

## DEPARTMENT OF DEFENSE SAFETY PROGRAM GUIDANCE AND POLICIES FOR THE PRINCIPAL FOR SAFETY (PFS)

By Peggy L. Rogers

### Author's Note:

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

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

### PRINCIPAL FOR SAFETY (PFS)

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



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

### IT’S THE LAW

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

### DIRECTIVES

#### *Department of Defense Directive (DoDD) 5000.1*

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

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

Whether the systems that we work on are weapons or explosives related, they are all required to address safety. As the point person for

safety, the PFS is responsible for guiding the system safety program in the development and implementation of a System Safety Program Plan that will address all aspects of the system life cycle and, thereby, all aspects of the acquisition process.

#### *Department of Defense Instruction (DoDI) 5000.02*

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

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

### INSTRUCTIONS

#### *Secretary of the Navy Instruction (SECNAVINST) 5000.2C*

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

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

#### *SECNAVINST 5100.10H*

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





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

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

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

#### *OPNAVINST 5100.24B*

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

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

#### *OPNAVINST 8000.16C*

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

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

#### *OPNAVINST 8020.14*

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

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

#### *Naval Sea Systems Command (NAVSEA) OP 4*

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

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

#### *Naval Sea Systems Command Instruction (NAVSEAINST) 5000.8*

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

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

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

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

#### *NAVSEAINST 5100.12A*

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

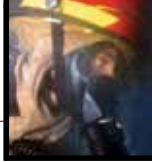
Enclosure (1) of this instruction provides guidance to the PFS on tailoring system safety program requirements, but the PFS should be cautioned on the outdated concepts and requirements recommended. The PFS should read this document in its entirety. It is an easy read and helps distinguish, for the PFS,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

#### *NAVSEAINST 8020.6E*

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







### *NAVSEAINST 9410.2*

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

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

## GUIDANCE AND POLICY

### *System Safety Program Requirements*

MIL-STD-882C, *System Safety Program Requirements*, dated 19 January 1993, is the overarching document that guides government and contractor safety programs. It specifies the analytical tasks that should be performed when

conducting a comprehensive safety program. MIL-STD-882C does a good job of guiding the safety team on what needs to be done, but the currently approved version, 882D, is lacking in the “how-to” area for generation of the safety analysis products.

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

### *Weapon System Safety Guidelines Handbook*

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



#### *WSESRB Interactive Safety Environment (WISE)*

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

#### *Software System Safety Handbook*

The Joint Software System Safety Committee released the *Software System Safety Handbook* in December 1999. The generation of this handbook was a joint effort developed by the Joint Services Computer Resources Management Group, the U.S. Navy, the U.S. Army, and the U.S. Air Force. The handbook was developed to “provide management and engineering guidelines to achieve a reasonable level of

assurance that software will execute within the system context with an acceptable level of safety risk.”

