Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System

by

Paul D. Stukus

B.S. Naval Architecture and Marine Engineering
United States Coast Guard Academy (1994)

M.S. Naval Architecture and Marine Engineering
University of Michigan (1998)

M.S. Mechanical Engineering
University of Michigan (1998)

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology

June 2017

Signature of Author: _____

Paul Stukus
System Design and Management Program
May 10, 2017

Certified by: _____

Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: _____

Joan Rubin
Executive Director
System Design & Management Program

Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System

by

Paul D. Stukus

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

ABSTRACT

The Systems-Theoretic Accident Model (STAMP) developed by MIT's Dr. Nancy Leveson was applied in this thesis to a ship navigation control system used on U.S. Coast Guard buoy tenders.

The legacy system installed on the Service's 16 sea-going buoy tenders experienced numerous incidents that had potential to be hazardous to the ships and their crews. Faced with the dual needs of ensuring safety of mission execution and restoring confidence in the overall ship control system, yet faced with a limited budget, Coast Guard decision-makers elected to conduct a partial recapitalization of the system's hardware and software.

This thesis explores the application of system safety methods to analyze the legacy system on the sea-going buoy tenders. An accident analysis of a particular incident was conducted using STAMP methodologies, and its results were compared/contrasted with the results of a more traditional root cause failure analysis that was contracted by the Coast Guard following the incident. Several added insights pertaining to system safety and process improvement were obtained by using STAMP. Additionally, a hazard analysis was performed on the control system using STAMP techniques. This hazard analysis yielded 92 specific design requirements that may be incorporated into future system upgrades on these or similar vessels.

The thesis concludes that STAMP methodologies are appropriate to generate actionable recommendations for future control system upgrades on U.S. Coast Guard buoy tenders. It also concludes that STAMP techniques may lead to safer controls in the greater hierarchical control structure for shipboard buoy tending operations. Finally, suggestions are made for future research/application of STAMP principles in the Coast Guard's management of operational safety, asset acquisition, and cybersecurity.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics

Acknowledgements

I must first thank God above for granting me the fortitude to not only pursue an advanced degree from MIT, but to finish all degree requirements in nine months. The past several months have been grueling and rewarding in equal measure, and I know He was with me every step of the way.

I am deeply appreciative of the opportunity provided by the U.S. Coast Guard for me to continue to further my education – I hope that the contributions I make in my future military service proves the investment to have been worthwhile. I am truly fortunate to be a member of such an outstanding organization. Along these lines, particular thanks go to Chief Warrant Officers Alfonso "Ponch" Mejia and Sean Gabriel of the Coast Guard Surface Forces Logistics Center, who put up with my multiple requests for technical data in support of this thesis and delivered every time I asked. Thanks are also due to LCDR John Singletary, Commanding Officer of *USCGC Juniper*, who advised me from a system operator's perspective.

My studies at MIT exposed me to several academic departments, and one denominator was common to them all: exceptionally bright, energetic, and dedicated teaching staff – from the newest teaching assistants to the longest tenured professors. In particular, I earnestly thank Dr. John Thomas, who kindled my interest in STPA and then stoked it – all in one high-octane three-hour lecture. The timely and extremely valuable feedback that he provided while I drafted this thesis was indispensable. I am also thankful to Professor Nancy Leveson for taking me on as a thesis advisee and providing insightful guidance to maximize my learning experience. I also learned much from my exceptional colleagues within the 2016 MIT System Design and Management Cohort. It was both a rare opportunity and a fulfilling experience to "rub elbows" with such intellectual and entrepreneurial giants. I additionally thank Professor Amedeo Odoni, whose wise counsel helped me to organize my thoughts after I completed an exhausting schedule of seven courses during the Fall 2016 semester and then arrived at the realization that I needed to quickly devote some serious thought to a thesis topic and advisor. Special thanks is due to Joan Rubin, whose flexibility and big-picture perspective as SDM Executive Director allowed me to maximize the "MIT experience" while minimizing negative impacts on my family.

"Lifetime achievement" recognition is due to my mother and late father, Pauline and Peter Stukus. They raised me through my formative years without providing any external pressure (that I can recall) to work hard and succeed – I merely had to follow their example. Years of consistent moral support from my exceptional parents, siblings, and in-laws enabled me to complete this chapter of my life's journey.

To my children: Megan, Madeleine, and Cole – I am grateful to you for bravely enduring the family separation that resulted from my "deployment" to Cambridge. Once you got over the initial hilarity associated with the idea of your dad "going back to school," your love and unwavering support for me was overwhelming, and you continued to do great things without my presence at home. I suppose that shows that you really don't need me around in order to thrive and succeed, which is a condition that would make any parent very proud. Still, I missed you tremendously while I was away.

Finally, I sincerely thank my wife and best friend, Natalie. You pushed me to accept the opportunity to go back to school when it was offered, and you stalwartly anchored the family through numerous tempests (including several that were surely unknown to me) over the past nine months. To be clear: you own a big part of this degree; it would have been "unobtainium" without your efforts on the home front. Your unselfishness humbles me daily, and I am very lucky to be your husband. I love you!

Table of Contents

List of Acronyms

ATON	Aids to Navigation
C2CEN	Command and Control Center
C3CEN	Command, Control, and Communications Center
C4IT	Command, Control, Communications, Computers, and Information Technology
C4ITSC	C4IT Service Center
CASREP	Casualty Report
CAST	Causal Analysis Using STAMP
CCM	Casualty Control Manual
CG DDS	Coast Guard Data Distribution System
CG ECDIS	Coast Guard Electronic Chart Display Information System
CG-1	Assistant Commandant for Human Resources
CG-11	Assistant Commandant for Health, Safety, and Work-Life
CG-4	Assistant Commandant for Engineering and Logistics
CG-45	Office of Naval Engineering
CG-6	Assistant Commandant for C4IT
CG-64	Office of Enterprise Infrastructure Management
CG-7	Assistant Commandant for Operational Capability
CG-9	Assistant Commandant for Acquisition
CO	Commanding Officer
CPP	Controllable Pitch Propeller
CPU	Central Processing Unit
DCMS	Deputy Commandant for Mission Support
DCO	Deputy Commandant for Operations
DHS	Department of Homeland Security
DoD HFACS	Department of Defense Human Factors Analysis and Classification System
DPS	Dynamic Positioning System
ECC	Engineering Control Center

ECCC	Engineering Control Center Console
ECPINS	Electronic Chart Precise Integrated Navigation System
ELC	Engineering Logistics Center
EOW	Engineer of the Watch
HSWL SC	Health, Safety, and Work-Life Service Center
ILSMT	Integrated Logistics Support Management Team
ILSP	Integrated Logistics Support Plan
ISMT	Integrated Systems Management Team
ISST	Integrated Systems Support Team
IT&E	Integration, Test and Evaluation
LAN	Local Area Network
LBSF	Land Based Support Facility
MDE	Main Diesel Engine
MMA	Major Midlife Availability
MPCMS	Machinery Plant Control and Monitoring System
MSCC	Main Ship Control Console
MTL	Mandatory Training List
OEM	Original Equipment Manufacturer
ORD	Operational Requirements Document
SAFEnet LAN	Survivable Adoptable Fiber-optic Embedded Network
SCSC	Secondary Conning Station Console
SFLC	Surface Forces Logistics Center
SMEF	System Management Engineering Facility
SQL	Structured Query Language
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
Tri-P	Tri-Partite
UART	Universal Asynchronous Receiver/Transmitter
UCA	Unsafe Control Action

UPS	Uninterruptable Power Supply
USCG	United States Coast Guard
VDT	Video Display Terminal
VME	Versa Module Europa
VRU	Vertical Reference Unit
WLB	Sea-going Buoy Tender
WLM	Coastal Buoy Tender

Chapter 1 – Introduction and Background

"'Wouldst thou,' – so the helmsman answered,
'Learn the secret of the sea?
Only those who brave its dangers
Comprehend its mystery!'"

- Henry Wadsworth Longfellow (from the poem *The Secret of the Sea*)

1.1 Chapter Overview

This chapter introduces the reader to the Coast Guard Aids to Navigation mission and the evolution of the electromechanical systems used in practice to facilitate safer, more efficient mission execution. Technological advancements were applied to the latest classes of buoy tending cutters, resulting in the current Integrated Ship Control System – the analysis of which is the focus of this thesis. Chapter 1 describes the motivation behind this thesis and explains why this topic is of interest to the U.S. Coast Guard. Finally, primary research questions are posed that will guide the remainder of the thesis.

1.2 U.S. Aids to Navigation Overview and Historical Background

Over $2 trillion of commerce moves through the United States' 361 major ports each year, and maritime channels are responsible for moving more than 99 percent of the nation's cargo arriving from or destined to other countries [1]. The safety and security of maritime commerce entering and leaving America's ports is foundational to the U.S. economy and is thus a homeland security issue at its very core. One of the U.S. Coast Guard's 11 missions, authorized in statute by 14 U.S. Code § 81, is Aids to Navigation (ATON). The scope of this mission includes maintaining fixed and floating aids to navigation in U.S. ports and waterways, including all beacons and buoys.

The history of domestic ATON had its genesis long before the enactment of the current governing statute. Boston Harbor was the site of the first permanent lighthouse (constructed in 1716) in what was then the British colonies, and buoys were used to mark shipping approaches to Philadelphia on the Delaware River as early as 1767. The obvious benefits provided by well-managed lighthouses spurred federal legislation, which created the Lighthouse Establishment (which later evolved in the Lighthouse Service) to manage construction and maintenance of "lighthouses, beacons, and buoys…." This statute was enacted in the ninth act of the First U.S. Congress in 1789 – the fledgling nation's first public works act [2]. Subsequent records indicate the use of "floating beacons" in Chesapeake Bay as early as 1792 [3].

Incremental improvements to the short range ATON system were made over the next century, but the dichotomous architecture of fixed and floating aids remained in place. In 1939, the Bureau of Lighthouses (which was created and given control of the Lighthouse Service in 1910) was brought under the control of the U.S. Coast Guard, which has since been responsible for all federally managed aspects of safe navigation within navigable U.S. waterways [4]. While custody of the majority of lighthouses has since been transferred to private concerns, the Coast Guard retains management of other fixed and floating ATON, including day boards, range markers, and buoys. Today, 78 years later after the Bureau of Lighthouses was folded into the U.S. Coast Guard, the Coast Guard is responsible for maintaining over 33,700 buoys and beacons.

The constellation of short range ATON in the U.S. and its territories provides mariners with a visible (and, in many cases, audible) means to determine their position relative to hazards to navigation on their approaches to and departures from port. It also marks the boundaries (and sometimes the center)

of shipping channels, allowing navigators to determine the safety of their vessels' current course or planned track. Given the economic and security implications of any potential disruption to the flow of shipping to and from ports, these aids must be kept reliably on-station, with the proper visible and audible characteristics. According to an email to the author from CDR Justin Kimura of the Coast Guard's Office of Navigation Systems, which has direct responsibility for managing this mission, the goal for aid availability is 97.5%. This high level of availability is achieved, in large part, by Coast Guard buoy tenders and their crews. Buoy tenders are ships (or "cutters" in Coast Guard parlance – a nod to the Service's roots as the Revenue Cutter Service, established upon the recommendation of Treasury Secretary Andrew Hamilton in 1790) that specialize in setting, retrieving, and maintaining buoys.

Buoy servicing is an inherently dangerous and complex evolution that is carried out by Coast Guard crews on a daily basis from Apra Harbor, Guam to Booth Bay Harbor, Maine – and on all navigable U.S. waterways in between. The cutters responsible for the majority of coastal and "off shore" ATON are the WLM and WLB class cutters, termed as coastal buoy tenders and sea-going buoy tenders, respectively. The design of the current generation of sea-going buoy tenders (also known as the "*Juniper* class" or "225s") and the coastal buoy tenders (alternately referred to as the "*Keeper* class" or "175s") incorporated modern technologies intended to greatly increase efficiency in both ship maneuvering and buoy positioning. For many years, buoys were positioned by application of horizontal sextant angles to define a location via three points and two lines of position [5]. While generally effective, this method was subject to sextant instrument error, sextant operator error, chart plotting error, and instability induced by sea swells on the cutter's position. Furthermore, positioning a buoy via this method was both time and manpower intensive.

Design specifications for the 225s and 175s included a dynamic positioning system (DPS) which, when interfaced with propulsion and steering controls, would have the ability to hold the cutter at a desired position by applying DGPS (Differential Global Positioning System) input and/or a desired heading using gyrocompass input. Additionally, the cutters were designed with the option to have their steering controlled by autopilot, which receives input from the electronic charting system, Doppler speed log, and gyrocompass. The first of each class of these new cutters were delivered from the shipbuilder in the mid-1990s. Not only did implementation of this new system architecture improve the accuracy of actual buoy placement, it also improved efficiency by decreasing both the time required to set a buoy and the minimum crew compliment necessary to carry out the evolution. This overall integrated system of navigation, propulsion, and steering subsystems (and its related sensors and networks) is referred to as the Integrated Ship Control System, or ISCS.

1.3 Thesis Motivation

"The Blue Book says we've got to go out, and it doesn't say a damn thing about having to come back."

- Patrick Etheridge, Keeper of Cape Hatteras Life-Saving Station, 1891 – 1909

"…Today, we disavow this motto – we like all our aviators and shipmates to return after every mission!"

- Robert Papp, 24th Commandant of the U.S. Coast Guard, in an address to cadets at the U.S. Coast Guard Academy, January 2012

On the morning of August 16, 2013, the United States Coast Guard Cutter (USCGC) *Elm* was underway in the vicinity of Fort Macon, NC for operational testing of a new electronic charting system, new radar, and upgraded differential global positioning system (DGPS) receiver. Prior to departing port, all pre-underway checks, including propulsion and steering, were satisfactorily completed. Upon entering the Morehead City turning basin at 10:23, the Conning Officer placed *Elm* in "hold position," an operating

mode of the vessel's dynamic positioning system (DPS) that is intended to control the ship's thrust in such a way as to offset the effects of wind and current and thus maintain position within 2 meters of the ordered coordinates. The Conning Officer proceeded to test the heading control knob at the DPS console by ordering a twist (yaw) to port. Instead of maneuvering as intended, the DPS relinquished control of the propulsion plant and steering. Attempts by the Conning Officer and the Officer of the Deck to transfer propulsion control modes on the bridge yielded negative results.

As the vessel drifted toward shoal water with no propulsion controls, the Officer of the Deck ordered the Boatswain to let go the starboard anchor. At this point, with the DPS controls and manual bridge controls both in the neutral position, the propeller pitch moved to 60% astern, and *Elm* began backing down from her anchored position. The Conning Officer depressed the main engine emergency shutdown button located on the bridge, at which time alarms indicated loss of both the primary and secondary propulsion control computers. Commercial tug assistance was requested via VHF radio, and the port anchor was lowered to minimize any further drift. At this point, *Elm's* stern was only 30 yards from a shoal, and an ebb current was pushing the ship toward it.

At 10:34, a toxic gas leak alarm annunciated, and the Officer of the Deck set the General Emergency Bill, initiating procedures to control and respond to vessel damage and threats to personnel. Upon entering the affected space, the damage control response team found the source of the toxic gas lead to be a leaking valve on one of the ship's refrigeration units. The leak was secured without further incident.

In the meantime, tugs arrived and mated up to *Elm* to assist her into port. *Elm's* Commanding Officer ordered the engines restarted, clutched in, and passed to bridge control. Propulsion checks were unsatisfactory, as the bow and stern thrusters did not remain energized. As a result, the Conning Officer passed propulsion control back to the Engineering Control Center, and the main engines were declutched. *Elm* embarked a harbor pilot and proceeded to be towed by tug to her mooring at Fort Macon.

The mishap described above ended without injury or significant damage. The potential for the mishap to have cascaded into a much more damaging incident is obvious. The ship was only minutes from running aground which, at a minimum, would have endangered the ship's structure and equipment – to say nothing of potential injury to personnel. The violent motion and vibration associated with the ship backing down while at anchor precipitated a localized toxic gas leak, but fortunately one that emanated from a source with relatively low acute toxicity and that was easily contained.

In accordance with established policy, *USCGC Elm's* command filed an official report detailing the circumstances of the mishap. The "narrative" section of the mishap report contained a reasonably detailed account of the environment and circumstances leading up to and immediately following the loss of propulsion control. In contrast to this level of detail, the "cause" section of the mishap consisted of only one word: "failure."

1.4 Background of WLB Control System Issue

The August 2013 incident onboard *USCGC Elm* was not the first time that automatically controlled propulsion and steering response was severely outside of expected parameters on a sea-going buoy tender. *Elm's* narrow escape from a grounding was a galvanizing event in achieving positive momentum toward isolating the issues and proposing fleet-wide solutions. In accordance with standard procedures, a Root Cause Failure Analysis (RCFA) was ordered by the Coast Guard Surface Forces Logistics Center

(SFLC). (The results of this RCFA are discussed in detail in Chapter 6 of this thesis.) One outcome of the events onboard *Elm* (and other cutters) was that the WLB fleet's Commanding Officers experienced a crisis of confidence in their cutters' ISCS to function properly.

With the Coast Guard's ability to complete its ATON mission and the safety of cutter crews hanging in the balance, the Service's senior leadership demanded a solution that would return the cutters to safe and reliable operation as soon as possible. The number one priority for the Coast Guard's naval engineering support network was clearly stated in tasking from Rear Admiral Mark Butt, the Assistant Commandant for Operational Capabilities, during a situation brief delivered in Summer 2014: "Restore the (WLB) operators' confidence in the ISCS." All major stakeholders understood that a necessary precursor to any meaningful restoration of confidence was demonstration of a safe and fully supportable system. By the very nature of their mission, buoy tenders operate at the margins of navigable waterways, where reaction time is crucial. Any compromise in maneuvering performance may translate directly to endangering the cutters and their crews.

A project team was formally chartered and was provided with unfettered access to subject matter experts. After initial scoping meetings, data analysis, and proposal reviews, the team recommended and received approval for a "partial system recapitalization" of the WLB Machinery Plant Control and Monitoring System (MPCMS) – a subsystem of the ISCS that directly controls propulsion machinery. This recapitalization was scoped to result in new processing computers, upgrading from Versa Module Eurocard-based computers to state-of-the-market industrial computers, as well as updated software code to operate the system. Other parts of the existing MPCMS infrastructure (and the larger ISCS infrastructure) would largely remain in place. This recommendation was approved by senior leadership as the solution that best optimized a timely return to safe and reliable operations without exceeding budgetary allocations. Installation and laboratory testing of the upgraded hardware and software began in Spring 2015 at the Coast Guard's ISCS land-based support facility (LBSF). Prototype shipboard installation began on *USCGC Juniper* in October 2015, and all 16 WLBs are scheduled to have received these upgrades by Summer 2017.

Crew safety was the primary concern of all parties involved in the effort to remediate the WLB ISCS issues. However, no rigorous system-based safety analysis was conducted as part of the project. The project team consulted human factors integration experts, whose feedback was directly incorporated into system controls and graphic user interfaces. Additionally, subcontracted consultants provided software optimization guidance to the prime contractor. However, the learning curve to integrating a working prototype was steeper than initially anticipated.

The WLM ISCS is very similar to the WLB ISCS, and similar safety concerns have been noted. As with the WLB ISCS, the "weakest link" appears to be the MPCMS and its rapidly diminishing commercial hardware and software support. A partial system recapitalization for the WLM MPCMS (and integration with the rest of the ISCS) is currently in the planning stage. Both the WLB and WLM ISCS will require robust lifecycle support to avoid future crises borne of diminished manufacturer product technical support, decreased ability to economically manufacture components, and asynchronous system evolution. The Coast Guard must capitalize on lessons learned from prior mishaps and the WLB MPCMS recapitalization effort when it moves forward with the WLM project. It is the goal of this thesis to shed light on system safety aspects of integrating improvements into the existing MPCMS and ISCS.

1.5 Research Questions

The research questions considered throughout this thesis are as follows:

- Are STAMP methodologies appropriate for use to generate actionable recommendations and requirements for future control system upgrades onboard U.S. Coast Guard buoy tenders?

- Are STAMP methodologies appropriate for use to provide greater insights that may lead to safer controls in the greater hierarchical control structure for U.S. Coast Guard buoy tenders?

Chapter 2 – Literature Search

"A system is not the sum of its parts, but the product of the interactions of those parts."

- Russel Ackoff, American operations research and systems thinking pioneer

2.1 Chapter Overview

This chapter presents the results of personal research into multiple existing safety analysis approaches that are important to understanding a number of methods that are widely used in practice today. The compendium offered in this chapter is not exhaustive, but is intended to lead the reader through advantages and disadvantages of selected methodologies, particularly when considering their application in analysis of complex systems. Description of the evolution of system safety analysis highlights the primary benefits of particular methods, and ultimately the conclusion is made that a more systems-based emphasis and approach is desired. The chapter concludes with a brief personal example of the importance of a systems-based approach to safety analysis.

2.2 The Roots and Evolution of System Safety Analysis

Safety culture has significantly advanced since the rapid industrialization of the U.S. economy that began in the 1880s. Passage of workers' compensation laws and formation of the National Safety Council in the earlier half of the twentieth century increased the attention that employers paid to industrial safety. This level of consideration was further increased and regulated by the formation of the Occupational Safety and Health Administration and the Mine Safety and Health Administration in 1970. Developments in accident modeling accompanied the increased spotlight on industrial safety, and preventive hazard analysis gained momentum as a field of study. It is instructive to understand these foundational theories, how they individually contribute the body of knowledge regarding safety analysis, and how they incrementally factor into a system safety approach. The following subsections provide a description of some of the seminal models that have influenced the approach taken by both industry and government (including the U.S. Coast Guard) to safety management through accident modeling and hazard analysis.

2.3 Accident Models

"All models are wrong, but some are useful"

- George Box, British statistician and quality control theorist

Dr. Nancy Leveson defines the word "accident" as "an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss." This is differentiated from an "incident," which is defined as "an event that involves no loss (or only minor loss) but with the potential for loss under different circumstances [6]." Clearly, both accidents and incidents are to be avoided whenever possible. Knowing *what* to avoid (i.e., an accident) is fairly trivial knowledge. It is knowing *how* to avoid accidents that provides the analyst, manager, worker, insurance underwriter, etc. with real value. To prevent accidents, hazards must be avoided. Leveson defines a hazard as "a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident [6]."

2.3.1 Chain of Event Models

2.3.1.1 Heinrich's Domino Model

In his 1931 text *Industrial Accident Prevention*, Herbert Heinrich described three basic principles of accident prevention:

1. Creation and maintenance of active interest in safety,
2. Fact finding, and
3. Corrective action based on the facts.

In further developing an approach to accident prevention, he explained a preventable accident as one of five factors in a sequence that results in injury. (Heinrich was primarily concerned with industrial accidents.) He represented these factors as a series of dominoes, as shown in Figure 2.1. The visual progression shows that satisfying one factor would lead to its "domino" falling, which would then impact the next factor, causing its domino to fall, and so on.

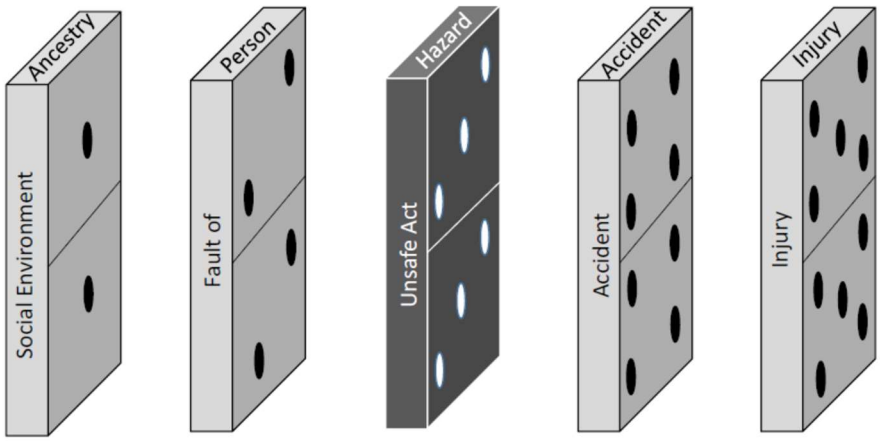


Figure 2.1 – The Five Factors in the Accident Sequence [7]

The first accident factor is ancestry and social environment. This assumes nature *and* nurture effects at work in the accident sequence. Heinrich presumed that some undesirable traits (e.g., recklessness, stubbornness, excitability, etc.) could be inherited and others (e.g., ignorance of safe practice, inconsiderateness, etc.) may be developed due to environmental causes, leading to what he termed "faults of person." These faults of person are the second accident factor, and are assumed to be proximate reasons for committing unsafe acts. Left uncorrected, these faults of person could lead to an unsafe act, whether through horseplay, removal of safeguards, or some other action. This unsafe act would then lead to the fall of the fourth domino in the sequence – the accident itself. Heinrich defines an accident as "an event in which (*a*) the contact of a person with an object, substance, or another person, or (*b*) the exposer of a person to objects, substances, other persons or conditions, or (*c*) the movement of a person, causes personal injury or suggests the probability of such injury [7]." The final accident factor in this model is any injury that results from the accident.

Heinrich focused on the central factor – i.e., unsafe control act/mechanical hazard. He posited that removal of this factor would make the action of the preceding factors – ancestry/social environment and fault of person – ineffective.

This model clearly focuses on individual persons and their place in the accident/loss sequence. The focus is on identifying unsafe actions and then reversing them. An example of an unsafe action may be ignorance of safety procedures; it could be reversed by providing effective training on safety procedures. A limitation of Heinrich's model is its one-dimensional nature. The accident and injury occur as part of a chain, visualized by falling dominoes, with no other influencers. Similarly, the domino theory does not consider methods of preventing accidents through means other than removing a factor from the linear event chain. Finally, this model makes the somewhat implicit assumption that an accident is produced by a single root cause. While this technique may be helpful in eliminating accident causes that are "low hanging fruit," it becomes myopic beyond identification of causes in the linear event chain that it describes. Restriction to one dimension constrains deeper analysis that may otherwise discover less obvious causal factors.

As noted by Thomas [8], the assignment of a primary or root cause of an accident may be influenced by factors pertaining to legal liability. Depending on the perspective (in terms of politics, funding sources, etc.) of the investigator, there may be a subconscious tendency to find a single root cause and then simply conclude the analysis if the root cause identified is deemed satisfactory for his or her purposes. In this way, a "root cause" can be seized upon to shape conversations in the news media that could potentially influence legal settlements or judgements that can run into the millions of dollars. A recent example may be observed in the lawsuit filed by a Tesla Model X owner against Tesla Motors, Inc. The owner alleged that his vehicle suddenly accelerated while he attempted to park it in his garage. According to the lawsuit, "The vehicle spontaneously began to accelerate at full power, jerking forward, and crashing through the interior wall of the garage, destroying several wooden support beams in the wall and a steel sewer pipe, among other things, and coming to rest in the plaintiff's living room [9]." The driver and his passenger each sustained injuries. Tesla's review of the computer logs from the accident led to their conclusion that the root cause of the accident was driver error. As stated by Tesla CEO Elon Musk, his cars "do not accelerate without the driver instructing it [sic] to do so." However, given the high degree of complexity associated with autonomous vehicles, a linear analysis and assignment of a single root cause would not be appropriate. Sensor inputs, control commands, and the operator's mental models must all be considered, along with other factors that influence the system.

2.3.1.2 Bird and Loftus' Domino Model

Bird and Loftus built upon Heinrich's model more than 40 years after it was originally published. The definition of accident used by Bird and Loftus was "an undesired event that results in physical harm to a person or damage to property." They went on to further specify their definition by stating that an accident "is usually the result of a contact with a source of energy (i.e., kinetic, electrical, chemical, thermal, ionizing radiation, non-ionizing radiation, etc.) above the threshold limit of the body or structure [10]." They identified four elements – people, equipment, material, and environment – that could be (alone or in combination) the source of accident causes. Using these insights, the domino sequence was updated to show direct management relationships (Figure 2.2).

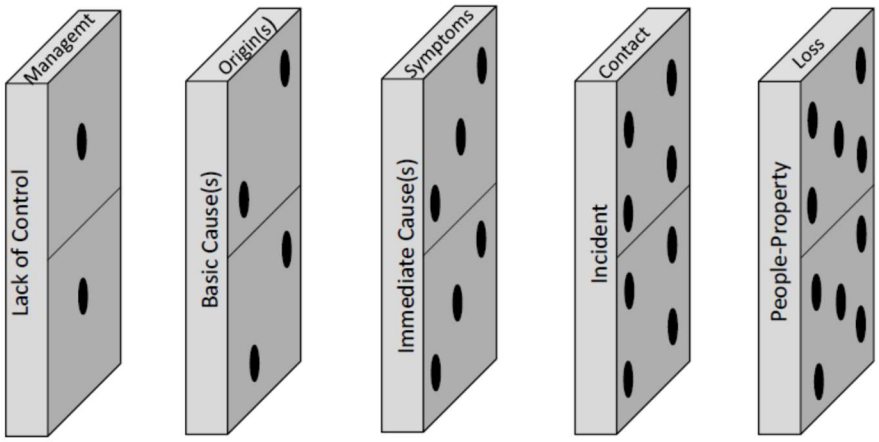


Figure 2.2 – Circumstances That Lead to Loss [10]

Similar to Heinrich's model, Bird and Loftus' paradigm is presented as a series of five dominoes. The first factor is a lack of control by management – specifically, regarding functions related to planning, organizing, leading or controlling. This may be manifested in inadequate program plans or standards, or in failure to comply with established standards. The second factor described is basic cause(s), which may be termed as the existence of personal and/or job factors. Personal factors include lack of skill, knowledge, or motivation, as well as mental or physical impediments to performance. Job factors are comprised of inadequate standards, design, and/or maintenance, as well as normal wear and tear or abnormal usage of a system component. When one or more of these basic causes exist, they open the window for error, which Bird and Loftus define as "any deviation from an accepted standard or practice." Error – or immediate causes – is the third domino in the series. However, Bird and Loftus recognized that errors (alternatively called substandard practices and conditions, or unsafe acts and conditions) are merely symptoms of a basic cause that permitted their existence. As they stated, "When we fail to determine what the basic causes behind the symptoms really are, we fail to keep this domino from falling, and the direct potential for loss exists [10]." The fourth factor is described as the incident. The incident does not necessarily result in loss. In fact, Bird and Loftus pointed to a 1969 study that inferred a 1-10-30-600 ratio. That is, for every one disabling injury sustained as a result of a reported accident, there were 10 accidents resulting in minor injuries, 30 accidents resulting in property damage, and 600 reported incidents with no visible injury or damage (sometimes referred to as "near miss" incidents). Finally, an incident that directly leads to loss involving people or property is the final domino to fall. Whether an incident becomes an accident is described as being subject to chance.

The enhanced domino event chain model proffered by Bird and Loftus refined Heinrich's work and began to open the door to consideration of accident causes that go beyond identification of a single root cause. The acknowledgement of "underlying causes" and the effects instigated by these often sleeping giants was a step toward a systems approach to safety. In fact, Bird and Loftus' 1976 book *Loss Control Management* (in which they describe their modifications to Heinrich's model) includes a chapter specifically devoted to system safety. They define the system safety concept through the following four points:

1. The pre-accident identification of potential hazards.

2. The timely incorporation of effective safety-related design and operational specifications, provisions, and criteria.
3. The early evaluation of design and procedures for compliance with applicable safety requirements and criteria.
4. The continued surveillance over all safety aspects throughout the total life-span, including disposal [10].

For these purposes, the authors define a system as "the sum total of all elements working together within a given environment to achieve a given purpose or mission [10]." They also stress the importance of defining the system boundary, which may include environmental factors beyond the system's physical components. Figure 2.3 is adapted from Bird and Loftus' work.

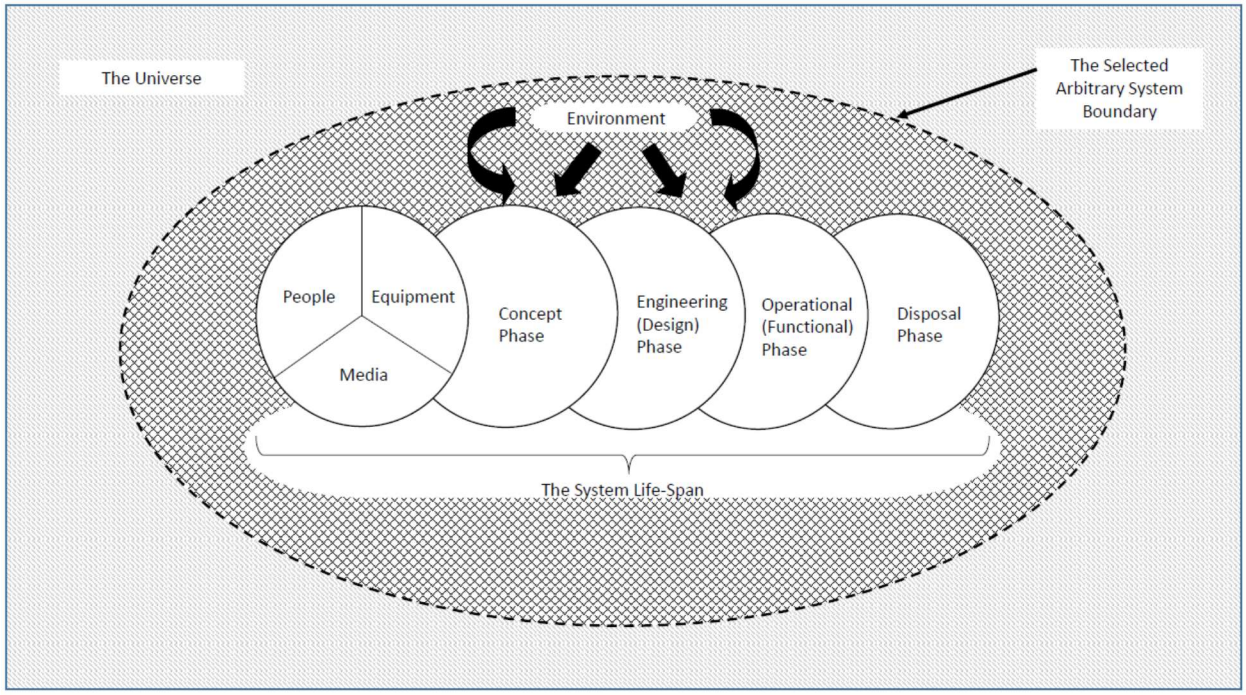


Figure 2.3 – The System Concept [10]

2.3.1.3 Reason's Swiss Cheese Approach

The Swiss cheese model, suggested by James Reason, focuses on the human elements of accident causation. It is depicted as a progression of successive barriers between local hazards and potential accidents. Each barrier has areas of weakness that may be penetrated by a hazard. These areas of weakness are shown as holes, hence leading to the moniker "Swiss cheese." Unlike Swiss cheese and its mostly static and highly visible holes, the gaps in each of the model's "slices" are continuously opening, closing, and in motion. Gaps are caused by unsafe acts and latent conditions. These latent conditions may be comprised of fallible decisions by management, deficiencies in line management/supervision, and psychological precursors of unsafe acts. The latent conditions pre-exist a loss event which, in previously considered models, were presumed to spawn only from active failures such as unsafe acts.

While Reason's model has evolved somewhat through the years, the basic premise remains unchanged [11]. A visual interpretation of this model is shown in Figure 2.4.

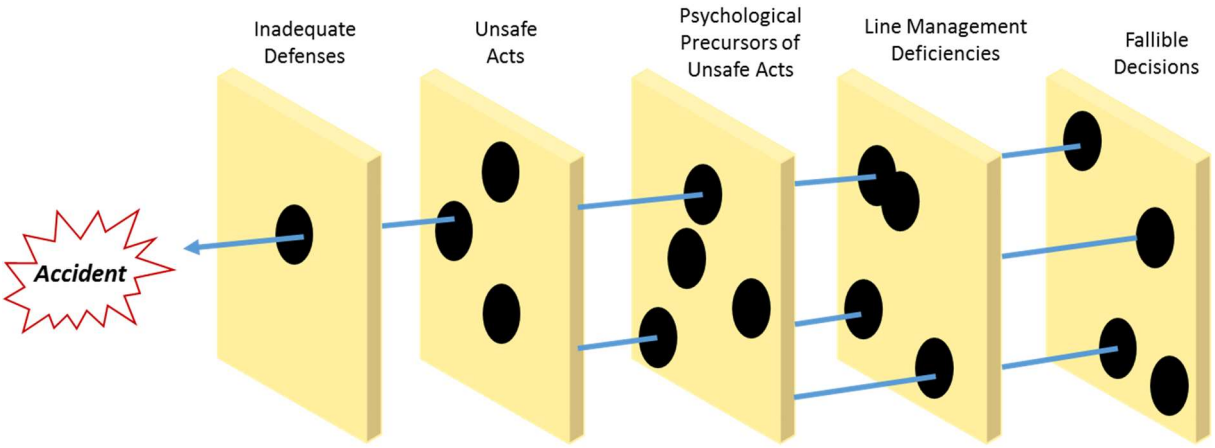


Figure 2.4 – Human Contributions to the Breakdown of Complex Systems [11]

Perhaps the "slice" that is the most difficult to intuitively understand is "psychological precursors of unsafe acts." Reason refers to these as "latent states," which "create the potential for a wide variety of unsafe acts" and are often characterized by stochasticity. These precursors include: "the capacities for being stressed, failing to perceive hazards, being imperfectly aware of the system, and having less than ideal motivation." Several of these may be by-products of negative life events, but Reason asserts that they may be accentuated or mitigated depending on decisions made at upper levels of management and communicated by the line management level [12].

In a later version of this model, Reason depicted a "slice of cheddar" at the end of the succession of Swiss cheese slices. The cheddar represents coping resources that effectively block the event trajectory that could lead to an accident. Using the metaphor of a mouse, Reason explains that this slice of cheddar gets "nibbled away" by "accumulated stresses associated with minor events." In this way, it is shown that even stout defenses can weaken to the point of failure due to the persistent pressure that may accompany repeated minor events [11].

Reason describes what he calls "the ironies of automation." In many complex systems that employ computer controls, human operators are required to monitor the controlled system to ensure that the desired automation is properly functioning. It is ironic that the potential for human operator error, one of the reasons to automate many systems in the first place, is re-introduced in system supervisory mode. Reason explains the "Catch 22" of human operator supervisory control as follows:

> The first part of the catch is thus revealed: Why do we have operators in complex systems? To cope with emergencies. What will they actually use to deal with these problems? Stored routines based on previous interaction with a specific environment. What, for the most part, is their experience within the control room? Monitoring and occasionally tweaking the plant while it performs within safe operating limits. So how can they perform adequately when they are called upon to reenter the control loop? The evidence is that this task has become so alien and the system so complex that, on a significant number of occasions, they perform badly [12].

2.3.2 Hierarchical Approaches

2.3.2.1 Lewycky Model

In his model, Peter Lewycky proposes a three-level representation of accidents. He uses the lowest level to describe the accident mechanism and the second level to list the conditions (or lack thereof) that enabled the lowest level events to occur. The top level includes constraints (or lack thereof) that enabled the conditions at the second level to exist, thus allowing the events that occurred at the first level. In this model, the third level is considered to be the home of the root causes of an accident [6]. This hierarchical approach goes deeper than event-chain or Swiss cheese models. The tiered analysis peels back the layers until organizational deficiencies are revealed that are at the "root" of the accident. The thought process involved may be compared to different approaches used in removing dandelions from one's lawn – to only cut a dandelion with a lawnmower will result in return of the dandelion. However, if you carefully remove the entire root, the dandelion (at least *that particular dandelion*) will not grow back. In a similar way, a hierarchical analysis decreases the tendency to apply "band-aids" as a final corrective action.

The mechanism of an accident is where energy is transferred between physical objects, and it is usually described via transitive (action) verbs. While the mechanism may seem obvious, it must be fully understood by the analyst to determine the necessary conditions and constraints. The conditions (level 2, as shown in Figure 2.5) refer to the existing circumstances which allowed the exchange of energy (mechanism) to occur. Examples of conditions include lighting, temperature, humidity, level of worker training/experience, etc. Level 3 represents what Lewycky refers to as "elements amenable to modification" or, more simply, constraints. These are circumstances which would exist whether or not an accident occurred. They may include technical and physical conditions (e.g., equipment design), social dynamics of the workplace (e.g., strength of supervision, individual knowledge, or worker selection), and the management system (e.g., planning, worker remuneration, maintenance procedures, or human resources planning). Lewycky states that "an accident investigation is 'Complete' when we have taken our discussion to this third level and are in a position to present recommendations that relate to each of the three aspects at this level [13]."

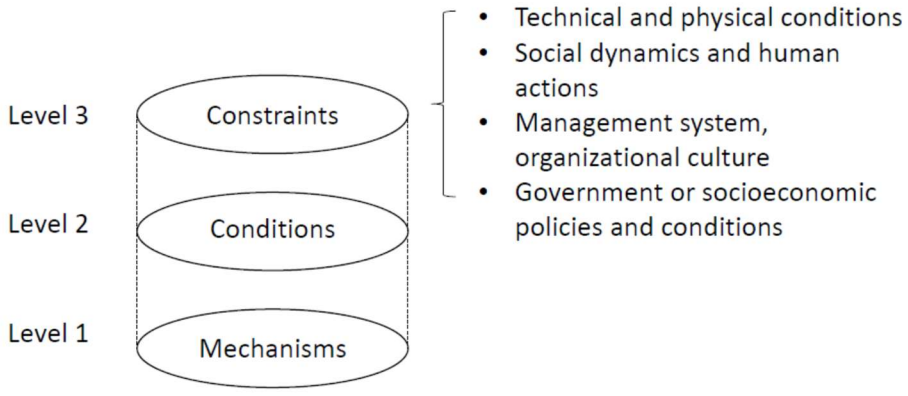


Figure 2.5 – Lewycky's Control Hierarchy [13]

2.3.2.2 NTSB model

The U.S. National Transportation Safety Board (NTSB) introduced a model during the 1970s that depicted accidents as patterns of direct events and causal factors that arise from contributory factors.

The contributory factors are spawned from systemic factors. This is similar to Lewycky's model, as it has three levels. This representation moves closer toward a systems thinking approach to accident modeling, and it has been applied by the NTSB in investigating road, air, rail, and marine accidents. Such a model could be easily adapted to examine a ship positioning control system, which integrates multiple constituent systems. Figure 2.6 is a general schematic of the theory behind the NTSB model.

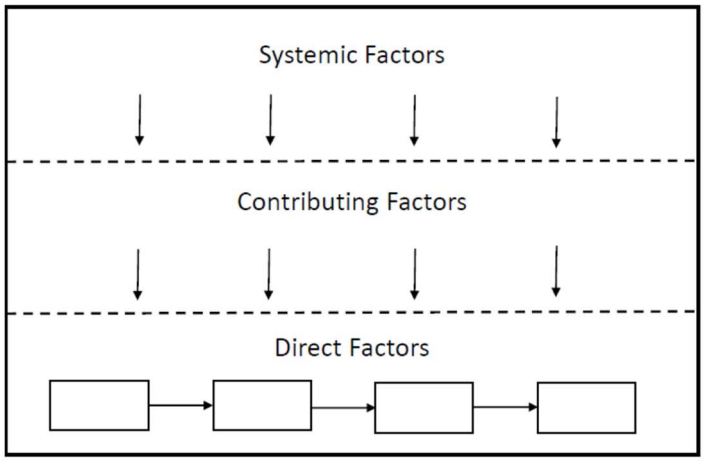


Figure 2.6 – NTSB Accident Causation Model [6]

Figure 2.7 shows an example of how the NTSB framework may be employed to analyze an accident. While "boys will be boys" may be a true enough adage, this example clearly demonstrates that preventively addressing systemic and contributing factors could have averted an accident caused by the boy being a boy.

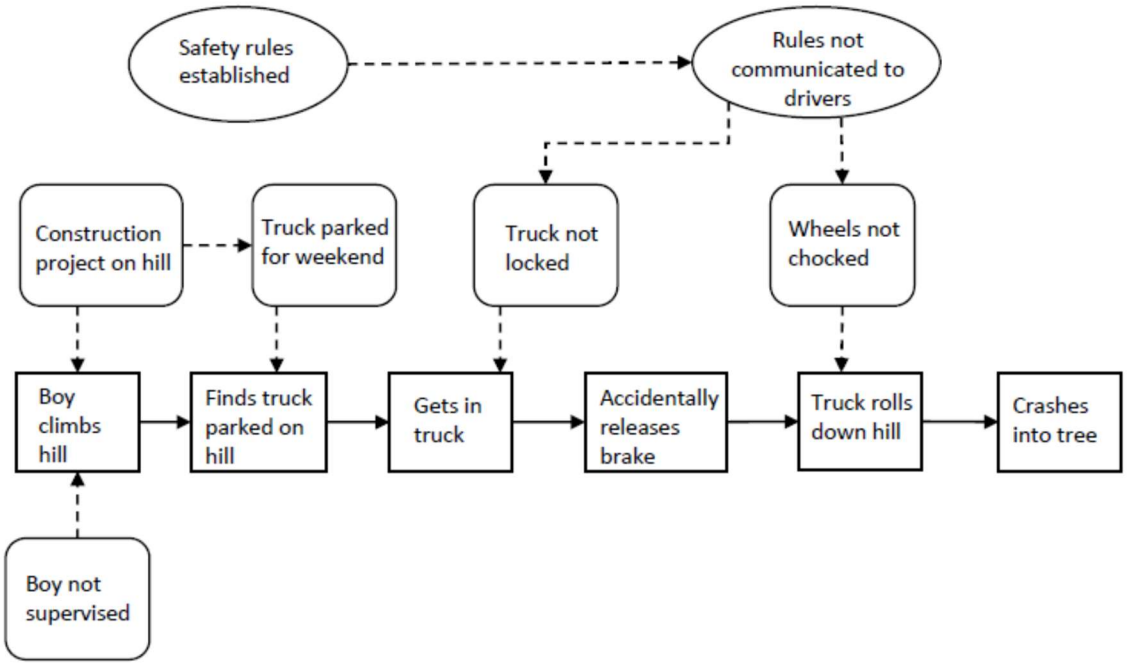


Figure 2.7 – Example NTSB Accident Causation Model Analysis [6]

2.4 Hazard Analysis Methods

"The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand."

-Sun Tzu

The many different accident models in existence, including those summarized in this chapter, provide a framework for understanding how accidents happen. It can be seen from examination of many of these models that the "element of chance" certainly comes into play and ultimately makes the difference between an accident happening (which, by most definitions, involves some type of injury or loss), an incident (an event not involving significant loss) occurring without notice, or a latent breakdown in the control of some element of the system control structure. Whether looking at a chain of events model or a hierarchical approach, it is apparent that the probability distributions of multiple conditions and events impacts the ultimate probability of an accident – similar to the visualization of Reason's Swiss cheese model.

It makes sense, then, to explore ways to prevent accidents by eliminating hazards. This proactive approach is exhibited in the use of various hazard analysis and modeling techniques. Hazard models are just that – models (all wrong, some useful, as Box stated); somewhat sterile exemplars of how elements within and surrounding a system can interact and lead to a loss event. A model aids in understanding the behavior of a real-life system, but it should never be viewed as deterministically predictive. How, then, are these models exercised in actual use, and what are the advantages and disadvantages of some widely employed hazard analysis techniques? How are models used to identify and address hazards before they have the opportunity to result in accidents?

2.4.1 Fault Tree Analysis

Developed in 1961 at Bell Telephone Labs to evaluate the Minuteman Intercontinental Ballistic Missile Launch Control System, Fault Tree Analysis (FTA) uses Boolean logic to drive a deductive process to determine potential causes of failures. The method counted Boeing Corporation as an early adopter and, given the company's high profile in the aerospace business, the use of FTA spread throughout the industry.

It is important to note that FTA does not necessarily *identify* hazards; rather it analyzes their causes. Thus, it is a backward-looking evaluation, and the hazards themselves must be identified prior to conducting an FTA for the analysis to have a positive impact on system safety. In the first step, an undesired event is defined and decomposed to its *immediate causes*. This decomposition continues until *basic causes* are identified. This resolution from a hazard down to its basic causes is displayed on a logical diagram known as a fault tree. Each level of the tree lists the events that are necessary and sufficient to cause the problem shown at the next level immediately above. The pre-identified hazard is perched on the tree's apex.

Systems that contain a number of true Boolean choices, such as "power available" vs. "power not available" or "catalyst present" vs. "catalyst not present" lend themselves well to hazard analysis via FTA. These outcomes are described through the use of logic gates (i.e., "and" and "or" decisions). An example FTA framework is shown in Figure 2.8.

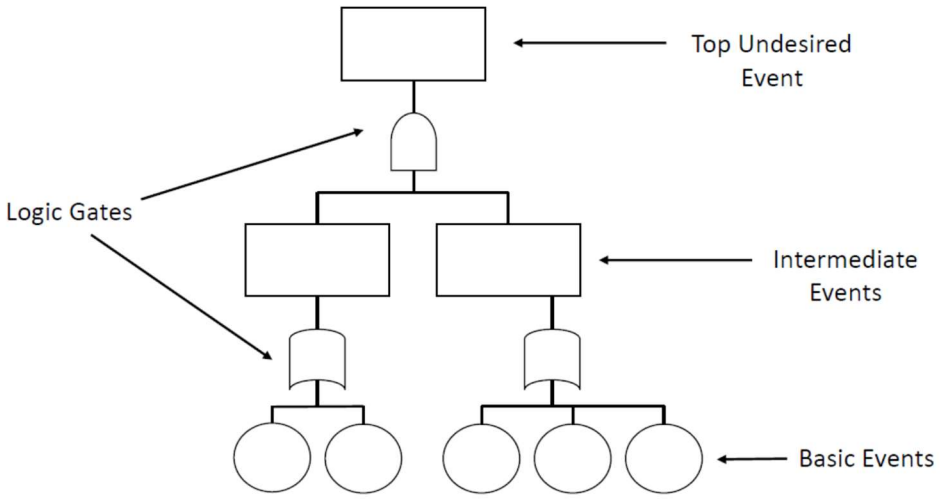


Figure 2.8 – Representative Fault Tree Analysis Framework [14]

Transient states (e.g., "valve cracked open" vice "valve fully open") and time delays in initiation of system processes introduce complexities that FTA may not handle particularly well. In many cases, the probability of an immediate or basic cause may be inferred from statistical data or prior experience. This allows a quantitative analysis to be conducted. Again, if the proper variables are not all included due to oversimplification, the results of such a quantitative analysis may be skewed.

While FTA is a very useful analysis tool that is applied widely throughout a number of industries, it is, at its core, a reliability study tool. Reliability may be defined as "the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions [6]." While reliability is an important factor in determining the safety of an engineering system, high reliability should not be confused with or used as a direct proxy for safety. Safety may be defined as "freedom from accidents or losses [6]." Given these definitions as a starting point, their close relationship is apparent. However, these two system properties can actually exist in direct conflict with one another. To illustrate this difference, Leveson uses the example of a pressure vessel. Designing a high ratio of bursting pressure to working pressure will make a pressurized tank more reliable – that is, improve its probability of not bursting while carrying out its intended function. However, should conditions arise that actually allow the pressure to rise to a level high enough that causes the tank to burst, the higher pressures involved may result in more catastrophic damage to surrounding equipment and personnel due to the greater release of energy. