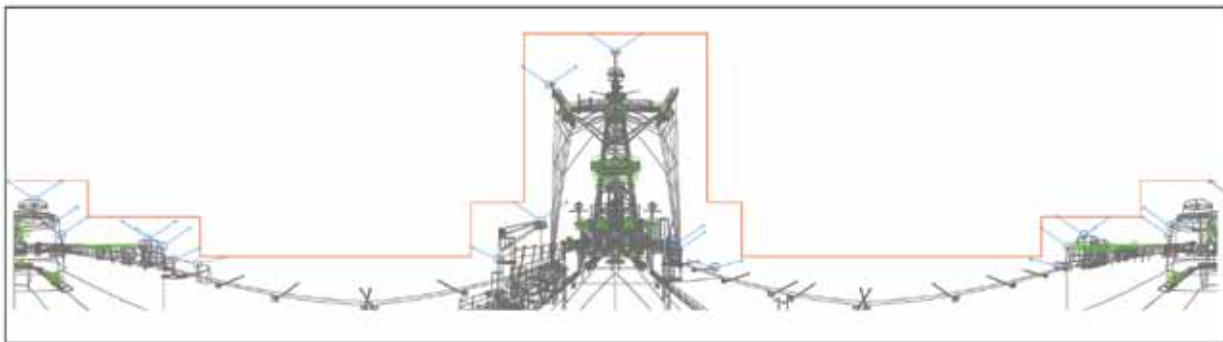


switch is paired with a train switch, and each pair defines a rectangle. Seven of these rectangles define an area where firing is allowed; their overlay defines the overall firing zone. The remaining rectangle defines an area where firing is not allowed and its activation results in an FCO “pop-up” over 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

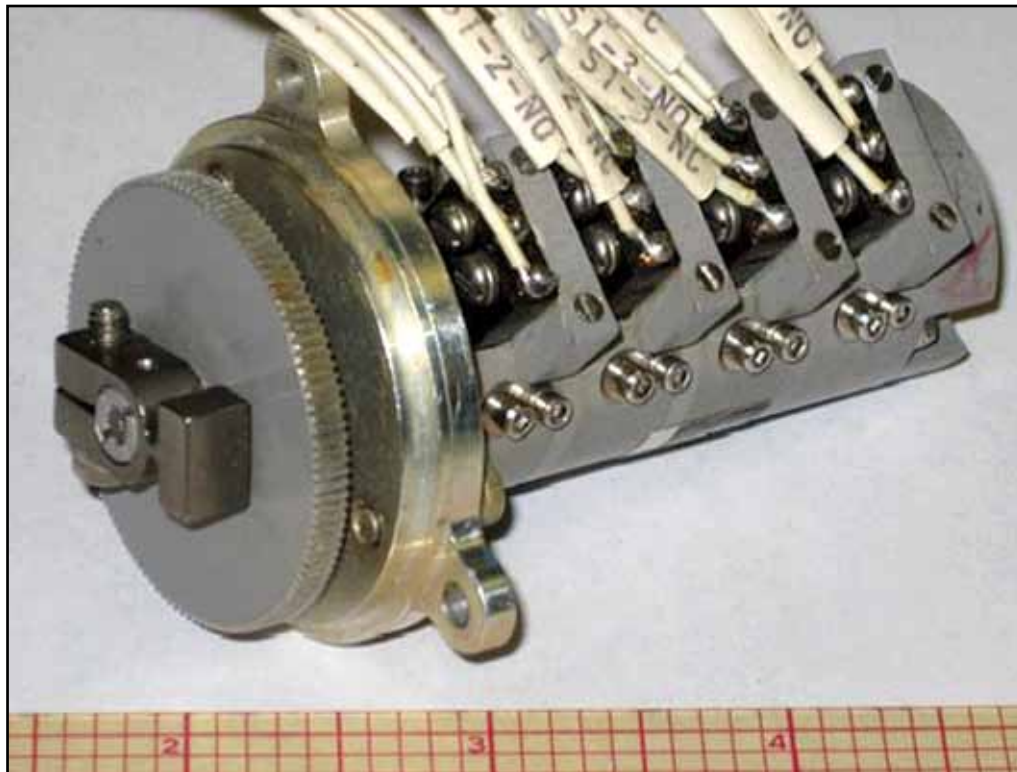


**Figure 4.** Typical 76mm Gun FCO Zone

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.

