SYM-AM-21-093

EXCERPT FROM THE PROCEEDINGS
OF THE
EIGHTEENTH ANNUAL
ACQUISITION RESEARCH SYMPOSIUM

A Governance Model and Safety Management System Framework for Industrial Fire Safety During Naval Ship Maintenance Availabilities

May 11–13, 2021

Published: May 10, 2021

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

A Governance Model and Safety Management System Framework for Industrial Fire Safety During Naval Ship Maintenance Availabilities

Cheryl Marek—is a licensed Professional Fire Protection Engineer and PhD Candidate in Civil Engineering at the University of Maryland, College Park. Her research interests lie at the intersection of fire protection engineering, systems engineering, and the social sciences. She has several years of experience in the shipbuilding industry, is an active member of the Society of Naval Architects and Marine Engineers (SNAME), and is studying acquisition system influences on shipboard industrial fire safety. [cmarek@umd.edu]

Joseph Bradley—is Chief Scientist at Main Sail, LLC, and an Adjunct Associate Professor at Old Dominion University (ODU). Prior to joining ODU, he was Deputy Director for Force Maintenance at Commander, Submarine Force, Atlantic Fleet. He has served in various consulting roles, including Program Manager's Representative for the SSGN conversion of the USS *Ohio* and USS *Michigan*. His research interests include complex system governance and decision-making using modeling and simulation. He received a Degree of Mechanical Engineering and a Master of Science in mechanical engineering from the Naval Postgraduate School, and a BE from The Cooper Union. [josephbradley@leading-change.org]

John (Jack) McGowan—is a Certified Safety Professional who works to help NAVSEA safety professionals reduce injuries and mishaps at NAVSEA Field Activities, which include Warfare Centers, Regional Maintenance Centers, and Naval Shipyards. Before starting at NAVSEA Headquarters, he worked as a Safety Manager at Puget Sound Naval Shipyard, San Diego Detachment, and as a Project Safety Manager at Puget Sound Naval Shipyard, Bremerton. McGowan is now the lead Safety Professional for the Information and Analysis Branch in NAVSEA 04, Industrial Operation Directorate. [john.mcgowan@navy.mil]

Qingbin Cui—is a Professor at the University of Maryland, College Park. He has over 20 years of industry and research experience and specializes in the areas of project management, public–private partnerships (P3), and sustainability. He is a technical consultant to the U.S. Department of Transportation for the P3 Capacity Building Program and a member of the expert panel for the U.S. Department of Energy on energy performance contracting, and built a university–industry partnership for data-driven construction research and education. [cui@umd.edu]

Abstract

Managing shipboard industrial fire safety during a depot or intermediate level maintenance availability on a commissioned naval vessel can be viewed as a complex system bounded by the defense acquisition system. Sociotechnical factors define the hazard and associated risk and risk management practices, and this complex system governs the resulting level of fire safety. Poor industrial fire safety practices during naval ship maintenance availabilities can directly impact project cost and schedule. If a fire is severe enough, these effects can trickle throughout the ship class's maintenance program, adversely impacting fleet readiness and operations. Traditional viewpoints on fire safety prescriptively regulate the fire hazard. Rote compliance with this type of requirement does not provide clear mechanisms for measuring safety performance, resulting in uneven risk management. This paper presents a safety management system (SMS) framework for shipboard industrial fire safety based on the Complex Systems Governance (CSG) reference model developed by Keating and Bradley (2015). The value of a clearly defined governance model and SMS framework in conjunction with industry standardization and information sharing is the emergence of trends. This supports feedback loops between requirements and outcomes, allowing more effective management of fire safety across the broad stakeholder groups involved.

Introduction

Shipboard fire incidents during industrial construction and maintenance activities pose a significant threat to fielding the required naval force strength. Naval vessels transition in and out of construction and maintenance periods throughout their life cycle, and protecting them from fires during industrial work is a complex issue. Fire risk involves not only risk associated with the fire itself, but also the risk associated with loss of an operational asset. The impact of small fires during ship construction or overhaul could be minor property damage or injury to a worker or sailor. Larger fires can result in schedule delays or loss of life, and a major fire can result in the total loss of a ship.

When the USS *Miami* (SSN 755) was decommissioned after suffering a major fire while in dry dock at Portsmouth Naval Shipyard in 2012, five deployments over her remaining 10-year operational life were lost (McDermott, 2013). Investigation of the July 12, 2020, fire aboard the USS *Bonhomme Richard* (LHD 6) while pier side at Naval Base San Diego, CA, towards the end of a GD NASSCO overhaul availability is ongoing, with the ship declared a total loss in early 2021 (Ziezulewicz, 2021). Shortly after this fire, Assistant Secretary of the Navy for Research, Development, and Acquisition James Geurts (2020) issued a memorandum to the entire shipbuilding and ship maintenance enterprise stating, “Preventing shipboard fires is a team sport, no matter where the ship is in its life cycle, and no matter who is working on the ship,” and “There is no place in our Navy for complacency – the lives of our teammates and the accomplishment of our mission depends upon it” (p. 1).

The USS *Miami* (SSN 775) Fire Panel Recommendations (Gortney, 2012, p. 1) also cite complacency, stating “the MIAMI investigation paints a picture of multiple processes within several organizations going through the motions, with no particular failure, but lacking focused attention and oversight, and missing the mark in the aggregate”, and “it is clear that the Navy has unintentionally accepted a reduced margin to fire safety when a ship enters an industrial environment -- where the risk of fire is at its highest.” In the weeks following the major fire on USS *Bonhomme Richard*, minor fire incidents related to hot work occurred on the USS *John F Kennedy* (CVN 79) at HII-Newport News Shipbuilding and USS *Kearsarge* (LHD 3) at GD NASSCO in Norfolk, VA (Eckstein, 2020), serving as a wake-up call to the industry.

A few months prior to the USS *Bonhomme Richard* fire, Naval Sea Systems Command (NAVSEA) presented the results of an effort initiated in June 2019 in response to 2018 fires aboard USS *Oscar Austin* (DDG 79) and USS *Fitzgerald* (DDG 62) to assess industrial fire safety, fire prevention, and control programs based on self-assessment responses and reported data on fires that had occurred over the previous 30 months at public and private maritime maintenance facilities (McGowan & Smith, 2020). Their effort is summarized herein and built upon to propose the framework for a data-driven direction to addressing the Navy’s shipboard industrial fire problem.

In June 2020, the Navy issued a new Safety and Occupational Health Manual that established the Navy Safety Management System (SMS) to “facilitate a transition from reactively managing safety to proactively managing safety and risk, and ultimately, to become predictive” (U.S. Department of the Navy [DoN], 2020, p. A1-2). This evolving direction provides an opportunity for deliberate implementation of a novel approach to managing fire safety during naval ship maintenance availabilities.

Our approach aims to assess common systemic threads in major safety mishaps—contributions of the system that frames management of risk to outcomes and the relationship between complacency and responsibility. The dual incidents of the recent major fire aboard USS *Bonhomme Richard* (LHD 6) and total loss of the USS *Miami* parallel the National Aeronautics and Space Administration’s (NASA’s) dual losses of space shuttles Challenger in

1986 and Columbia in 2003, albeit separated by a much shorter period of time. The Columbia Accident Investigation Board (CAIB) identified organizational system failures and flawed organizational practices, including complacency and cultural beliefs. Specifically, “history again at work: how past definitions of risk combined with systemic problems in the NASA organization caused both accidents” (Columbia Accident Investigation Board [CAIB], 2003, p. 195).

