14 SUBSAFE: An Example of a Successful Safety Program

This book is filled with examples of accidents and of what not to do. One possible conclusion might be that despite our best efforts accidents are inevitable in complex systems. That conclusion would be wrong. Many industries and companies are able to avoid accidents: the nuclear Navy SUBSAFE program is a shining example. By any measure, SUBSAFE has been remarkably successful: In nearly fifty years since the beginning of SUBSAFE, no submarine in the program has been lost.

Looking at a successful safety program and trying to understand why it has been successful can be very instructive.[1] This chapter looks at the history of the program and what it is, and proposes some explanations for its great success. SUBSAFE also provides a good example of most of the principles expounded in this book.

Although SUBSAFE exists in a government and military environment, most of the important components could be translated into the commercial, profit-making world. Also note that the success is not related to small size—there are 40,000 people involved in the U.S. submarine safety program, a large percentage of whom are private contractors and not government employees. Both private and public shipyards are involved. SUBSAFE is distributed over large parts of the United States, although mostly on the coasts (for obvious reasons). Five submarine classes are included, as well as worldwide naval operations.

14.1 History

The SUBSAFE program was created after the loss of the nuclear submarine *Thresher*. The USS *Thresher* was the first ship of her class and the leading edge of U.S. submarine technology, combining nuclear power with modern hull design and newly designed equipment and components. On April 10, 1963, while performing a

1. I am particularly grateful to Rear Admiral Walt Cantrell, Al Ford, and Commander Jim Hassett for their insights on and information about the SUBSAFE program.

deep test dive approximately two hundred miles off the northeastern coast of the United States, the USS *Thresher* was lost at sea with all persons aboard: 112 naval personnel and 17 civilians died.

The head of the U.S. nuclear Navy, Admiral Hyman Rickover, gathered his staff after the *Thresher* loss and ordered them to design a program that would ensure such a loss never happened again. The program was to be completed by June and operational by that December. To date, that goal has been achieved. Between 1915 and 1963, the U.S. had lost fifteen submarines to noncombat causes, an average of one loss every three years, with a total of 454 casualties. *Thresher* was the first nuclear submarine lost, the worst submarine disaster in history in terms of lives lost (figure 14.1).

SUBSAFE was established just fifty-four days after the loss of *Thresher*. It was created on June 3, 1963, and the program requirements were issued on December 20 of that same year. Since that date, no SUBSAFE-certified submarine has ever been lost.

One loss did occur in 1968—the USS *Scorpion*—but it was not SUBSAFE certified. In a rush to get *Scorpion* ready for service after it was scheduled for a major overhaul in 1967, the Chief of Naval Operations allowed a reduced overhaul process and deferred the required SUBSAFE inspections. The design changes deemed necessary after the loss of *Thresher* were not made, such as newly designed central valve control and emergency blow systems, which had not operated properly on *Thresher*. Cold War pressures prompted the Navy to search for ways to reduce the duration of overhauls. By not following SUBSAFE requirements, the Navy reduced the time *Scorpion* was out of commission.

In addition, the high quality of the submarine components required by SUBSAFE, along with intensified structural inspections, had reduced the availability of critical parts such as seawater piping [8]. A year later, in May 1968, *Scorpion* was lost at sea. Although some have attributed its loss to a Soviet attack, a later investigation of the debris field revealed the most likely cause of the loss was one of its own torpedoes exploding inside the torpedo room [8]. After the *Scorpion* loss, the need for SUBSAFE was reaffirmed and accepted.

The rest of this chapter outlines the SUBSAFE program and provides some hypotheses to explain its remarkable success. The reader will notice that much of the program rests on the same systems thinking fundamentals advocated in this book.

Details of the *Thresher* Loss

The accident was thoroughly investigated including, to the Navy's credit, the systemic factors as well as the technical failures and deficiencies. Deep sea photography, recovered artifacts, and an evaluation of the *Thresher*'s design and operational