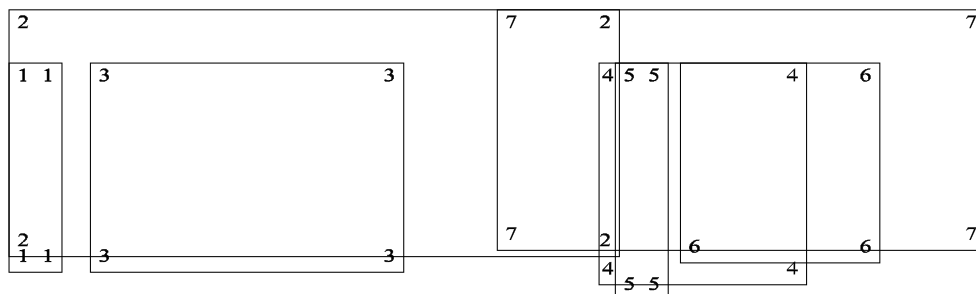
A major step forward in P&FCO zone implementation was achieved in the Rolling Airframe Missile (RAM) launcher. While this system also uses a programmed circuit board, the input file is a table of 256 elevation values in 1.4° train steps. While in earlier systems the number of steps in the FCO zone design 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



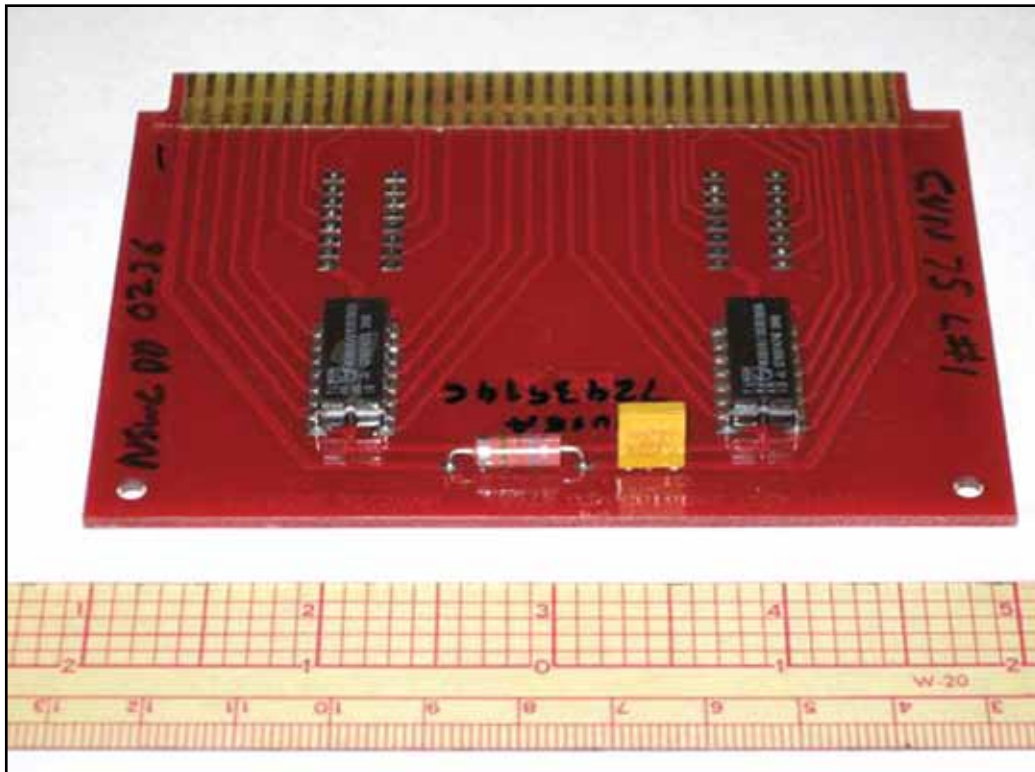


Figure 8. NSSMS FCO Circuit Card

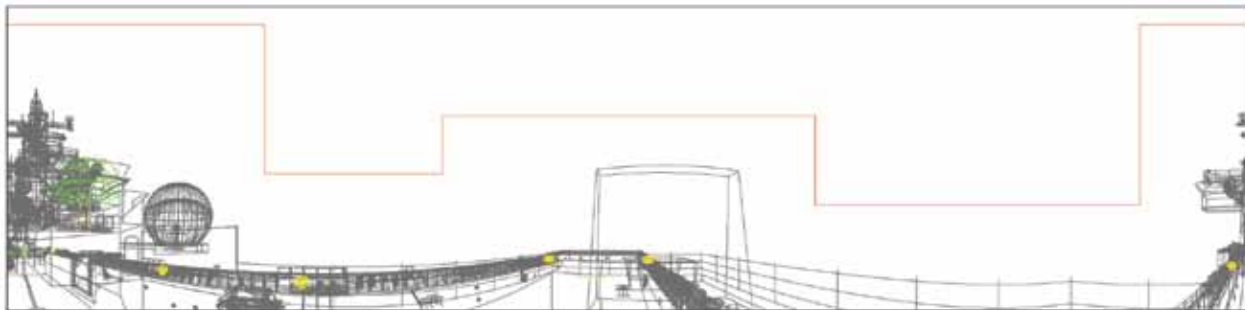


Figure 9. Typical NSSMS FCO Zone

RAM. In fact, the mechanics of launcher motion is the limiting factor in zone design, and steps as small as  $5.6^\circ$  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  $1.4^\circ$ . 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