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

#### CONCLUSION

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





## TRAINING THE SYSTEMS SAFETY ENGINEER

By Mike Zemore and Etienne (Steve) Boscovitch

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

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

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

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



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

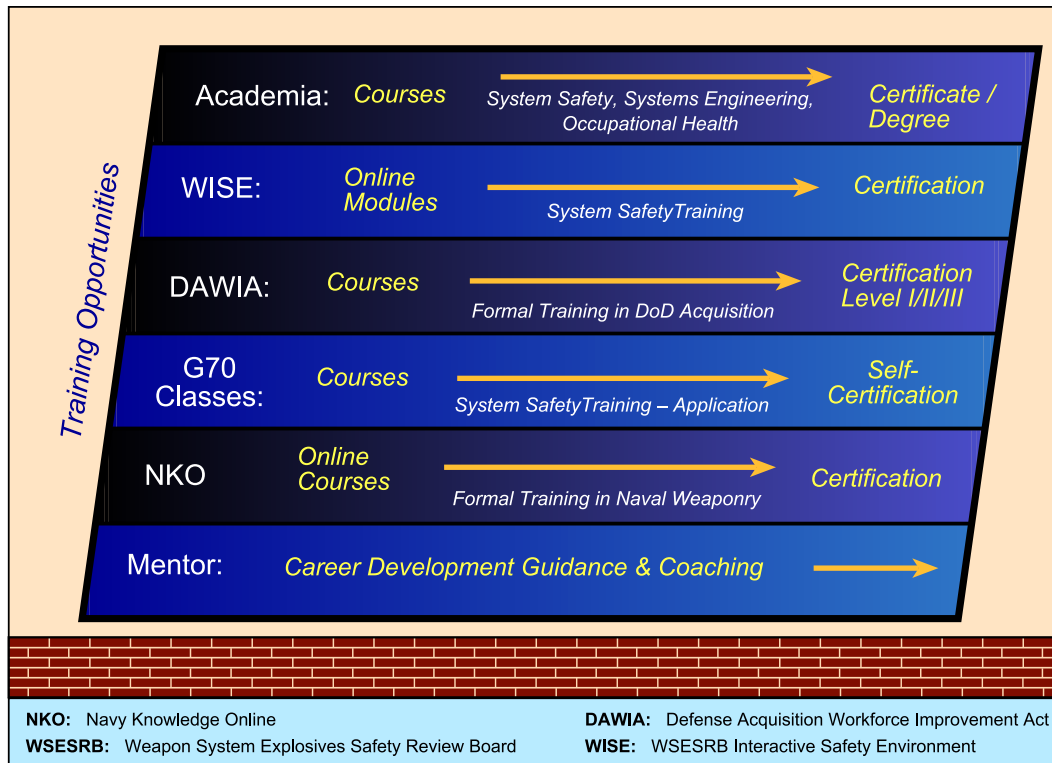
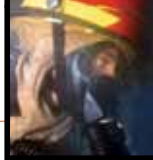
- Gun systems
- Launchers
- Missile systems
- United States Marine Corps (USMC) weapons
- Integrated surface ship combat systems
- Surface ship topside pointing and firing zones
- Lasers
- Unmanned systems
- Ground platforms
- Integrated surface ship platforms

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

combined with sound systems safety engineering methods, ensure that professionals can effectively support the customers and the goal of producing and deploying safe systems for the fleet.

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





**Figure 1.** Training Opportunities for the Safety Practitioner

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

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

Delving down to specific combat system components, safety practitioners can access specific “A” schools and community-of-practice (CoP) lessons to acquire detailed understanding of system

designs and functionality. For example, if a safety analysis is intended for a radar system, the practitioner can access basic radar systems theory to better understand radar functionality and then follow up with CoP lessons to understand design and use details. The CoP also provides access to subject matter experts (SMEs), the mechanism for electronic discussions, support, solutions, and lessons learned.

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

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






—			"A" Schools Page
	+		Apprentice Technical (ET) A CoP
	+		Apprentice Technical (FC) A CoP
	+		Apprentice Technical (GM/TM) A CoP
	+		STG A School CoP

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

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

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

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

Beyond traditional degree programs, there are several opportunities for the safety practitioner to gain relevant training within the academic environment. Historically, training in this area has focused on Occupational Safety and Health Administration (OSHA) requirements. While extremely important, OSHA-specific training does not encompass the essence of systems safety engineering as applied to acquisition programs and weapon system safety. Fortunately, there has been

movement over the years to offer expanded curriculums that include systems safety engineering methods. Obviously, safety training—whether OSHA or systems safety engineering focused—can enhance the effort and add value for the practitioner, customer, and user. A number of universities (see Figure 3) now offer safety-related courses, certificates, and degrees. Examples are:

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

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





Figure 3. Advanced Studies

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

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

Developed by EG&G under the guidance and direction of the NOSSA, the WISE program provides open access as a centralized repository of safety knowledge and training as an efficient means of learning and understanding system safety. Each WISE training module is designed to increase knowledge and comprehension of system

safety processes for application within an acquisition program. The E-Learning capability comes without cost to the safety practitioner or sponsoring program office. This approach supports the initiative to facilitate training and use of consistent system safety methodologies within the Department of the Navy (DON) with minimal or no impact to program cost or schedule. The expectation is that this investment—applied across DON programs—will enhance the safety of the systems deployed and ease the process for WSESRB review. A snapshot of the WISE home page is shown as Figure 4.