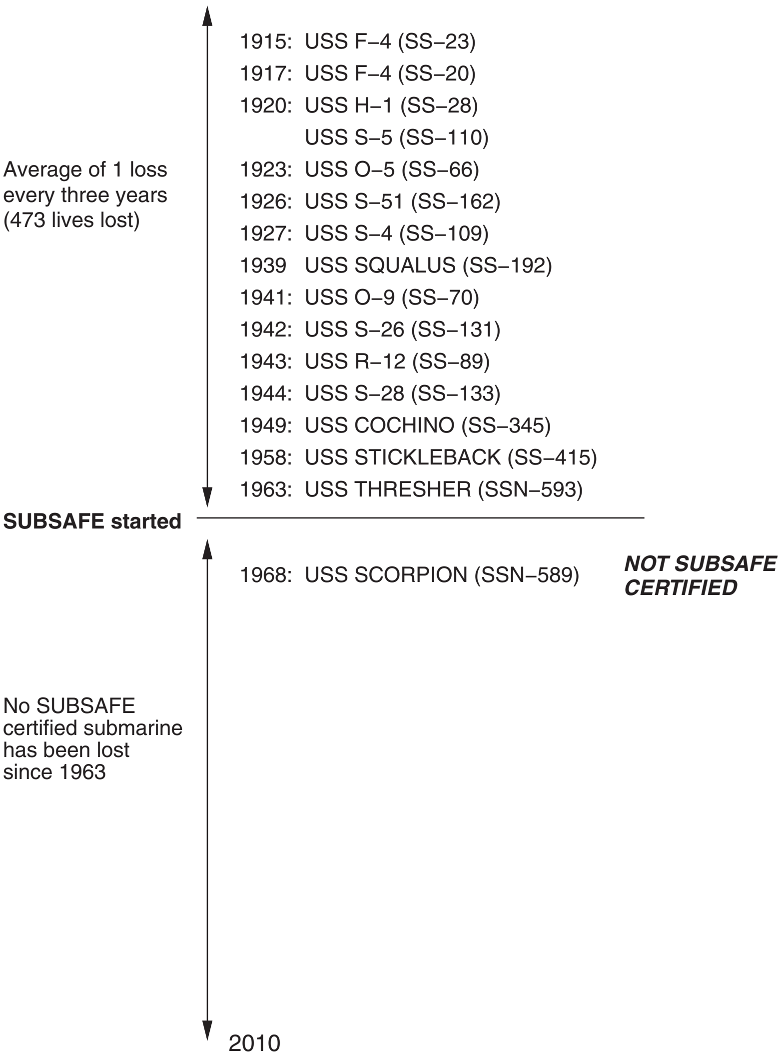

Figure 14.1
The history of noncombat U.S. submarine losses.

history led a court of inquiry to conclude that the failure of a deficient silver-braze joint in a salt water piping system, which relied on silver brazing instead of welding, led to flooding in the engine room. The crew was unable to access vital equipment to stop the flooding. As a result of the flooding, saltwater spray on the electrical components caused short circuits, shutdown of the nuclear reactor, and loss of propulsion. When the crew attempted to blow the main ballast tanks in order to surface, excessive moisture in the air system froze, causing a loss of airflow and inability to surface.

The accident report included recommendations to fix the design problems, for example, to add high-pressure air compressors to permit the emergency blow system to operate property. The finding that there were no centrally located isolation valves for the main and auxiliary seawater systems led to the use of flood-control levers that allowed isolation valves to be closed remotely from a central panel.

Most accident analyses stop at this point, particularly in that era. To their credit, however, the investigation continued and looked at why the technical deficiencies existed, that is, the management and systemic factors involved in the loss. They found deficient specifications, deficient shipbuilding practices, deficient maintenance practices, inadequate documentation of construction and maintenance actions, and deficient operational procedures. With respect to documentation, there appeared to be incomplete or no records of the work that had been done on the submarine and the critical materials and processes used.

As one example, *Thresher* had about three thousand silver-brazed pipe joints exposed to full pressure when the submarine was submerged. During her last shipyard maintenance, 145 of these joints were inspected on a "not-to-delay" vessel basis using what was then the new technique called ultrasonic testing. Fourteen percent of the 145 joints showed substandard joint integrity. Extrapolating these results to the entire complement of three thousand joints suggests that more than four hundred joints could have been substandard. The ship was allowed to go to sea in this condition. The *Thresher* loss investigators looked at whether the full scope of the joint problem had been determined and what rationale could have been used to allow the ship to sail without fixing the joints.

One of the conclusions of the accident investigation is that Navy risk management practices had not advanced as fast as submarine capability.