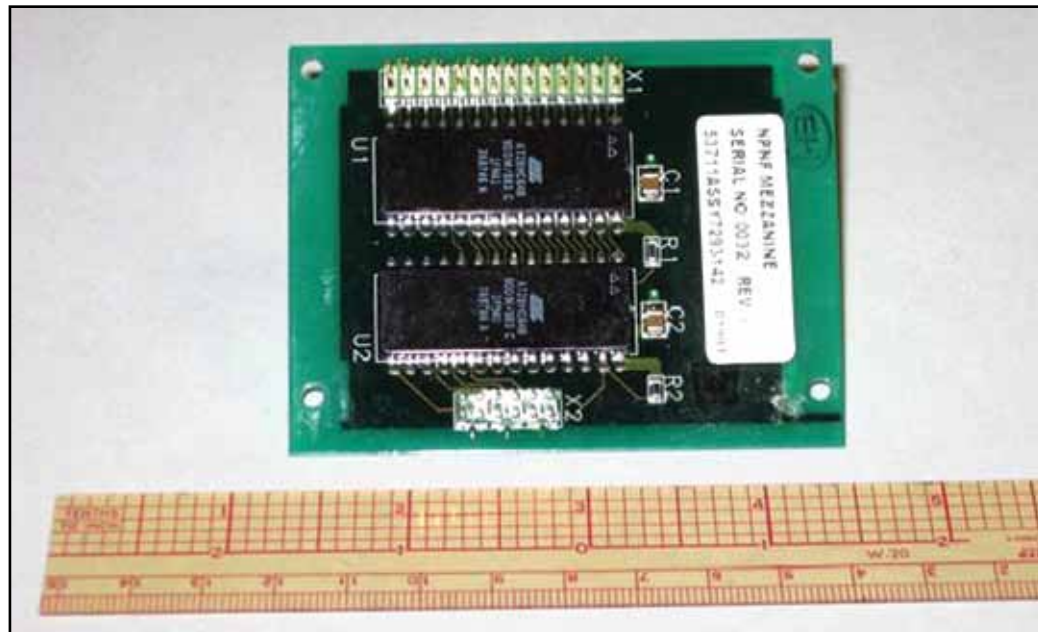


Figure 10. RAM P&FCO Card

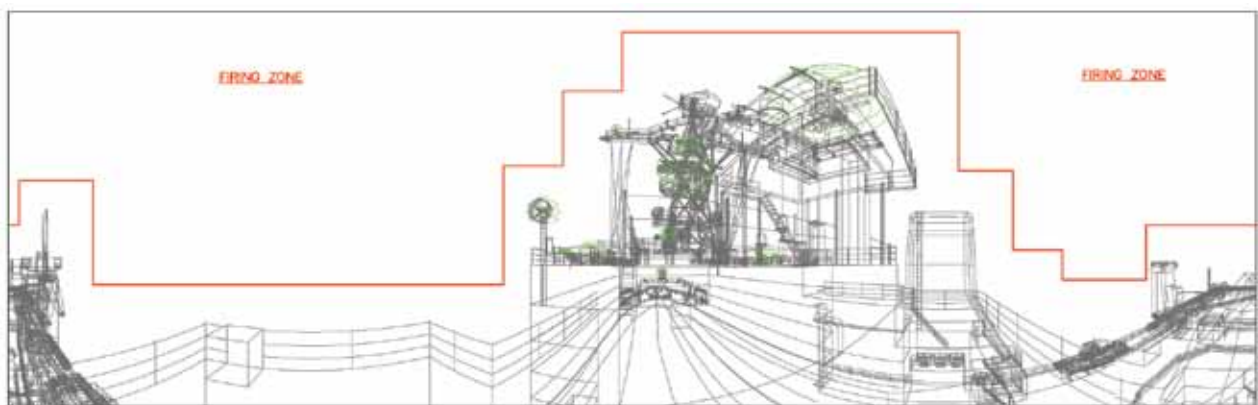


Figure 11. Typical RAM P&FCO Zone