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

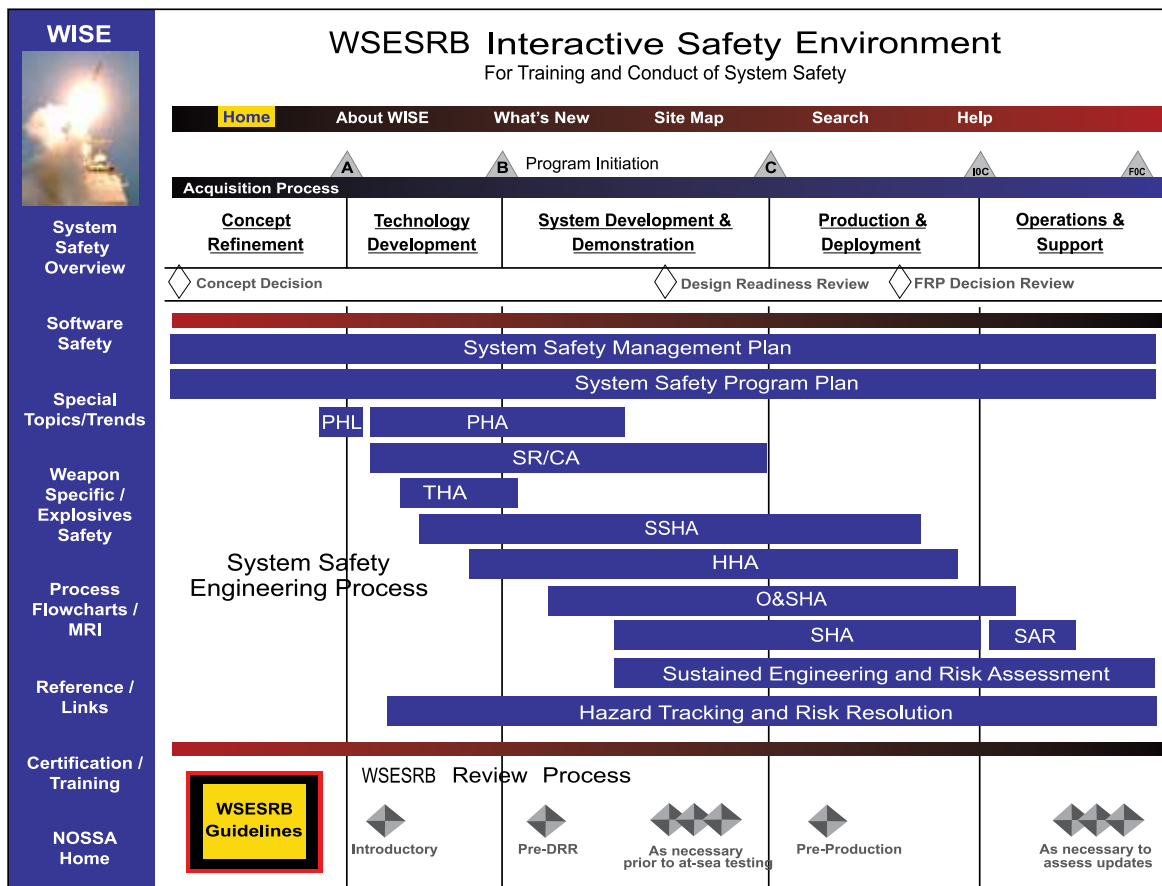
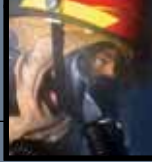


Figure 4. WISE Homepage





## ESTABLISHING AND TRAINING BEST PRACTICES IN SYSTEMS SAFETY ENGINEERING

By Robert C. Heflin Jr.