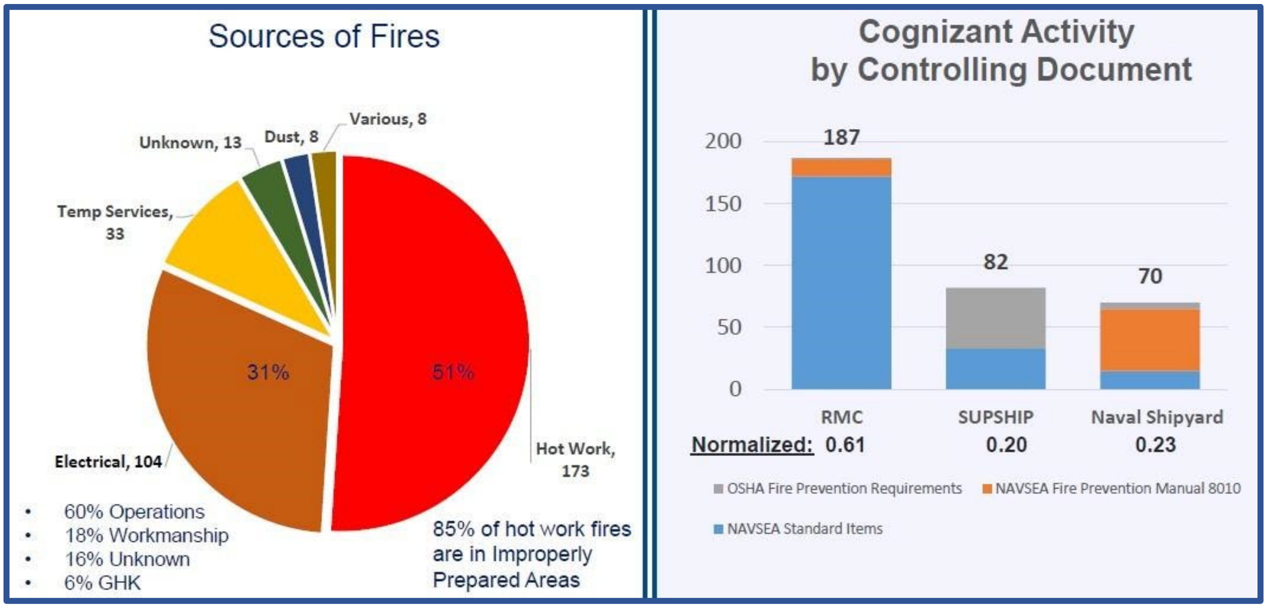
We propose an SMS framework for shipboard industrial fire safety based on the Complex Systems Governance (CSG) reference model developed by Keating and Bradley (2015) to inform the transition from regulating fire hazards to systematic management of fire safety during maintenance availabilities on commissioned naval vessels. The focus is on developing feedback loops between requirements and outcomes through a data-driven approach to support proactive management of shipboard industrial fire safety, a reduction in lost operational days due to fire incidents, and identification of the gaps that must be addressed to implement this framework.

Table 1. Research Goals and Objectives

Goals	Objectives
Dissect the shipboard industrial fire safety problem, including acquisition system influences	Evaluate the problem within the sociotechnical safety perspective on risk
	Evaluate the problem with respect to defense-in-depth
Develop an SMS framework for Shipboard Industrial Fire Safety based on the CSG reference model	Evaluate the problem within the Cynefin framework
	Evaluate how the Navy SMS framework integrates into the CSG reference model
	Identify necessary feedback loops between requirements and outcomes
	Identify gaps between framework architecture and the current state

NAVSEA Shipboard Industrial Fire Incident Data Analysis Summary

In June 2019, “COMNAVSEA directed Naval activities and requested private maintenance facilities to report all fires over the last 30 months. NAVSEA received responses from public and private maritime maintenance facilities. These responses were analyzed by 04RS for completeness, self-reflection, and innovation/solutions” (McGowan & Smith, 2020, slide 2). Data from 339 fire incidents were reviewed, and NAVSEA 04RS (Industrial Operations, Safety) performed an analysis of causal factors using the Department of Defense’s Human Factors Analysis and Classification System (HFACS) to identify trends and lessons learned. The top three sources of shipboard fires during industrial work were hot work, electrical, and temporary sources. Shipboard industrial fire incidents were also analyzed with regards to the Cognizant Activity and controlling document for fire safety requirements. Results are summarized in Figure 1.



- 60% Operations
- 18% Workmanship
- 16% Unknown
- 6% GHK

85% of hot work fires are in Improperly Prepared Areas

Figure 1. Fire Reporting Data
(McGowan & Smith, 2020, slide 4)

Regardless of the source of the requirements, non-compliance related to fundamental fire prevention practices was identified as the cause of 85% of hot work fires, which occurred in improperly prepared areas. The distribution of fires among Cognizant Activities is related to the volume of work overseen by each, suggesting that the problem is universal across the naval maritime repair industry.

Significant findings outlined next “were remarkably similar to other fires experienced by the Navy,” including “1942 SS Normandie, Total loss of the ship, 285 Injuries” and “1944 USS Saturn, 15 fatalities, 20 injuries.” “Both events were the result of improper hot-work controls” (McGowan & Smith, 2020, slide 8). These findings include the following:

- Failure to follow the “35-foot rule” is the most frequent cause of hot work fires.
- Port loading variations and high influx of temporary employees with low experience increase the likelihood of fire safety non-compliance.
- Communication between fire watches and hot workers, and inspections by hot work supervisors, are less than adequate.
- Failure to comply with the invoked standard (OSHA, NAVSEA Requirements) was common. (McGowan & Smith, 2020, slide 7)

In addition to the analytic side of this effort, actions taken by NAVSEA included establishing new hot work requirements in NAVSEA Standard Item (NSI) Fiscal Year 2020, Change 2, and “VADM Moore wrote a letter to all parties stating that a ship repair contractor’s non-compliance with fire prevention standards and regulations is a contractual non-compliance” (McGowan & Smith, 2020, slide 10). A variety of recommendations to improve compliance were made for Naval maritime facilities (Naval shipyards, Regional Maintenance Centers (RMCs) and the Supervisor of Shipbuilding (SUPSHIP/SOS). Future initiatives identified by NAVSEA include sharing best practices across the industry and establishing a multi-functional committee to address issues uncovered through information sharing (McGowan & Smith, 2020). Uniformly implementing good and best practices in private shipyards requires a combination of approaches, largely due to contractual influences.

Methodology

Defining the Problem

Sociotechnical Safety Perspective on Risk

The concept of a sociotechnical system is derived from the context of work systems and was defined by Ropohl (1999) as

> established to stress the reciprocal interrelationship between humans and machines and to foster the program of shaping both the technical and the social conditions of work, in such a way that efficiency and humanity would not contradict each other any longer. (p. 59)

Sociotechnical systems in this sense are made up of a hierarchy of action systems, or subsystems, with three primary levels that perform the work, oversee the work, and set goals for the work. These subsystems can further be divided into sub-subsystems, and significant feedback loops and couplings exist between them. In the case of overhaul work on a commissioned naval vessel, these lines can sometimes be blurred, and a single organization can have functions within multiple subsystems. Sociotechnical is further defined by Aven and Ylönen (2018)

> to include the following dimensions: 1) two or more persons, interaction with some form of 2) technology, 3) and internal work environment (both physical and cultural), 4) external environment (can include political, regulatory, technological, economic, educational and cultural sub-environments), 5) an organisational design and management subsystems. (p. 14)

Continuing the parallels to the dual NASA accidents, the CAIB devoted chapters of its report to discussing organizational causes, history as a cause, and decision-making within the organization. The report identified a broken safety culture and pointed to Naval Reactors and the Navy’s SUBSAFE programs as strong examples of a good culture, with key differences being requirements ownership (technical authority) and emphasis on lessons learned (CAIB, 2003).