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

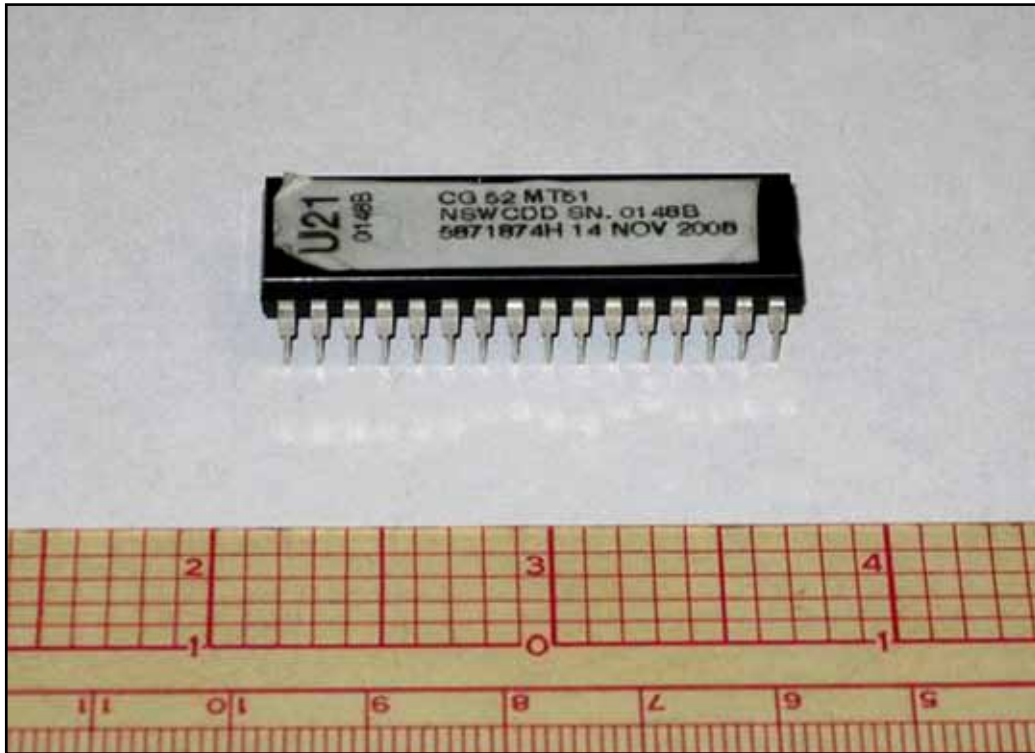
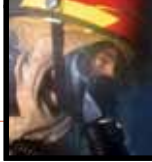