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

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

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



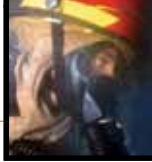
analysis process as ideally practiced and identified 34 separate areas of focus that participants concurred are key elements in performing consistent, high-quality safety analysis. While most of these areas fell within the technical analysis process itself, others were associated more closely with associated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

Addressing the issue thus necessitated a two-pronged approach. First, safety analysis methodologies within G70 needed to be standardized, and second, a process for training personnel in those methodologies on a consistent basis needed to be formalized. To accomplish the former, G70

embarked on a series of Lean events aimed at developing a concise and consistent process for safety analysis implementation and documentation. Over a 24-month period, individual events were conducted for each of the 34 identified focus areas. Each event included personnel from each of the three branches within the division, as well as contractor support personnel and customer representatives wherever possible. These events reviewed existing methodologies for performing and/or documenting different major elements within the overall system safety process, and established and documented a single best-practice methodology for each of those elements. This best practice was accepted as part of the official consolidated G70 safety analysis process.

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





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

To accomplish the short-term goal of providing a high-level foundation of systems and system safety knowledge, the WFD team developed a curriculum consisting of six classes. These six classes focused on introducing the students to U.S. Navy and U.S. Marine Corps systems, describing system safety concepts at a high level and detailing the overall system safety analysis process as designed for practice within G70. Each class was offered on multiple dates and times over a 6-month period to the existing workforce and planned for

further future periodic iterations to account for workforce expansion and turnover. Attendance was mandatory for some of the classes and voluntary for others, as necessitated by the importance of the material being presented and the topical familiarity of individual safety engineers.

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

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



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

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

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

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





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

Photo Courtesy of U.S. Navy

## NAVY SAFETY REVIEW BOARDS: WSESRB, SSSTRP, AND FISTRP

By Mary Ellen Caro, David Shampine, and Jack Waller

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


—Robert C. Heflin



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

Photo Courtesy of U.S. Navy





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

Photo Courtesy of U.S. Navy



**(WSESRB)**

Weapon System Explosives Safety  
Review Board

*By Mary Ellen Caro*

**(SSSTRP)**

Software System Safety Technical  
Review Panel

*By David Shampine*

**(FISTRP)**

Fuze and Initiation System  
Technical Review Panel

*By Jack Waller*



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

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



## THE NAVY'S WEAPON SYSTEM EXPLOSIVES SAFETY REVIEW BOARD (WSESRB)

*By Mary Ellen Caro*





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

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

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

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

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

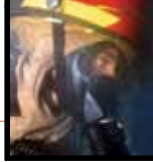


Early engagement of the WSESRB review process benefits the DON, as well as the acquisition program manager (PM). Early incorporation of safety requirements and allocation of resources for safety analysis and testing allows a program to plan and execute the weapon system safety program and uncover safety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

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

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





Radiation to Ordnance (HERO) and electrostatic discharge

- Temperature and vibration exposures
- Shipboard shock and packaging tests

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

Weapon acquisition programs come before the WSESRB at several points in their acquisition life cycle to obtain Board concurrence before proceeding to the next stage of development. Normally, there is an introductory review upon a contract award to assess the planned safety analysis and

testing program. This review can benefit PMs in the early stages of a program acquisition by ensuring the needed testing and analysis are available by the time the program is ready to proceed to production.

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

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

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

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

The WSESRB Secretariat (NOSSA N3) is available to the PMs and program Principals for Safety to coordinate WSESRB reviews. Points of contact have been established for different families of

weapon systems. The Secretariat staff can make recommendations for WSESRB reviews and facilitate scheduling Board meetings. Each review by the WSESRB (or an associate board; i.e., the SSSTRP or FISTRP) requires the submission of a technical data package. The expectations for these data packages are found in NAVSEAINST 8020.6E.