Safety vs. Risk

A goal of the Navy SMS is to proactively manage both safety and risk (DoN, 2020). To do this, it is important to distinguish between these two interrelated objectives. The Society for Risk Analysis Glossary defines safe as “without unacceptable risk,” and safety as “the antonym of risk” (Society for Risk Analysis [SRA], 2018, p. 7). Risk is given several qualitative definitions, but for the context of this paper we will use “the occurrences of some specified consequences of the activity and associated uncertainties” (SRA, 2018, p. 4). Möller et al. (2006) argue that safety goes beyond the antonym of risk due to epistemic uncertainty and proposed the intersubjective concept of safety: “(1) it is based on the comparative judgments of severity of harm that the majority of humans would agree on, and (2) it makes use of the best available expert judgments on the probabilities and uncertainties involved” (p. 427). Aven (2009) argues that safety is the antonym of risk for certain perspectives (definitions) of risk, specifically, when risk is the two-dimensional combination of uncertainty and consequences, uncertainty is integral to the definition, safety is the antonym of risk, and safe can be defined as “acceptable risk and acceptable safety” (p. 929). This is the perspective adopted in this paper.

Defense-in-Depth

Sorensen et al. (1999) identify that defense-in-depth as a nuclear industry safety strategy began development in the 1950s. Their review of the history of the term indicated that there was as of yet no official or preferred definition, but that when the term is used and if a definition is needed, “one is created consistent with the intended use of the term. Such definitions are often made by example” (p. 1). By 1999, the term had come to have two different meanings, roughly corresponding to the perspective of the particular model. Those perspectives were cast as either denoting “the philosophy of high level lines of defense, such as prevent accident initiators from occurring, terminate accident sequences quickly, and mitigate accidents that are not successfully terminated” (p. 3). The other portrays “the multiple physical barrier approach, most often exemplified by the fuel cladding, primary system, and containment” (p. 2). These two model perspectives are cast as either structuralist or rationalist:

> The structuralist model asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The requirements for defense in depth are derived by repeated application of the question, “What if this barrier or safety feature fails?”. (pp. 3–4)

Sorensen et al. (1999) portray that “the rationalist model asserts that defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression” (p. 4). They also assert that “the structuralist and rationalist models are not generally in conflict. Both can be construed as a means of dealing with uncertainty,” and further, they note that “neither incorporates any reliable means of determining when the degree of defense in depth achieved is sufficient” (p. 5).

As more nuclear power plants were built and more service experience acquired, new rules were progressively added, yielding a very complex set of requirements for the last part of the existing fleet of reactors to be built. A variation of technical debt was building up; even with “the accumulation of experience with various incidents and accidents, a growing list of unresolved safety issues emerged” (Fleming & Silady, 2002, p. 206). Fleming and Silady (2002) highlight that even as requirements were increased,

> many additional incidents occurred, including literally hundreds of common cause failures in redundant safety systems. This experience casts doubt on the wisdom of excluding common cause failures from the design basis envelope, thereby exposing a serious limitation of the single failure criterion as a tool to help define what is credible. (p. 206)

A footnote in Fleming and Silady (2002) notes that

> In the peer review of an earlier draft of this paper it was pointed out that the regulations governing nuclear power include one definition of defense-in-depth in 10 CFR Part 50 Appendix R which sets rules for fire protection in older plants. This definition sets forth the following objectives for the defense-in-depth of fire protection. Prevent fires from starting, detect rapidly, control and extinguish the fires that do occur, and to protect SSCs needed to safely shutdown the plant from the effects of the fire and firefighting activities. (p. 207)

Saleh et al. (2014), discussing the Texas City refinery fire, noted “a fundamental failure mechanism in this accident, namely the absence of observability or ability to diagnose hazardous states in the operation of the refinery, in particular within the raffinate splitter tower and the blowdown drum of the isomerization unit” (p. 1). They go on to “propose a general safety–diagnosability principle for supporting accident prevention, which requires that all safety-degrading events or states that defense-in-depth is meant to protect against be diagnosable, and that breaches of safety barriers be unambiguously monitored and reported." Further "violation of the safety–diagnosability principle translates into a shrinking of the time window available for operators to understand an unfolding hazardous situation and intervene to abate it." They go onto conclude that "defense-in-depth be augmented with this principle, without which it can degenerate into an ineffective defense-blind safety strategy" (Saleh et al., 2014, p. 1).

Cynefin Framework

Cynefin framework is a sense-making framework first developed by a group of researchers at IBM "conducting a program of disruptive action research using the methods of narrative and complexity theory to address critical business issues" (Kurtz & Snowden, 2003, p. 462). This work was partially funded through the Defense Advanced Research Project Agency (DARPA) with an interest in "new approaches to support policy-making" (Kurtz & Snowden, 2003, p. 462). The group challenged three basic assumptions of decision-making and policymaking—order, rational choice, and intentional capability—believing that while commonly available tools and techniques assume they are true, they are not universally true. With regard to order, they discuss situations where lack of order isn't a bad thing and the concept of emergent order (un-order) that is self-organizing rather than controlled and emerges from the interaction of many entities. Ordered-systems thinking has limitations because it assumes "we can derive or discover general rules or hypotheses that can be empirically verified and that create a body of reliable knowledge, which can then be developed and expanded" (Kurtz & Snowden, 2003, p. 466), and this does not hold true for all domains.

Unlike the more traditional categorization framework with a two-by-two matrix where the most desirable condition exists in the upper right-hand quadrant, the Cynefin sense-making framework "is used primarily to consider the dynamics of situations, decisions, perspectives, conflicts, and changes in order to come to a consensus for decision-making under uncertainty" (Kurtz & Snowden, 2003, p. 468) and does not favor any of the domains as more desirable or imply value axes. The five domains, currently referred to as clear, complicated, complex, chaotic, and confused, are depicted in Figure 2.