Figure 12. Computer Chip for Implementing 5-inch/62 Gun FCO Zone

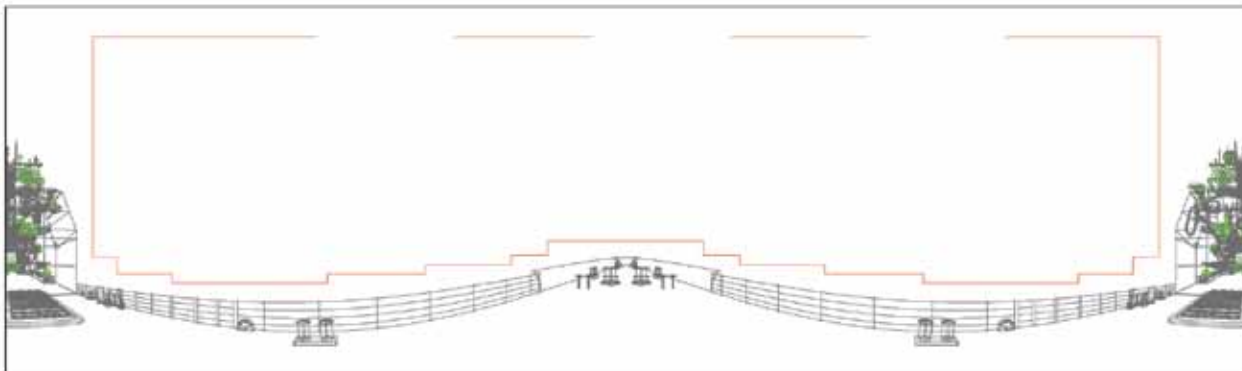


Figure 13. Typical 5-inch/62 Gun FCO Zone

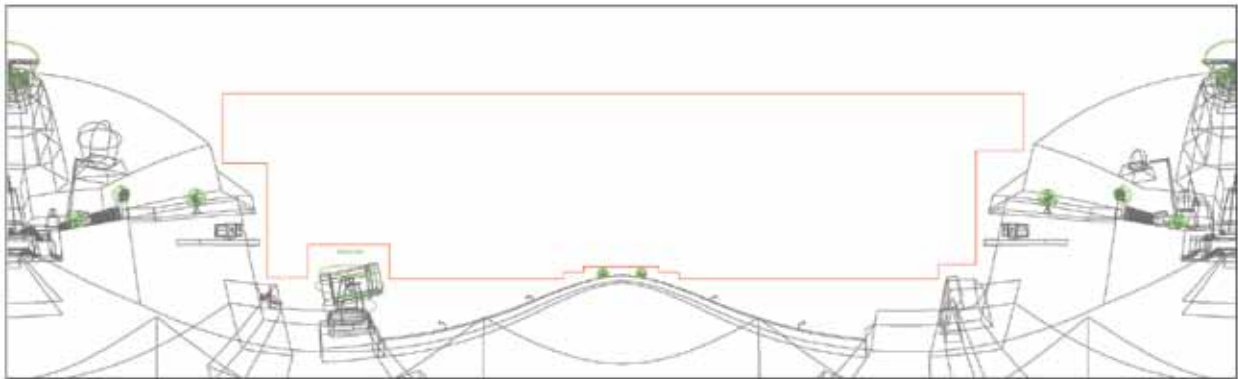


across the ship class, but this goal conflicts with the staggered implementation of topside changes. Experience shows that FCO design needs to be hull-specific. Indications are that software changes are being contemplated that would keep FCO zone information separate from the compiled portion of the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