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







## THE NAVY'S SOFTWARE SYSTEM SAFETY TECHNICAL REVIEW PANEL (SSSTRP)

By David Shampine



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

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

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





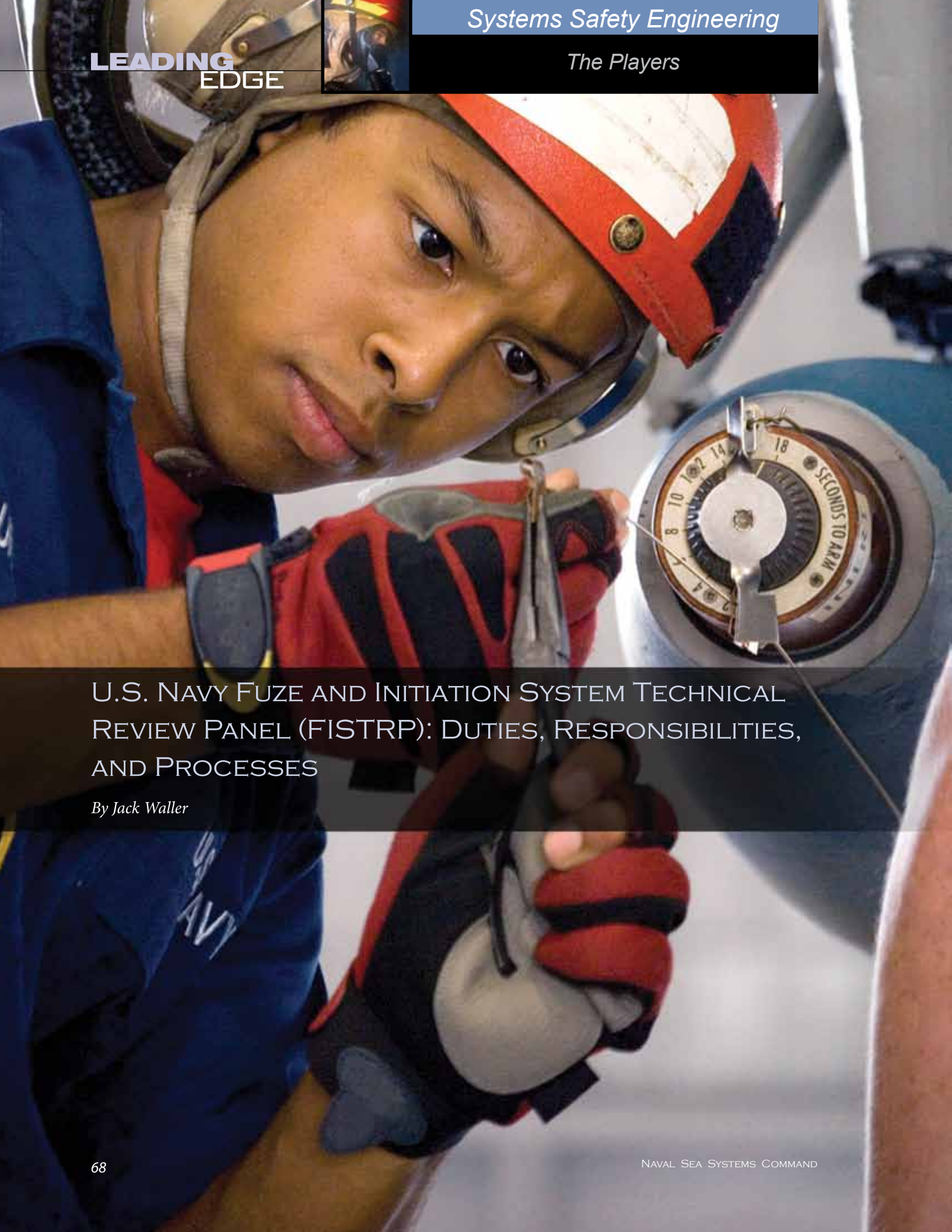
has been developed in accordance with the guidelines established in NAVSEAINST 8020.6E, Enclosure 8. This package is submitted no later than 21 days in advance of the target date for the meeting. Once the TDP is received by the WSESRB, it is reviewed by the NOSSA Point of Contact and the SSSTRP Chairperson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

SSSTRP meetings consist of three parts: the pre-brief, the presentation, and the caucus. The pre-brief is conducted by the Chairperson and is meant to set the tone for the presentation. Any preliminary issues discovered by panel members during the review of the TDP are discussed during the pre-brief and are identified as potential focus points for discussion during the presentation. The presentation is scheduled to last no more than 6 hours, with the program office being responsible for managing both the content and the time to present the safety case for the system under review. The caucus immediately follows the presentation, with its attendance limited to the panel members and the program's Principal for Safety. During this phase of the process, the panel members discuss

the data presented in the data package and during the presentation, and then develop recommendations and action items for the program to aid in improving their safety program. At the end of the meeting, the program representatives are provided with a draft copy of the results of the review, with the caveat that it is not final until approved by the WSESRB.