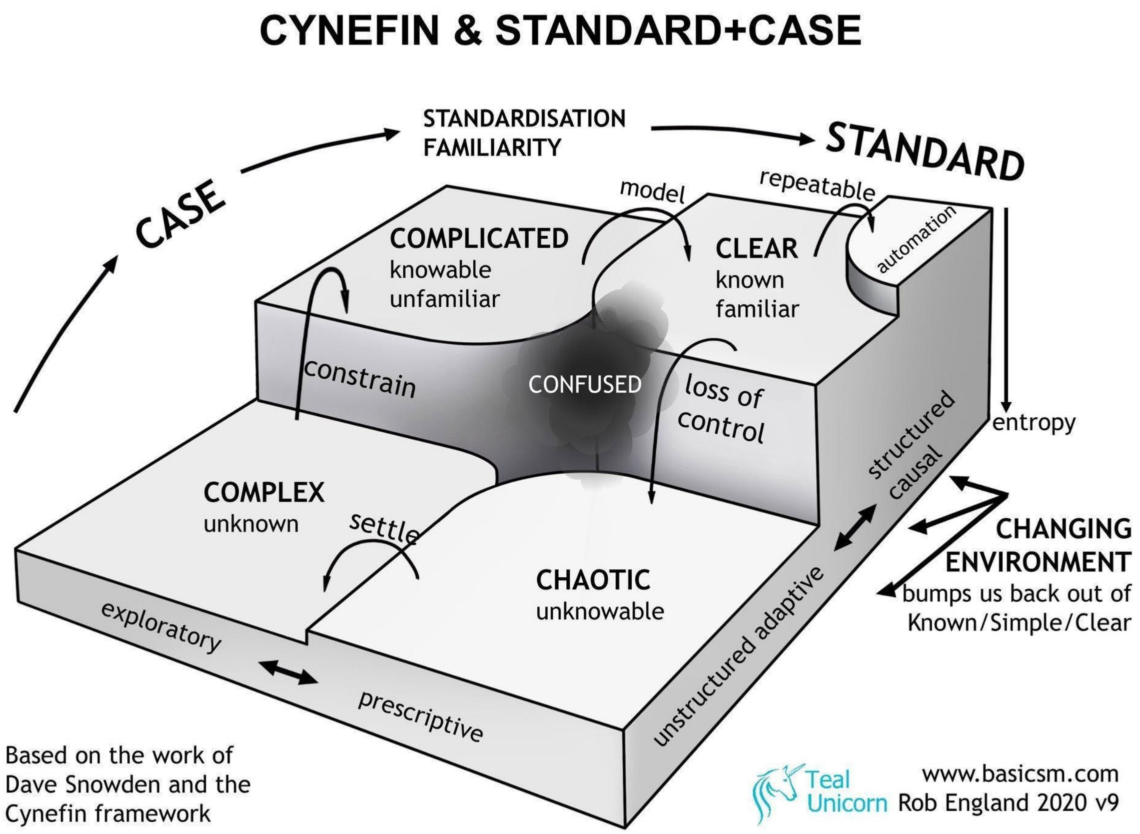


Figure 2. Cynefin Framework and Relationships

Descriptions of Domains

Clear (simple) is the domain of the known, with clear cause and effect relationships that are undisputed and generally empirical in nature. It is the domain of structured techniques and process engineering, with focus on consistency and efficiency (Kurtz & Snowden, 2003). In this ordered and obvious domain, optimal solutions can be identified. In other words, it is the domain of best practices (Fierro et al., 2018).

Complicated is the domain of the knowable, or “known unknowns” (Fierro et al., 2018, p. 6), with stable cause and effect relationships that are either not fully known or only known to a small group of people (Kurtz & Snowden, 2003). With enough time and resources, anything in this domain could become known and move to the clear domain. Kurtz and Snowden (2003) described this as “the domain of methodology, which seeks to identify cause-effect relationships through the study of properties which appear to be associated with qualities” (p. 468). In this domain of reductionism, the goal is to analyze, versus categorize, and decompose a system or problem into its constituent parts with approaches governed by things like standard rules, procedures, and protocols manuals. Because there may be multiple right answers and multiple options must be considered, good practices are preferred to best practices (Fierro et al., 2018).

Complex is the domain of the “unknown knowns” (Fierro et al., 2018, p. 8), where “there are cause and effect relationships between the agents, but both the number of agents and the number of relationships defy categorization or analytic techniques” (Kurtz & Snowden, 2003, p.

469). This is the domain of complexity theory, and “emergent patterns can be perceived but not predicted.” Fierro et al. (2018) refer to this domain as “unordered—obvious in hindsight” (p. 8), where the facts can be understood through reconstruction and rationalized after the fact. In this realm, there a range of potential failures, and emergent behaviors between highly interconnected subsystems can result in the emergence of different failure modes as actions are applied. The best approach in this domain is to “probe, sense, and then respond” (p. 8), and detailed planning is of minimal value due to the dynamic nature of sub-system interactions. An evolutionary strategy is recommended where solutions are developed in builds, and unlike an incremental strategy, it is acknowledged “that the user need is not fully understood and not all requirements can be defined up front” (p. 9).

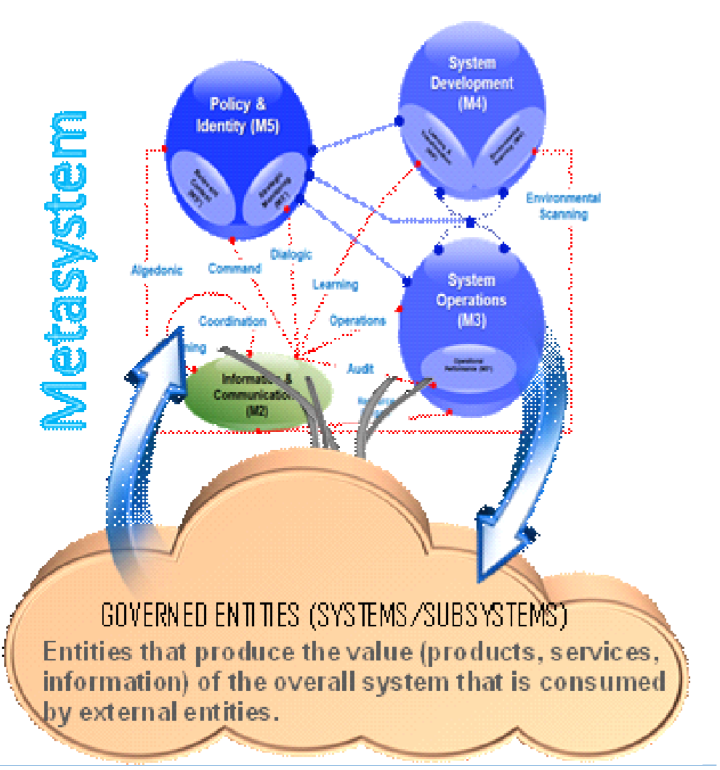
Chaotic is the domain of “unknown unknowns” (Fierro et al., 2018), where there are no perceivable relationships between cause and effect and there is insufficient response time to evaluate change because the system is turbulent. Here, best practices can contribute to the chaos because there is nothing to analyze and “waiting for patterns to emerge is a waste of time” (Kurtz & Snowden, 2003). This is an unordered domain where “we don’t even know which are the relevant aspects related to the problem, and no information is available even to be able to define the problem” (Fierro et al., 2018). Response in this domain is to act quickly to reduce turbulence, sense where stability is or is not present based on this action, and then “respond by working to transform the situation from chaos to complexity, where the identification of emerging patterns can both help prevent future crises that discern new opportunities” (p. 12). This is also known as “the domain of novel practice” (p. 12) and can sometimes be desirable on the path to innovation.

Confused or Aporetic, formerly Disorder, is at the interaction of the other domains of the Cynefin framework, reflective in the conflict of decision-makers approaching a problem from different points of view (Kurtz & Snowden, 2003). In this domain, each decision-maker relies on their own comfort zone to pull the issue into the domain that plays to their strengths or desires. The goal in this domain is to adapt leadership styles based on context and shift the problem into the appropriate domain given the nature of the problem and decision-making context (Fierro et al., 2018).

Complex Systems Governance

Complex System Governance (CSG) is an emerging field formally defined by Keating et al. (2014) as the “design, execution, and evolution of the metasystem functions necessary to provide control, communication, coordination, and integration of a complex system” (p. 274). Theory and concepts are derived from the fields of systems theory, management cybernetics, and system governance. The domain of complex systems includes the characteristics of complexity, contextual dominance, ambiguity, and holistic nature. The governance perspective of CSG is rooted in the cybernetic perspective of “design for ‘regulatory capacity’ to provide appropriate controls capable of maintaining system balance” (Keating & Katina, 2019, p. 690) and differs from management by emphasizing outcomes versus outputs with a higher degree of separation between action and response. The CSG model provides a framework for improving system performance (Keating et al., 2019). Discovery, classification, and engagement are neither mutually exclusive nor interdependent aspects of the framework, facilitating emergence of unabsorbed pathologies and the ability to improve resilience of the system. Included meta-functions (pathologies), definitions, and their relationships are depicted in Table 2.