14.2 SUBSAFE Goals and Requirements

A decision was made in 1963 to concentrate the SUBSAFE program on the essentials, and a program was designed to provide maximum reasonable assurance of two things:

- Watertight integrity of the submarine's hull.
- Operability and integrity of critical systems to control and recover from a flooding hazard.

By being focused, the SUBSAFE program does not spread or dilute its focus beyond this stated purpose. For example, mission assurance is not a focus of SUBSAFE, although it benefits from it. Similarly, fire safety, weapons safety, occupational health and safety, and nuclear reactor systems safety are *not* in SUBSAFE. These additional concerns are handled by regular System Safety programs and mission assurance activities focused on the additional hazards. In this way, the extra rigor required by SUBSAFE is limited to those activities that ensure U.S. submarines can surface and return to port safely in an emergency, making the program more acceptable and practical than it might otherwise be.

SUBSAFE requirements, as documented in the SUBSAFE manual, permeate the entire submarine community. These requirements are invoked in design, construction, operations, and maintenance and cover the following aspects of submarine development and operations:

- Administrative
- Organizational
- Technical
- Unique design
- Material control
- Fabrication
- Testing
- Work control
- Audits
- Certification

These requirements are invoked in design contracts, construction contracts, overhaul contracts, the fleet maintenance manual and spare parts procurement specifications, and so on.

Notice that the requirements encompass not only the technical aspects of the program but the administrative and organizational aspects as well. The program requirements are reviewed periodically and renewed when deemed necessary. The Submarine Safety Working Group, consisting of the SUBSAFE Program Directors from all SUBSAFE facilities around the country, convenes twice a year to discuss program issues of mutual concern. This meeting often leads to changes and improvements to the program.

14.3 SUBSAFE Risk Management Fundamentals

SUBSAFE is founded on a basic set of risk management principles, both technical and cultural. These fundamentals are:

- Work discipline: Knowledge of and compliance with requirements
- Material control: The correct material installed correctly
- Documentation: (1) Design products (specifications, drawings, maintenance standards, system diagrams, etc.), and (2) objective quality evidence (defined later)
- Compliance verification: Inspections, surveillance, technical reviews, and audits
- Learning from inspections, audits, and nonconformances

These fundamentals, coupled with a questioning attitude and what those in SUBSAFE term a *chronic uneasiness*, are credited for SUBSAFE success. The fundamentals are taught and embraced throughout the submarine community. The members of this community believe that it is absolutely critical that they do not allow themselves to drift away from the fundamentals.

The Navy, in particular, expends a lot of effort in assuring compliance verification with the SUBSAFE requirements. A common saying in this community is, "Trust everybody, but check up." Whenever a significant issue arises involving compliance with SUBSAFE requirements, including material defects, system malfunctions, deficient processes, equipment damage, and so on, the Navy requires that an initial report be provided to Naval Sea Systems Command (NAVSEA) headquarters within twenty-four hours. The report must describe what happened and must contain preliminary information concerning apparent root cause(s) and immediate corrective actions taken. Beyond providing the information to prevent recurrence, this requirement also demonstrates top management commitment to safety and the SUBSAFE program.

In addition to the technical and managerial risk management fundamentals listed earlier, SUBSAFE also has cultural principles built into the program:

- A questioning attitude
- Critical self-evaluation
- Lessons learned and continual improvement
- Continual training
- Separation of powers (a management structure that provides checks and balances and assures appropriate attention to safety)

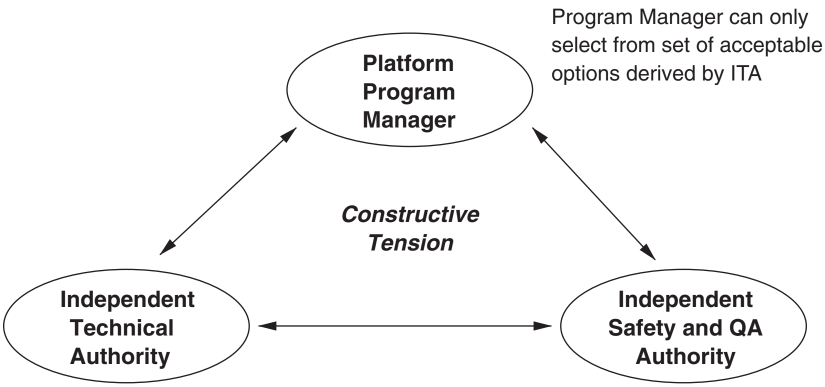

Figure 14.2
SUBSAFE separation of powers ("three-legged stool").