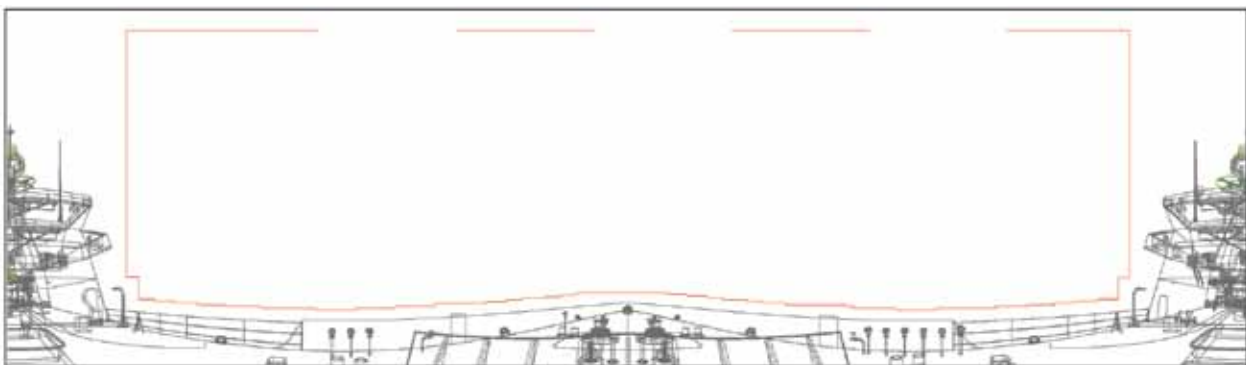
An example of a more flexible approach is provided by the Mk 110 57mm gun, found on the Littoral Combat Ship (LCS)-class ships and the WMSL 750-class Coast Guard cutter. The P&FCO zone information for this gun is uploaded as adaptation data to the GCS using a dedicated laptop and connector. The P&FCO 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. NSWCCD 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 (MTRV)



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.

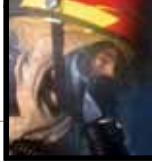
As an Army project, FSEP follows a different path than Gunslinger. The Dahlgren PFS performs the same basic safety tasks as for Gunslinger, but the documentation delivered to the Army is condensed into a Safety Assessment Report and a report of the hazards from the Hazard Tracking Database. Once these 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