Table 2. CSG Reference Model and Metasystem Definitions

Policy and Identity (M5) – overall steering and trajectory for the system includes context and monitoring of the governance system.	
System Development (M4) – models current and future system; includes learning and environmental scanning.	
System Operations (M3) – day to day execution of the metasystem includes performance monitoring of the governed systems.	
Information and Communications (M2) – flow and interpretation of information necessary to execute metasystem functions; the "spine" of the system.	
Governed Systems (S1s) – the organizational components of the larger system that are governed by the meta-systems. They are identified here as Regional Maintenance Commands and the Contractors executing work.	

CSG provides a suitable framework for modeling the complex relationships between the ship/ship's force, contractor/activity performing the work, and various Navy activities involved in the management of shipboard industrial fire risk. A model-centric approach to evaluating these relationships and the delegation of ownership for each aspect of the sociotechnical problem reveals emergence of the system and reduces ambiguity, providing answers to questions such as *who owns the risk* and *are all aspects of the risk accounted for*?

Navy Safety Management System Framework

The Navy Safety program updated its policy in June 2020 with the release of a revised *Navy Safety and Occupational Health Manual* (DoN, 2020). This manual "establishes the Navy Safety Management System (SMS), a comprehensive framework that will ensure operational readiness through continuous improvement and risk-based decision making processes and procedures" (DoN, 2020, p. A1-2). It defines an SMS as "a system of processes that proactively manages day-to-day safety and risk management in an organization across all operations and business lines. It is not a single written policy or database" (DoN, 2020, p. A1-4). The Submarine Safety (SUBSAFE) Program is given as a Navy community-level example, with policy supporting the operational safety functional area of an SMS.

The Navy SMS is a high-level framework intended to be both transparent and scalable. The policy applies directly to Navy civilian and military personnel and operations worldwide but is not applicable where Navy contractors are responsible directly to state or the Department of Labor (DOL) Occupational Safety and Health Administration (OSHA) for the occupational safety and health of its employees. However, the requirement for Navy SMS framework is an enterprise-level policy that encompasses areas beyond occupational safety, including industrial ship safety, industrial ship fire protection and prevention, and safety mishap reporting and investigation (DoN, 2020). Shipboard industrial fire safety is unique in that requirements and outcomes can dually influence both occupational safety and ship safety. Maintaining ship conditions goes above and beyond what is required to protect workers, similar to how building and life safety codes distinguish between life safety and property protection requirements.

The manual is a requirements document that outlines the minimum requirements for an SMS framework, consisting of “an iterative continuous improvement cycle, four pillars, and one or more minimum fundamental elements that underpin those pillars” (DoN, 2020, p. A1-6). The four pillars and their fundamental elements are depicted in Figure 3.

Figure 3. Four Pillars of a Navy SMS and Fundamental Elements

Note that some of the fundamental elements cross, or exist, in multiple pillars. Personnel awareness, education, and training are fundamental to both “Policy and Organizational Commitment” and “Promotion.” Similarly, risk monitoring and change management cross “Risk Management” and “Assurance.” These particular elements are key to establishing feedback loops between requirements and outcomes, or the continuous improvement cycle.

With regards to appointment of SMS personnel, “SMS-related responsibilities and authorities must be defined, documented, and communicated throughout the organization” and “Safety management system personnel must be appointed with the authority to execute SMS processes and programs.” Although aspects of shipboard industrial fire safety are distributed among various safety functional areas, NAVSEA 04RS[1] (Industrial Operations, Safety) the technical warrant holder (TWH) for safety policy, is emerging in a leadership role in addressing fires throughout the naval enterprise. Previously NAVSEA 04RS limited its scope to collecting data and sharing that data within the NAVSEA community. During the past 2 years, NAVSEA 04RS has been engaged with the private shipbuilding community and the maritime industry at large to bring attention to the problem of fires onboard naval vessels during construction and maintenance availabilities. The focus of this paper is on identifying ownership, accountability, and communication channels as they relate to roles and responsibilities within the framework.

Research Results

The Sociotechnical Problem

Complexity emerges from decomposing contributing factors to the Navy’s shipboard industrial fire safety problem. Figure 4 outlines the sociotechnical factors that contribute to industrial fire safety during ship maintenance availabilities in each of the five contributing dimensions and corresponding sub-environments.

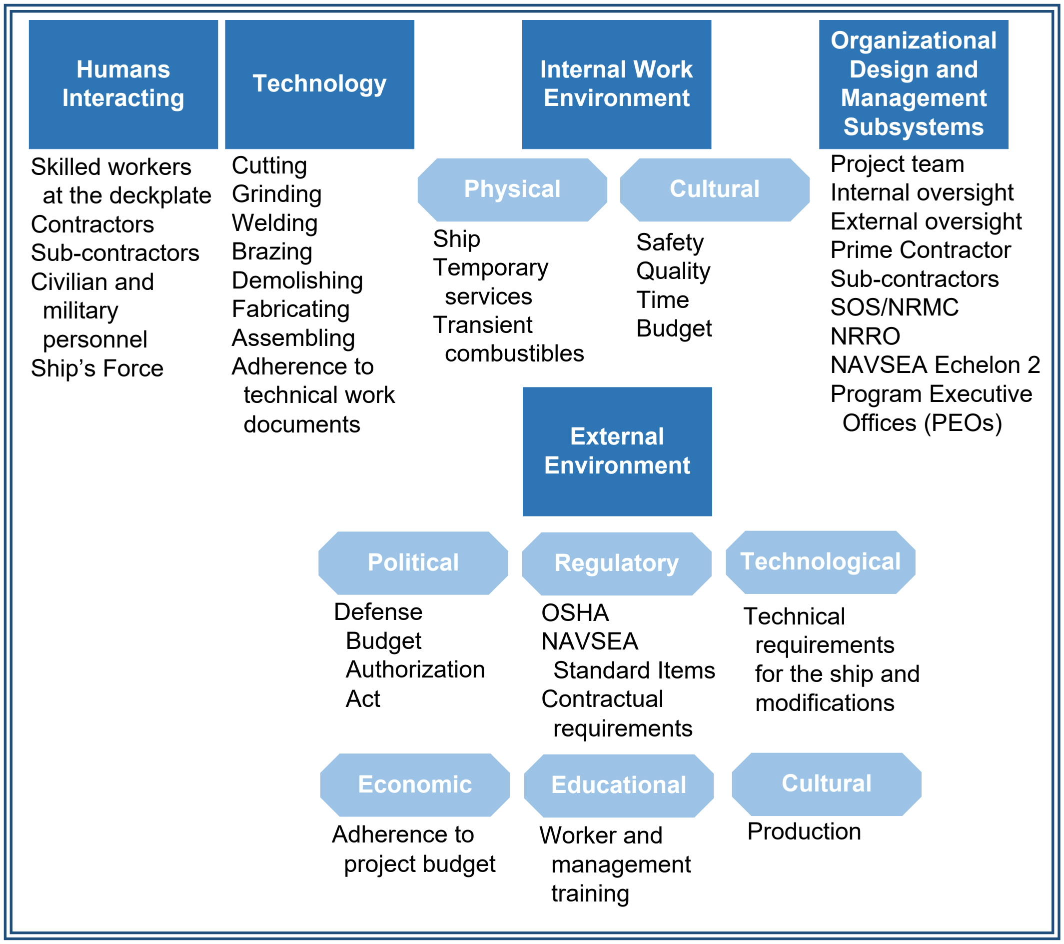


Figure 4. Sociotechnical Decomposition of Shipboard Industrial Fire Safety

In addition to the underlying technical factors, multiple parties are involved with managing the risk. Shipboard industrial fire risk management occurs at the intersection of the contracting authority overseeing the work (NAVSEA), the contractor performing the work, and the ship that is being worked on or constructed. For a commissioned ship, U.S. Navy Regulations dictate that when work is performed in a private shipyard under a contract being administered by the Supervisor of Shipbuilding Conversion and Repair, responsibility for safe execution of the work is assigned via contract to the contractor. The commanding officer retains responsibility for safety of the ship and requesting services necessary to maintain safety of the ship (DoN, 1990). This relationship is depicted in Figure 5.

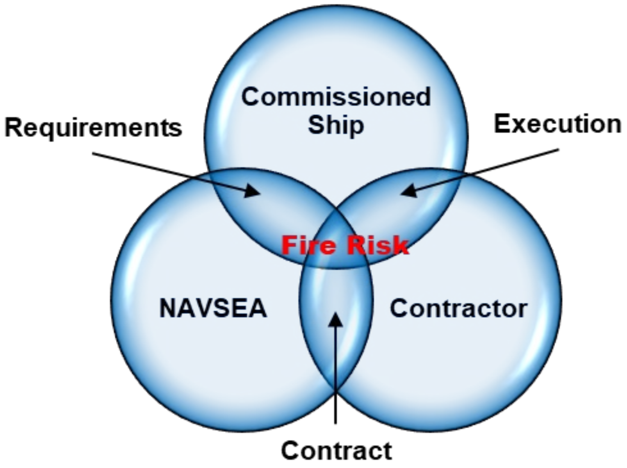


Figure 5. Relationship Between Risk Management Parties

While the responsibility for ship safety is shared, the contractor is directly responsible for occupational safety (DoN, 2020). Unlike in the commercial shipbuilding and repair industry, Navy ship maintenance contracts do not require the contractor to retain a significant marine builder's risk insurance policy, thus limiting the options for fire risk transfer between parties. This also limits the solution set for determining how to manage fire risk to what is in the contract, necessitating that the Government be specific in identifying fire protection and prevention measures above and beyond what is required by OSHA Standard 1915 Subpart P, *Fire Protection in Shipyard Employment.* The SUPSHIP Operations Manual states,

> Under vessel fixed-price contracts, the Government customarily assumes the same risk of loss or damage as would have been assumed by private insurance underwriters had the contractor obtained and maintained marine builders risk insurance. This risk is subject to a deductible as identified in the contract. (Naval Sea Systems Command, 2021, p. 3-101)

Transferring more of the liability for determining how to provide adequate fire protection and prevention for commissioned naval vessels to a contractor would have the unintended consequence of increasing the amount of insurance the contractor would need to carry in order to assume this liability.

Defense-in-Depth

Ships are most vulnerable to fire during construction and overhaul periods because the normal layers of protection are not present. Permanent fire protection systems may be out of service, fire resistant boundaries may be compromised, less of the ship's force is present, and many industrial workers are present. As opposed to strict controls on material aboard, temporary services are run throughout the ship, and a significant amount of combustible materials are brought on board. When a ship is at sea, sources of fire ignition are planned for in the design of protective measures. During industrial work, sources of fire ignition include industrial work evolutions, permanent or temporary services installed in the ship, and human causes such as discarded smoking materials or criminal acts. There is a high reliance on human intervention rather than a layered approach to protection, which can be a critical single point of failure in preventing the escalation of an incident.

Cynefin Domains

Within the “Policy and Organizational Commitment” pillar of the Navy SMS framework, it is important to recognize that different management approaches are required for different aspects of the problem. Approaching decision-making modalities from the correct domain is as important as making decisions at the right level. This could mean best practices (clear domain), good practices (complicated domain), evolutionary or novel approaches, or decomposing the problem in order to shift it into a domain where it is more easily managed. Table 3 provides examples of shipboard industrial safety problems that currently exist within each Cynefin domain. Note that from a programmatic standpoint, this topic currently exists in the confused domain at the intersection of other domains primarily due to identified gaps that will be discussed in more detail in a later section of this paper. The goal of implementing an SMS framework based on the CSG model and using the Cynefin framework to analyze it is to decompose the problem in a manner that makes it manageable.

Table 3. Industrial Fire Safety Examples in Each Cynefin Domain

Complicated	Clear
The work done by the welding engineer to determine the welding requirements and produce the technical work documents for a particular work evolution.	Skilled work (tasks) performed by a welder.
Complex	**Chaotic**
Interaction between welding (hot work) and the surrounding environment. Factors such as type of welding, proximity to combustibles, fire resistant and non fire-resistant separations, and adequacy of the fire watch all contribute to the safe execution of this work evolution.	Introducing a transient and unequally trained workforce with a few workers that may randomly decide to follow no rules into ship repair work evolutions. While emergence between sub-systems in the shipboard fire safety problem should be discernable, this is only possible when all agents are playing by an identifiable and uniform set of rules.
Confused/Aporetic	
From a programmatic standpoint, this is the current domain of shipboard industrial fire safety.	

System Architecture

The system of interest (SOI) in this paper, depicted in Figure 6, is a maintenance availability on a commissioned naval vessel (otherwise known as a project). Boundary conditions (other systems) that interact with this system include the acquisition system that contracts the work, the ship maintenance activity that undertakes the work, and the ship itself. The context includes the shipboard industrial fire safety system and associated requirements that are transmitted into the SOI by contract items and include reference to Manuals and Instructions.

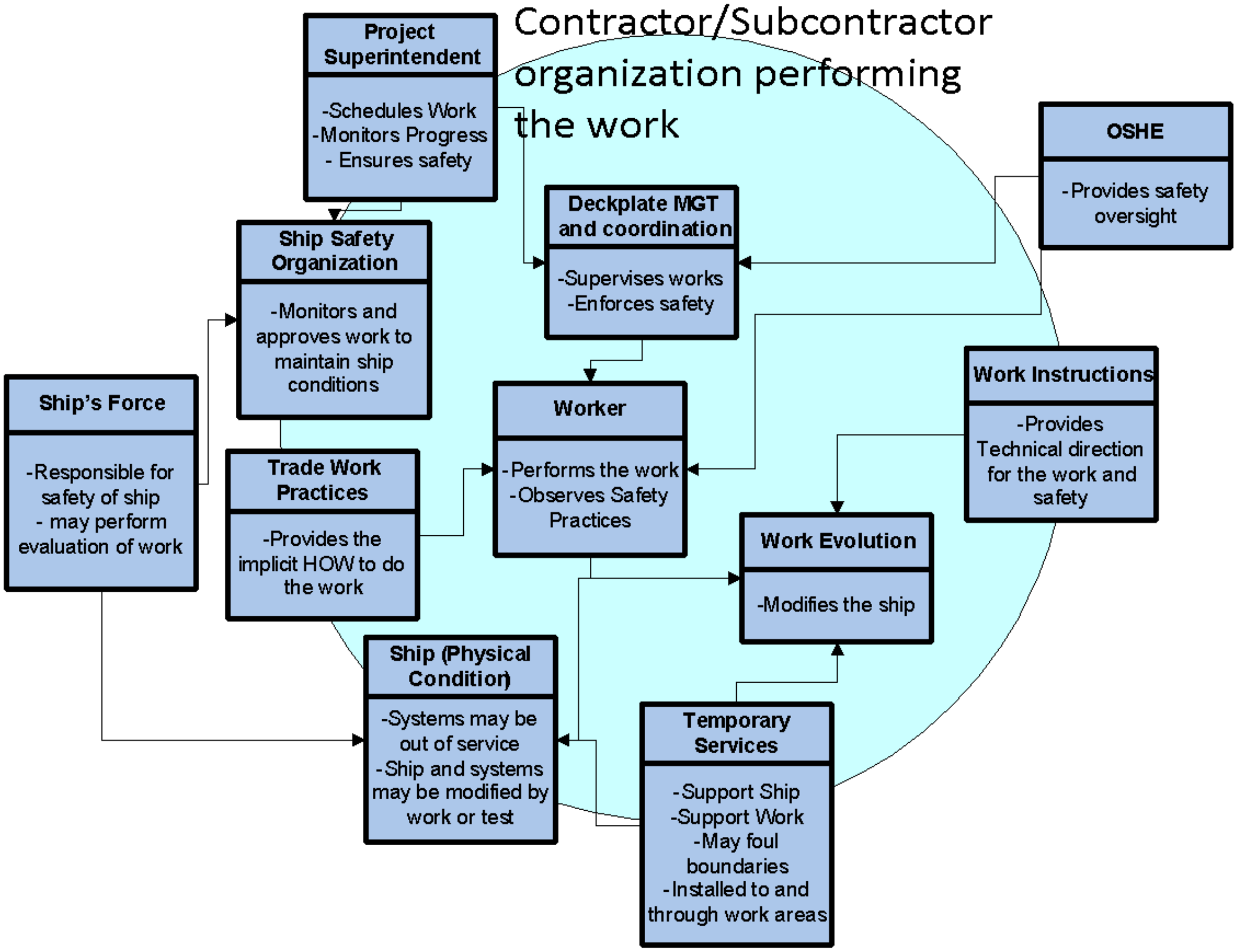


Figure 6. Architecture of System of Interest

SMS Framework and Complex System Governance Model

The governance model meta-function descriptions in Keating and Bradley (2015) provide the reference model assignments of requisite responsibilities and products. In Figure 7, we identify a preliminary assignment of the responsibilities with the corresponding meta functions. We also identify explicitly the governed systems (referred to as S1s) to place them in the appropriate location in the schema.

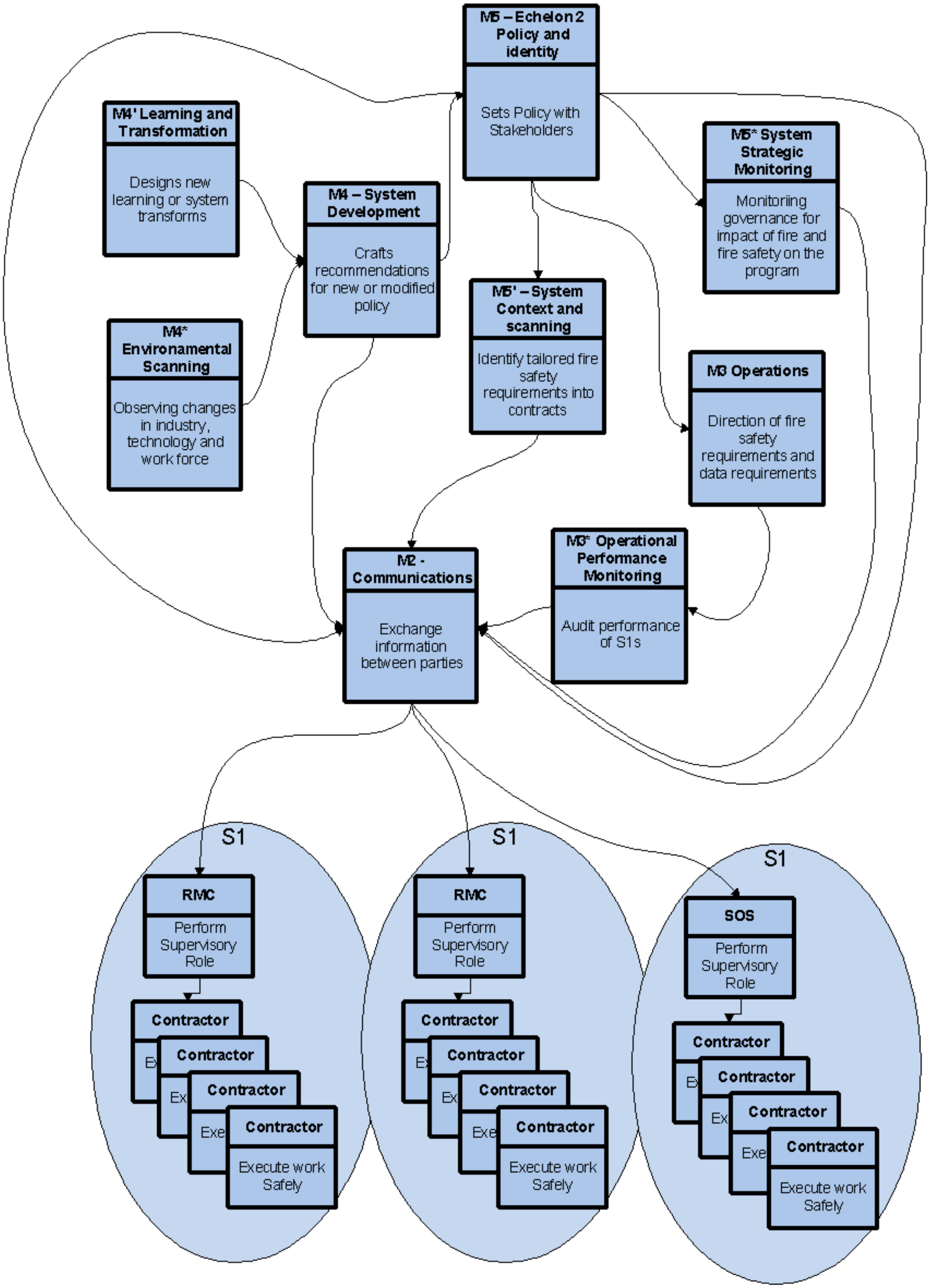


Figure 7. Metasystem Functions Identified for Shipboard Industrial Fire Safety Perspective

Setting policy at the NAVSEA Echelon 2 level that incorporates all the functions of the CSG model, which is inherently a risk communication and iterative continuous improvement cycle, can result in an SMS that is compliant with the new requirements for the Navy SMS framework. Developing procedures that adapt decision-making modalities and risk management practices based on system decomposition using the Cynefin framework support utilizing limited resources in a manner that is more likely to bring about meaningful change in shipboard industrial fire safety than seeking "one size fits all" solutions. Given that significant fires in the past decade on the USS *Gunston Hall* (LSD 44) and USS *Oscar Austin* (DDG 79) had similar root causes to historical fires on the SS *Normandie* and USS *Saturn* (AK 49), (McGowan & Smith, 2020), the current state mirrors NASA's "'failures of foresight' in which history played a prominent role" (CAIB, 2003, p. 195).

Identified Gaps

Technical Authority

There is not a single technical authority or TWH with responsibility for shipboard industrial fire safety. This role is split between NAVSEA 04RS responsibilities as the TWH for safety policy, NAVSEA 04X6 responsibility for maintaining the NAVSEA *Industrial Ship Safety Manual for Fire Prevention and Response (8010 Manual)*, and NAVSEA 05P responsibility for damage and survivability, which includes the ship's fixed fire protection systems. Other TWHs have input within their respective areas of responsibility, but decision-making and responsibilities do not roll up to a single entity. The lack of a TWH with overall responsibility can lead to issues such as contract negotiations over industrial fire protection and prevention requirements without the involvement of all relevant stakeholders.

Technical Cognizance

In conjunction with the lack of an overarching TWH, there is not a clear flow down of technical requirements or a single entity responsible for adjudicating technical issues that arise in the domain of shipboard industrial fire safety. Nor do the activities performing the work have specific requirements to house this technical expertise internally. Where requirements are not clearly defined and rooted with a technical basis, decisions are made at the deckplate by individuals who may or may not have the expertise to make them.

Weaknesses in Defense-in-Depth

Our initial work has indicated that the unwanted occurrence of significant fire events may be an indicator of an ineffective system to provide defense-in-depth. This potential gap will need to be explored further in later phases of this work.

Lags in Incorporating Lessons Learned Into Contracts

Technical requirements related to shipboard industrial fire safety are typically found in NAVSEA Standard Items (standard specifications for ship repair and alteration), either directly or by reference to other documents, which may or may not be incorporated into every contract. Lessons learned from the USS MIAMI fire are still not fully incorporated into NSIs 9 years later, and even when new requirements are invoked, the multi-year nature of ship maintenance availabilities means that contractual requirements typically lag current recommendations.

Contract Requirements Are Not Driven by Data

Trends are collected and analyzed by data; collection is not standardized and does not directly influence what is required in future contracts or contract modifications. Use of data is critical to the risk communication, risk monitoring, and change management fundamental elements of the Navy SMS framework. Within the CSG model, this reflects feedback loops between metasystems.

Conclusions

There is not currently a uniform level of industrial fire safety during ship maintenance availabilities, primarily because there is not currently a cohesive governance model or framework that is driving specificity of requirements to manage risk. Rather than the current state of rote compliance (or noncompliance) to general requirements, contractual requirements should be data driven and vary based on risk, and there should be clear technical authority over setting these requirements and technical cognizance in ensuring they are met. Feedback loops between requirements and outcomes in conjunction with faster routes (such as contract modifications) to incorporate lessons learned into ship maintenance contracts support a higher level of safety through better management of the risks involved. Note that the underlying goal is not necessarily to avoid all fire due to the nature of the work but have defense-in-depth and "right-sized" work controls to prevent major fires and reduce the impact of minor ones while not unduly impacting production schedule or project cost.

Planned Future Work

This paper is the first step in a concerted effort towards implementing data driven decision-making for industrial fire safety during ship maintenance availabilities by defining the governance model and SMS framework. NAVSEA 04RS has already done a significant amount of work analyzing human factors in historical fire incident data, and the intent is to continue to build upon their efforts. The next step is to further analyze available historical data to identify causal factors in why small fires become large, forming the basis of determining what standardized data needs to be collected to analyze future trends and inform contract requirements. We will also evaluate where and how more robust defense-in-depth principles can be incorporated. Then, we intend to create a standard data architecture and viewpoints for data-driven decision-making that could be implemented through creation of a new data repository held by a neutral third party.

The long-term vision is for decision support systems that are a model-based engineering cross between tools like the National Fire Incident Reporting System (NFIRS) database used for land-based fire reporting, the Aviation Safety Reporting System (ASRS) maintained by NASA for the Federal Aviation Administration (FAA), and more traditional project and program management dashboards. Having a tool such as this in the toolbox would allow the Navy, contractors, and the broader maritime repair industry to learn and evolve based on data from shipboard industrial fire incidents and near misses.

References

Aven, T. (2009). Safety is the antonym of risk for some perspectives of risk. *Safety Science, 47*(7), 925–930. https://doi.org/10.1016/j.ssci.2008.10.001

Aven, T., & Ylönen, M. (2018). A risk interpretation of sociotechnical safety perspectives. *Reliability Engineering & System Safety*, *175,* 13–18. https://doi.org/10.1016/j.ress.2018.03.004

Columbia Accident Investigation Board. (2003). *Report of Columbia Accident Investigation Board, volume I.* National Aeronautics and Space Administration. https://www.nasa.gov/columbia/home/CAIB_Vol1.html

Eckstein, M. (2020, July 22). *Stop-work order lifted at NASSCO-Norfolk after fire safety walk-through, training*. USNI News. https://news.usni.org/2020/07/22/stop-work-order-lifted-at-nassco-norfolk-after-fire-safety-walk-through-training

Fleming, K. N., & Silady, F. A. (2002). A risk informed defense-in-depth framework for existing and advanced reactors. *Reliability Engineering & System Safety*, *78*(3), 205–225. https://doi.org/10.1016/s0951-8320(02)00153-9

Geurts, J. (2020). *Memorandum for the shipbuilding and ship maintenance enterprise. Subject: Fire safety.* https://assets.documentcloud.org/documents/7007810/Fire-Safety-20200724-1.pdf

Gortney, W. (2012). *USS* Miami *(SSN 755) fire panel recommendations* (USFF ltr Ser N00/200). https://archive.org/details/ussmiamissn755firepanelrecommendations/mode/2up

Keating, C. B., Katina, P. F., & Bradley, J. M. (2014). Complex system governance: Concept, challenges, and emerging research. *International Journal of System of Systems Engineering*, *5*(3), 263–288.

Keating, C. B., & Bradley, J. M. (2015). Complex system governance reference model. *International Journal of System of Systems Engineering*, *6*(1/2), 33–52.

Keating, C. B., & Katina, P. F. (2019). Complex system governance: Concept, utility, and challenges. *Systems Research and Behavioral Science*, *36*(5), 687–705.

Keating, C. B., Katina, P. F., Jaradat, R., Bradley, J. M., & Hodge, R. (2019). Framework for improving complex systems performance. In *29th Annual INCOSE International Symposium Conference Proceedings*.

Kurtz, C. F., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal*, *42*(3), 462–483.

McDermott, J. (2013, November 13). USS *Miami* crew not exactly idle as ill-fated sub gets new skipper. *The Day*. https://www.theday.com/article/20131115/NWS09/131119792

McGowan, J., & Smith, S. (2020, September 29–October 2). *Industrial fire safety, fire prevention and control January 2017 - June 2019 self-assessment and recommendations* [PowerPoint presentation]. SNAME Maritime Convention, Virtual.

Möller, N., Hansson, S. O., & Peterson, M. (2006). Safety is more than the antonym of risk. *Journal of Applied Philosophy, 23*(4), 419–432.

Naval Sea Systems Command. (2021). *Supervisor of shipbuilding, conversion, and repair (SUPSHIP) operations manual (SOM)* (S0300-B2-MAN-010; Revision 2, change 32). https://www.navsea.navy.mil/Portals/103/Documents/SUPSHIP/SOM/SOM2008-14Jan2021.pdf

Ropohl, G. (1999). Philosophy of socio-technical systems. *Society for Philosophy and Technology Quarterly Electronic Journal*, *4*(3), 186–194.

Saleh, J. H., Haga, R. A., Favarò, F. M., & Bakolas, E. (2014). Texas City refinery accident: Case study in breakdown of defense-in-depth and violation of the safety–diagnosability principle in design. *Engineering Failure Analysis*, *36,* 121–133. https://doi.org/10.1016/j.engfailanal.2013.09.014

Society for Risk Analysis. (2018). *Society for Risk Analysis glossary.* https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Sorensen, J., Apostolakis, G., Kress, T., & Powers, D. (1999). On the role of defense in depth in risk-informed regulation. *Proceedings of PSA*, *99,* 22–26.

U.S. Department of the Navy. (1990). Chapter 8: The commanding officer. In *U.S. Navy regulations.*

https://www.secnav.navy.mil/doni/US%20Navy%20Regulations/Chapter%208%20-%20The%20Commanding%20Officer.pdf

U.S. Department of the Navy. (2020). *Navy safety and occupational health manual* (OPNAV M-5100.23). https://www.secnav.navy.mil/doni/SECNAV%20Manuals1/5100.23.pdf

Ziezulewicz, G. (2021, January 3). New in 2021: *Bonhomme Richard* will be turned into scrap. *Navy Times*. https://www.navytimes.com/news/your-navy/2021/01/03/new-in-2021-bonhomme-richard-will-be-turned-into-scrap/

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net