As is the case with most risk management programs, the foundation of SUBSAFE is the personal integrity and responsibility of those individuals who are involved in the program. The cement bonding this foundation is the selection, training, and cultural mentoring of those individuals who perform SUBSAFE work. Ultimately, these people attest to their adherence to technical requirements by documenting critical data, parameters, statements and their personal signature verifying that work has been properly completed.

14.4 Separation of Powers

SUBSAFE has created a unique management structure they call *separation of powers* or, less formally, the *three-legged stool* (figure 14.2). This structure is the cornerstone of the SUBSAFE program. Responsibility is divided among three distinct entities providing a system of checks and balances.

The new construction and in-service Platform Program Managers are responsible for the cost, schedule, and quality of the ships under their control. To ensure that safety is not traded off under cost and schedule pressures, the Program Managers can only select from a set of acceptable design options. The Independent Technical Authority has the responsibility to approve those acceptable options.

The third leg of the stool is the Independent Safety and Quality Assurance Authority. This group is responsible for administering the SUBSAFE program and for enforcing compliance. It is staffed by engineers with the authority to question and challenge the Independent Technical Authority and the Program Managers on their compliance with SUBSAFE requirements.

The Independent Technical Authority (ITA) is responsible for establishing and assuring adherence to technical standards and policy. More specifically, they:

- Set and enforce technical standards.
- Maintain technical subject matter expertise.
- Assure safe and reliable operations.
- Ensure effective and efficient systems engineering.
- Make unbiased, independent technical decisions.
- Provide stewardship of technical and engineering capabilities.

Accountability is important in SUBSAFE and the ITA is held accountable for exercising these responsibilities.

This management structure only works because of support from top management. When Program Managers complain that satisfying the SUBSAFE requirements will make them unable to satisfy their program goals and deliver new submarines, SUBSAFE requirements prevail.

14.5 Certification

In 1963, a SUBSAFE certification *boundary* was defined. Certification focuses on the structures, systems, and components that are critical to the watertight integrity and recovery capability of the submarine.

Certification is also strictly based on what the SUBSAFE program defines as *Objective Quality Evidence* (OQE). OQE is defined as any statement of fact, either quantitative or qualitative, pertaining to the quality of a product or service, based on observations, measurements, or tests *that can be verified.* Probabilistic risk assessment, which usually cannot be verified, is not used.

OQE is evidence that deliberate steps were taken to comply with requirements. It does not matter who did the work or how well they did it, if there is no OQE then there is no basis for certification.

The goal of certification is to provide maximum reasonable assurance through the initial SUBSAFE certification and by maintaining certification throughout the submarine's life. SUBSAFE inculcates the basic STAMP assumption that systems change throughout their existence. SUBSAFE certification is not a one-time activity but has to be maintained over time: SUBSAFE certification is a process, not just a final step. This rigorous process structures the construction program through a specified sequence of events leading to formal authorization for sea trials and delivery to the Navy. Certification then applies to the maintenance and operations programs and must be maintained throughout the life of the ship.

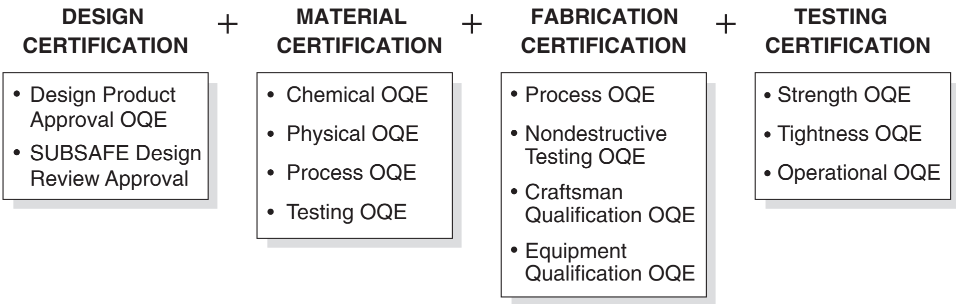

Figure 14.3
The four components of SUBSAFE certification.