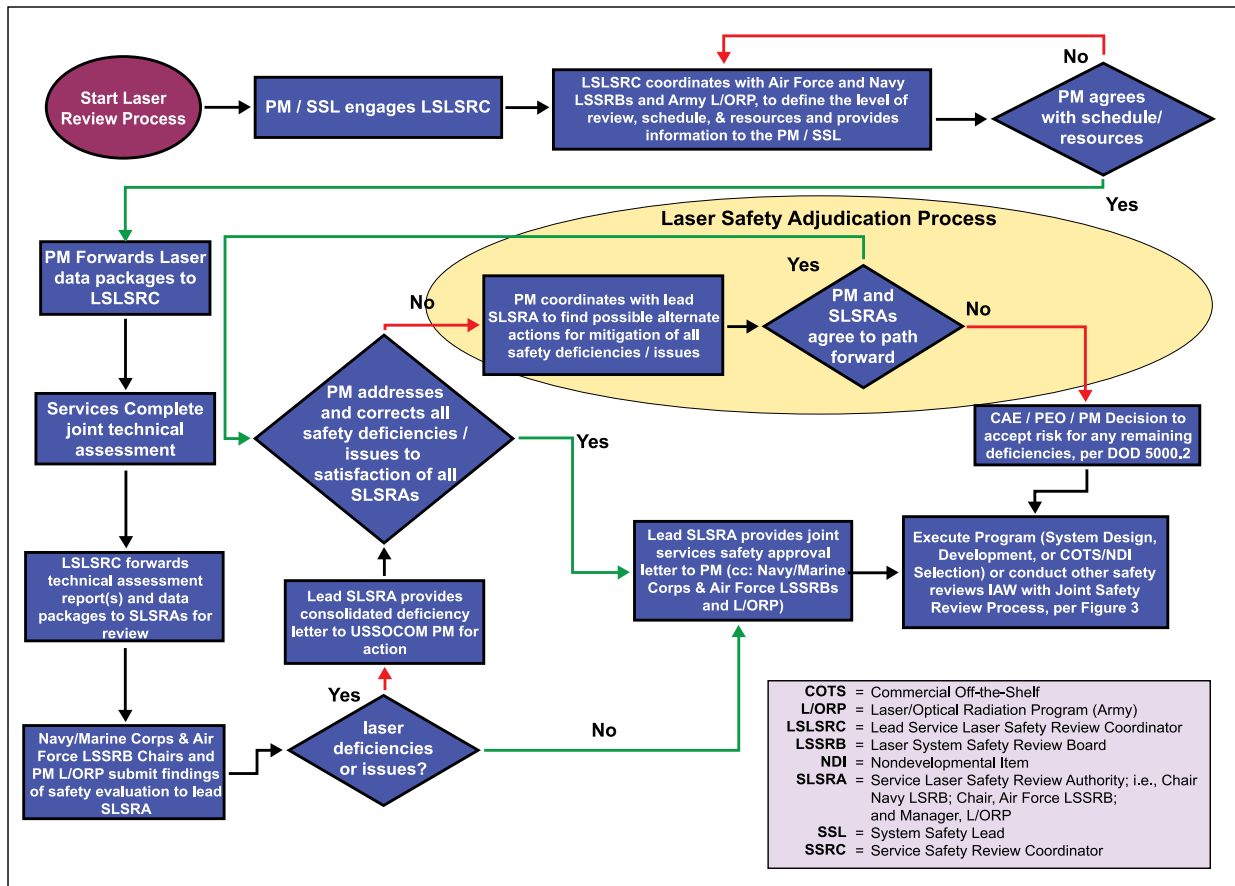


Figure 1. Joint Laser System Safety Review Process

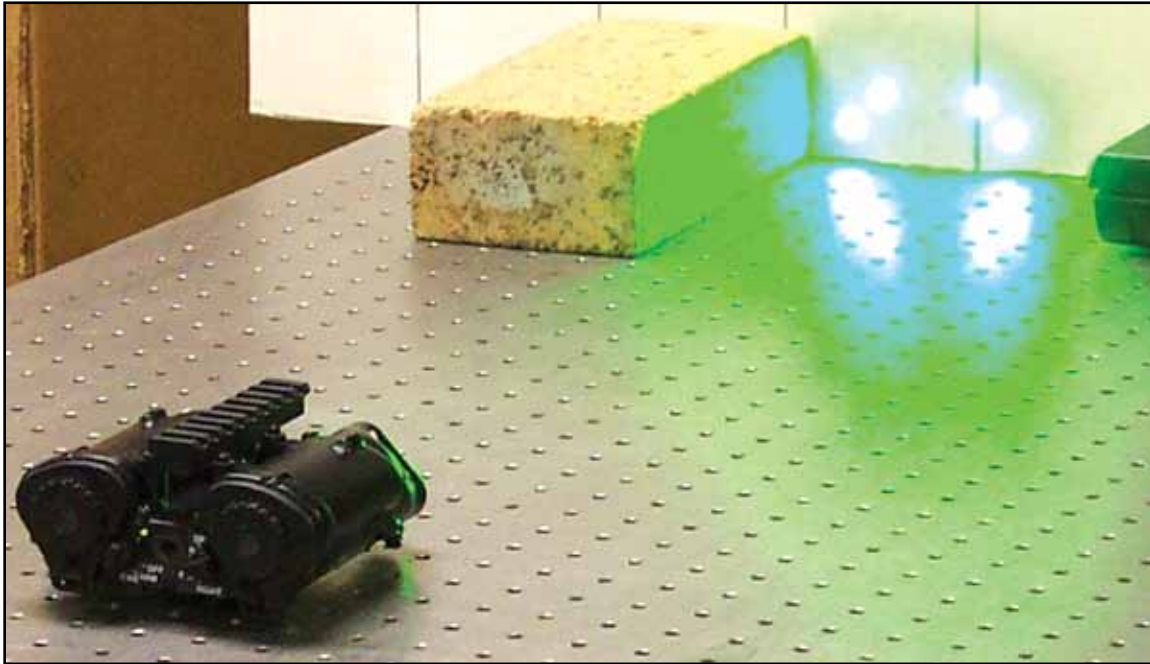


Figure 2. Ghost Laser System Under Evaluation

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







## *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)*







## Fallen Warriors

*Here we honor those who died while serving their country*



NSWCDD/MP-09/33

Statement A: Approved for public release; distribution is unlimited