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

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



U.S. NAVY FUZE AND INITIATION SYSTEM TECHNICAL  
REVIEW PANEL (FISTRP): DUTIES, RESPONSIBILITIES,  
AND PROCESSES

*By Jack Waller*

## INTRODUCTION

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

## PURPOSE AND MEMBERSHIP

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

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

NATO STANAGs:

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

Military Standards:

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

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

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

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

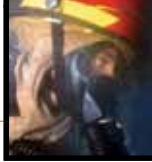
- Fuze design
- Ignition safety device design
- Explosives safety
- Logic systems
- System safety
- Fuze development
- Individual weapon systems design and development

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

## SCOPE

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





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

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

- Identification/description of independent safety features in safety devices, complex

logic devices, or firmware used in the safety logic

- Cut sets and numerical analysis associated with fault tree analysis
- Safety and environmental test programs
- Qualification of explosive devices

### THE REVIEW PROCESS

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



## LESSONS LEARNED

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

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

**Lesson 2:** Design safety evaluations early in the development process are essential to arriving at the most effective design approaches, while

minimizing the impact to the programs involved. Unfortunately, program costs and schedules have been impacted as the result of lack of compliance with design safety requirements. Technology advancements also impact safety design criteria. This is particularly true in the rapidly advancing capabilities of logic devices and their associated tools and implementation. The safety community is examining these impacts and applying lessons learned to the existing safety design criteria documents.

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

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

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

## SUMMARY

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





## JOINT SERVICE WEAPON SAFETY REVIEW PROCESSES

By Robert Gmitter

### BACKGROUND

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

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

### USSOCOM JOINT WEAPON SAFETY REVIEW PROCESS

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

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



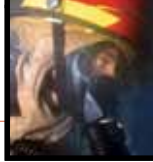


Figure 1. List of U.S. Services' Safety Review Boards and Organizations



Figure 2. USSOCOM Organizations





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

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

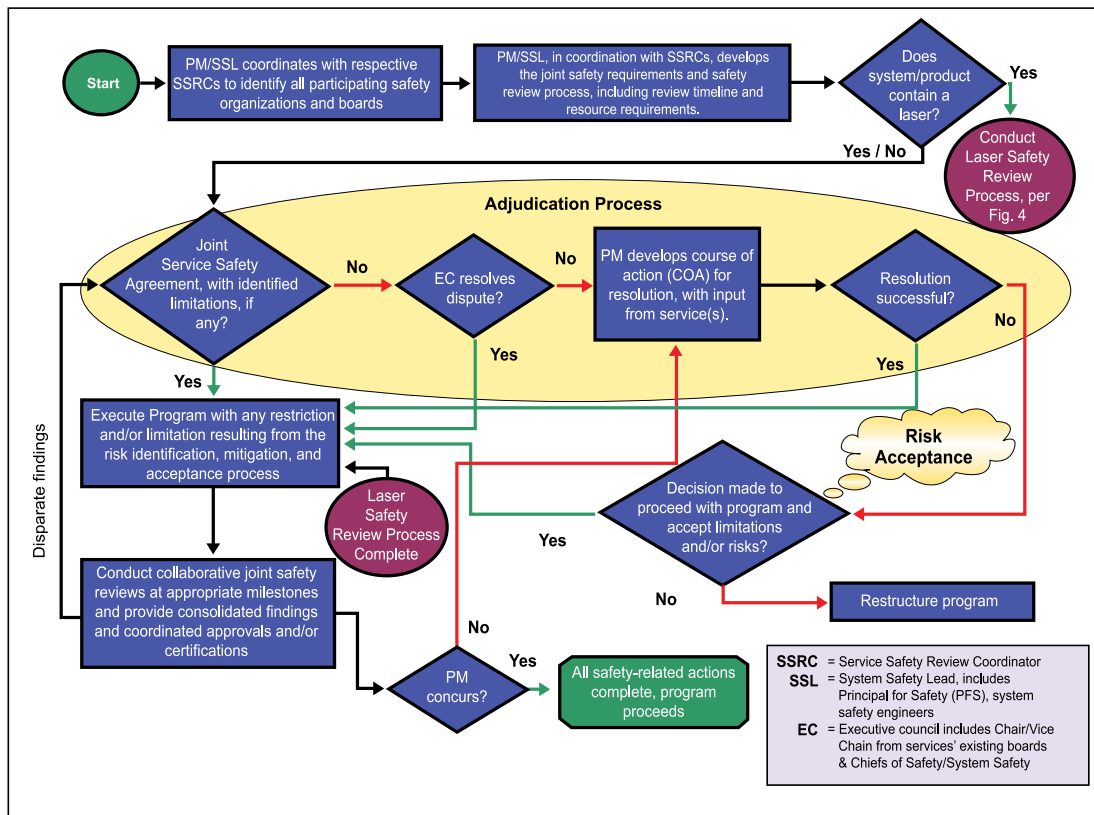
The USSOCOM Joint Weapon Safety Review process consists of seven main elements:

1. Collaborative planning & consolidation of requirements
2. Adjudication of requirements (if necessary)
3. Execution of testing and analysis for system/product
4. Collaborative reviews of testing and analysis results
5. Adjudication of results (if necessary)

6. Identification and documentation of residual risks (if necessary)
7. Acquisition community acceptance of residual risk(s). User representative must provide formal concurrence prior to all **high** and **serious** risk acceptance decisions.

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

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



**Figure 3. Joint Weapon Safety Review Process**

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

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

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

The leadership role in the USSOCOM Joint Weapon Safety Review Process is provided by

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

### USSOCOM JOINT LASER SAFETY REVIEW PROCESS

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

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

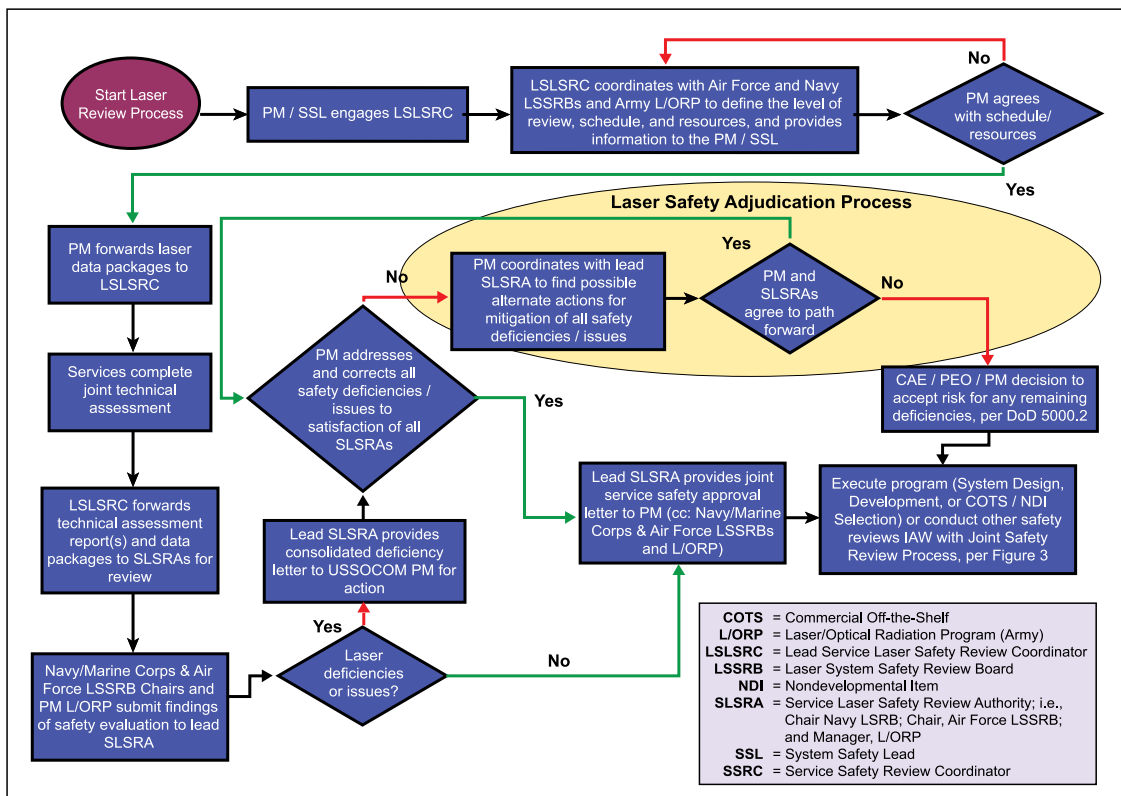


Figure 4. Joint Laser Safety Review Process





### USSOCOM JOINT WEAPON SAFETY AND LASER SAFETY REVIEW SUMMARY

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

### DEPARTMENT OF DEFENSE (DOD) JOINT SERVICE WEAPON AND LASER SAFETY REVIEW PROCESS

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

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

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

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

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





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

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

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

## SUMMARY

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

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

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

## BIBLIOGRAPHY

- Demmick, Michael H., *Integrated System Safety Across the DoD Services: Why, When, & How; a.k.a. Joint Service Weapon Safety Review Process*, Naval Ordnance Safety and Security Activity (NOSSA).  
Kratovil, Edward W., SAIC, 25 June 2008.






## UNITED STATES SPECIAL OPERATIONS COMMAND SYSTEM SAFETY

By Cathi Crabtree

### INTRODUCTION



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

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

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

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

## BACKGROUND

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

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

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

## WAY AHEAD

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

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

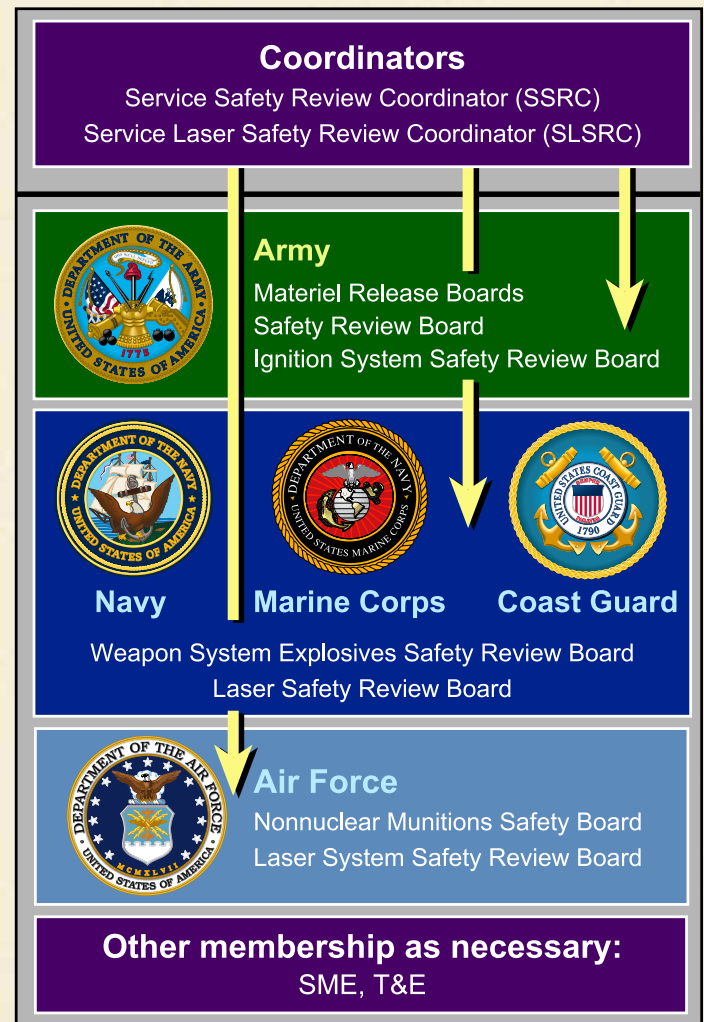


Figure 1. Joint Service Coordination