14.5.1 Initial Certification

Initial certification is separated into four elements (figure 14.3):

1. *Design certification:* Design certification consists of design product approval and design review approval, both of which are based on OQE. For design product approval, the OQE is reviewed to confirm that the appropriate technical authority has approved the design products, such as the technical drawings. Most drawings are produced by the submarine design yard. Approval may be given by the Navy's Supervisor of Shipbuilding, which administers and oversees the contract at each of the private shipyards, or, in some cases, the NAVSEA may act as the review and approval technical authority. Design approval is considered complete only after the proper technical authority has reviewed the OQE and at that point the design is certified.
2. *Material certification:* After the design is certified, the material procured to build the submarine must meet the requirements of that design. Technical specifications must be embodied in the purchase documents. Once the material is received, it goes through a rigorous receipt inspection process to confirm and certify that it meets the technical specifications. This process usually involves examining the vendor-supplied chemical and physical OQE for the material. Records of chemical assay results, heat treatment applied to the material, and nondestructive testing conducted on the material constitute OQE.
3. *Fabrication certification:* Once the certified material is obtained, the next step is fabrication where industrial processes such as machining, welding, and assembly are used to construct components, systems, and ships. OQE is used to document the industrial processes. Separately, and prior to actual fabrication of the final product, the facility performing the work is certified in the industrial processes necessary to perform the work. An example is a specific

high-strength steel welding procedure. In addition to the weld procedure, the individual welder using this particular process in the actual fabrication receives documented training and successfully completes a formal qualification in the specific weld procedure to be used. Other industrial processes have similar certification and qualification requirements. In addition, steps are taken to ensure that the measurement devices, such as temperature sensors, pressure gauges, torque wrenches, micrometers, and so on, are included in a robust calibration program at the facility.

4. *Testing certification:* Finally, a series of tests is used to prove that the assembly, system, or ship meets design parameters. Testing occurs throughout the fabrication of a submarine, starting at the component level and continuing through system assembly, final assembly, and sea trials. The material and components may receive any of the typical nondestructive tests, such as radiography, magnetic particle, and representative tests. Systems are also subjected to strength testing and operational testing. For certain components, destructive tests are performed on representative samples.

Each of these certification elements is defined by detailed, documented SUBSAFE requirements.

At some point near the end of the new construction period, usually lasting five or so years, every submarine obtains its initial SUBSAFE certification. This process is very formal and preceded by scrutiny and audit conducted by the shipbuilder, the supervising authority, and finally, by a NAVSEA Certification Audit Team assembled and led by the Office of Safety and Quality Assurance at NAVSEA. The initial certification is in the end granted at the flag officer level.

14.5.2 Maintaining Certification

After the submarine enters the fleet, SUBSAFE certification must be maintained through the life of the slip. Three tools are used: the Reentry Control (REC) Process, the Unrestricted Operations Maintenance Requirements Card (URO MRC) program, and the audit program.

The Reentry Control (REC) process carefully controls work and testing within the SUBSAFE boundary, that is, the structures, systems, and components that are critical to the watertight integrity and recovery capability of the submarine. The purpose of REC is to provide maximum reasonable assurance that the areas disturbed have been restored to their fully certified condition. The procedures used provide an identifiable, accountable, and auditable record of the work performed.

REC control procedures have three goals: (1) to maintain work discipline by identifying the work to be performed and the standards to be met, (2) to establish personal accountability by having the responsible personnel sign their names on the reentry control document, and (3) to collect the OQE needed for maintaining certification.

The second process, the Unrestricted Operations Maintenance Requirements Card (URO MRC) program, involves periodic inspections and tests of critical items to ensure they have not degraded to an unacceptable level due to use, age, or environment. In fact, URO MRC did not originate with SUBSAFE, but was developed to extend the operating cycle of USS *Queenfish* by one year in 1969. It now provides the technical basis for continued unrestricted operation of submarines to test depth.

The third aspect of maintaining certification is the audit program. Because the audit process is used for more general purposes than simply maintaining certification, it is considered in a separate section.

14.6 Audit Procedures and Approach

Compliance verification in SUBSAFE is treated as a process, not just one step in a process or program. The Navy demands that each Navy facility participate fully in the process, including the use of inspection, surveillance, and audits to confirm their own compliance. Audits are used to verify that this process is working. They are conducted either at fixed intervals or when a specific condition is found to exist that needs attention.

Audits are multi-layered: they exist at the contractor and shipyard level, at the local government level, and at Navy headquarters. Using the terminology adopted in this book, responsibilities are assigned to all the components of the safety control structure as shown in figure 14.4. Contractors and shipyard responsibilities include implementing specified SUBSAFE requirements, establishing processes for controlling work, establishing processes to verify compliance and certify its own work, and presenting the certification OQE to the local government oversight authority. The processes established to verify compliance and certify their work include a quality management system, surveillance, inspections, witnessing critical contractor work (contractor quality assurance), and internal audits.

Local government oversight responsibilities include surveillance, inspections, assuring quality, and witnessing critical contractor work, audits of the contractor, and certifying the work of the contractor to Navy headquarters.

The responsibilities of Navy headquarters include establishing and specifying SUBSAFE requirements, verifying compliance with the requirements, and providing SUBSAFE certification for each submarine. Compliance is verified through two types of audits: (1) ship-specific and (2) functional or facility audits.

A ship-specific audit looks at the OQE associated with an individual ship to ensure that the material condition of that submarine is satisfactory for sea trial and

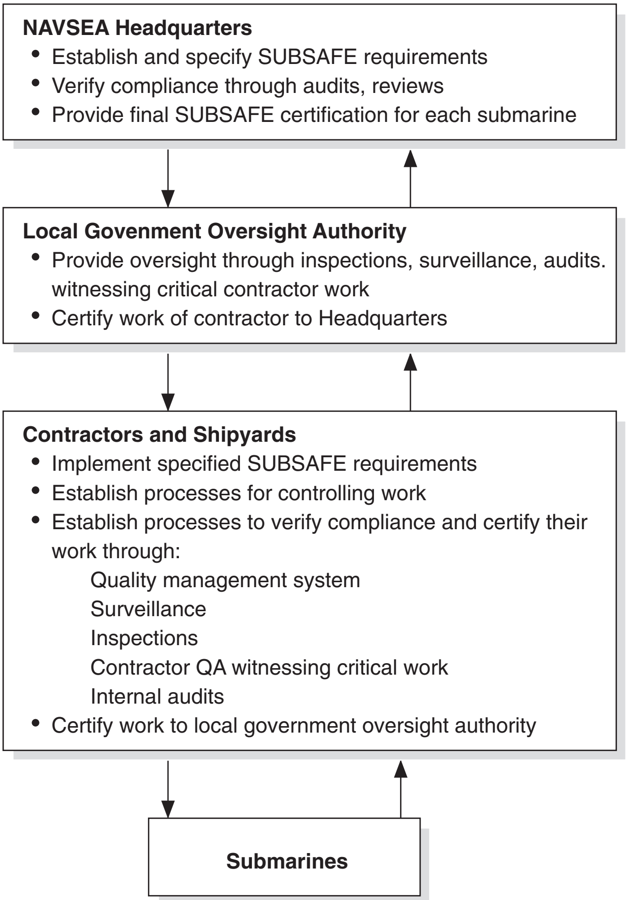

Figure 14.4
Responsibility assignments in the SUBSAFE compliance control structure.

unrestricted operations. This audit represents a significant part of the certification process that a submarine's condition meets SUBSAFE requirements and is safe to go to sea.

Functional or facility audits (such as contractors or shipyards) include reviews of policies, procedures, and practices to confirm compliance with the SUBSAFE program requirements, the health of processes, and the capability of producing certifiable hardware or design products.

Both types of audits are carried out with structured audit plans and qualified auditors.

The audit philosophy is part of the reason for SUBSAFE success. Audits are treated as a *constructive, learning* experience. Audits start from the assumption that policies, procedures, and practices are in compliance with requirements. The goal of the audit is to confirm that compliance. Audit findings must be based on a clear violation of requirements or must be identified as an "operational improvement."

The objective of audits is "to make our submarines safer" not to evaluate individual performance or to assign blame. Note the use of the word "our": the SUBSAFE program emphasizes common safety goals and group effort to achieve them. Everyone owns the safety goals and is assumed to be committed to them and working to the same purpose. SUBSAFE literature and training talks about those involved as being part of a "very special family of people who design, build, maintain, and operate our nation's submarines."

To this end, audits are a peer review. A typical audit team consists of twenty to thirty people with approximately 80 percent of the team coming from various SUBSAFE facilities around the country and the remaining 20 percent coming from NAVSEA headquarters. An audit is considered a team effort—the facility being audited is expected to help the audit team make the audit report as accurate and meaningful as possible.

Audits are conducted under rules of continuous communication—when a problem is found, the emphasis is on full understanding of the identified problem as well as identification of potential solutions. Deficiencies are documented and adjudicated. Contentious issues sometimes arise, but an attempt is made to resolve them during the audit process.

A significant byproduct of a SUBSAFE audit is the learning experience it provides to the auditors as well as those being audited. Expected results include cross-pollination of successful procedures and process improvements. The rationale behind having SUBSAFE participants on the audit team is not only their understanding of the SUBSAFE program and requirements, but also their ability to learn from the audits and apply that learning to their own SUBSAFE groups.

The current audit philosophy is a product of experience and learning. Before 1986, only ship-specific audits were conducted, not facility or headquarters audits. In 1986, there was a determination that they had gotten complacent and were assuming that once an audit was completed, there would be no findings if a follow-up audit was performed. They also decided that the ship-specific audits were not rigorous or complete enough. In STAMP terms, only the lowest level of the safety control structure was being audited and not the other components. After that time, biennial audits were conducted at all levels of the safety control structure, even the highest levels of management. A biennial NAVSEA internal audit gives the field activities a chance to evaluate operations at headquarters. Headquarters personnel must be willing to accept and resolve audit findings just like any other member of the nuclear submarine community.

One lesson learned has been that developing a robust compliance verification program is difficult. Along the way they learned that (1) clear ground rules for audits must be established, communicated, and adhered to; (2) it is not possible to "audit in" requirements; and (3) the compliance verification organization must be equal with the program managers and the technical authority. In addition, they determined that not just anyone can do SUBSAFE work. The number of activities authorized to perform SUBSAFE activities is strictly controlled.

14.7 Problem Reporting and Critiques

SUBSAFE believes that lessons learned are integral to submarine safety and puts emphasis on problem reporting and critiques. Significant problems are defined as those that affect ship safety, cause significant damage to the ship or its equipment, delay ship deployment or incur substantial cost increase, or involve severe personnel injury. Trouble reports are prepared for all significant problems encountered in the construction, repair, and maintenance of naval ships. Systemic problems and issues that constitute significant lessons learned for other activities can also be identified by trouble reports. Critiques are similar to trouble reports and are utilized by the fleet.

Trouble reports are distributed to all SUBSAFE responsible activities and are used to report significant problems to NAVSEA. NAVSEA evaluates the reports to identify SUBSAFE program improvements.

14.8 Challenges

The leaders of SUBSAFE consider their biggest challenges to be:

- *Ignorance:* The state of not knowing;
- *Arrogance:* Behavior based on pride, self-importance, conceit, or the assumption of intellectual superiority and the presumption of knowledge that is not supported by facts; and
- *Complacency:* Satisfaction with one's accomplishments accompanied by a lack of awareness of actual dangers or deficiencies.

Combating these challenges is a "constant struggle every day" [69]. Many features of the program are designed to control these challenges, particularly training and education.

14.9 Continual Training and Education

Continual training and education are a hallmark of SUBSAFE. The goals are to:

- Serve as a reminder of the consequences of complacency in one's job.
- Emphasize the need to proactively correct and prevent problems.
- Stress the need to adhere to program fundamentals.
- Convey management support for the program.

Continual improvement and feedback to the SUBSAFE training programs comes not only from trouble reports and incidents but also from the level of knowledge assessments performed during the audits of organizations that perform SUBSAFE work.

Annual training is required for all headquarters SUBSAFE workers, from the apprentice craftsman to the admirals. A periodic refresher is also held at each of the contractor's facilities. At the meetings, a video about the loss of *Thresher* is shown and an overview of the SUBSAFE program and their responsibilities is provided as well as recent lessons learned and deficiency trends encountered over the previous years. The need to avoid complacency and to proactively correct and prevent problems is reinforced.

Time is also taken at the annual meetings to remind everyone involved about the history of the program. By guaranteeing that no one forgets what happened to USS *Thresher*, the SUBSAFE program has helped to create a culture that is conducive to strict adherence to policies and procedures. Everyone is recommitted each year to ensure that a tragedy like the one that occurred in 1963 never happens again. SUBSAFE is described by those in the program as "a requirement, an attitude, and a responsibility."

14.10 Execution and Compliance over the Life of a Submarine

The design, construction, and initial certification are only a small percentage of the life of the certified ship. The success of the program during the vast majority of the certified ship's life depends on the knowledge, compliance, and audit by those operating and maintaining the submarines. Without the rigor of compliance and sustaining knowledge from the petty officers, ship's officers, and fleet staff, all of the great virtues of SUBSAFE would "come to naught" [30]. The following anecdote by Admiral Walt Cantrell provides an indication of how SUBSAFE principles permeate the entire nuclear Navy:

> I remember vividly when I escorted the first group of NASA skeptics to a submarine and they figured they would demonstrate that I had exaggerated the integrity of the program

> by picking a member of ship's force at random and asked him about SUBSAFE. The NASA folks were blown away. A second class machinist's mate gave a cogent, complete, correct description of the elements of the program and how important it was that all levels in the Submarine Force comply. That part of the program is essential to its success—just as much, if not more so, than all the other support staff effort [30].

14.11 Lessons to Be Learned from SUBSAFE

Those involved in SUBSAFE are very proud of their achievements and the fact that even after nearly fifty years of no accidents, the program is still strong and vibrant. On January 8, 2005, USS *San Francisco*, a twenty-six-year-old ship, crashed head-on into an underwater mountain. While several crew members were injured and one died, this incident is considered by SUBSAFE to be a success story: In spite of the massive damage to her forward structure, there was no flooding, and the ship surfaced and returned to port under her own power. There was no breach of the pressure hull, the nuclear reactor remained on line, the emergency main ballast tank blow system functioned as intended, and the control surfaces functioned properly. Those in the SUBSAFE program attribute this success to the work discipline, material control, documentation, and compliance verification exercised during the design, construction, and maintenance of USS *San Francisco*.

Can the SUBSAFE principles be transferred from the military to commercial companies and industries? The answer lies in why the program has been so effective and whether these factors can be maintained in other implementations of the principles more appropriate to non-military venues. Remember, of course, that private contractors form the bulk of the companies and workers in the nuclear Navy, and they seem to be able to satisfy the SUBSAFE program requirements. The primary difference is in the basic goals of the organization itself.

Some factors that can be identified as contributing to the success of SUBSAFE, most of which could be translated into a safety program in private industry are:

- Leadership support and commitment to the program.
- Management (NAVSEA) is not afraid to say "no" when faced with pressures to compromise the SUBSAFE principles and requirements. Top management also agrees to be audited for adherence to the principles of SUBSAFE and to correct any deficiencies that are found.
- Establishment of clear and written safety requirements.
- Education, not just training, with yearly reminders of the past, continual improvement, and input from lessons learned, trouble reports, and assessments during audits.
- Updating the SUBSAFE program requirements and the commitment to it periodically.

- Separation of powers and assignment of responsibility.
- Emphasis on rigor, technical compliance, and work discipline.
- Documentation capturing what they do and why they do it.
- The participatory audit philosophy and the requirement for objective quality evidence.
- A program based on written procedures, not personality-driven.
- Continual feedback and improvement. When something does not conform to SUBSAFE specifications, it must be reported to NAVSEA headquarters along with the causal analysis (including the systemic factors) of why it happened. Everyone at every level of the organization is willing to examine his or her role in the incident.
- Continual certification throughout the life of the ship; it is not a one-time event.
- Accountability accompanying responsibility. Personal integrity and personal responsibility is stressed. The program is designed to foster everyone's pride in his or her work.
- A culture of shared responsibility for safety and the SUBSAFE requirements.
- Special efforts to be vigilant against complacency and to fight it when it is detected.

Engineering a Safer World

Systems Thinking Applied to Safety

By: Nancy G. Leveson

Citation:

Engineering a Safer World: Systems Thinking Applied to Safety
By: Nancy G. Leveson
DOI: 10.7551/mitpress/8179.001.0001
ISBN (electronic): 9780262298247
Publisher: The MIT Press
Published: 2016

The MIT Press

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Syntax and Times Roman by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Leveson, Nancy.
Engineering a safer world : systems thinking applied to safety / Nancy G. Leveson.
p. cm.—(Engineering systems)
Includes bibliographical references and index.
ISBN 978-0-262-01662-9 (hardcover : alk. paper)
1. Industrial safety. 2. System safety. I. Title.
T55.L466 2012
620.8′6—dc23
2011014046

10 9 8 7 6 5 4 3 2 1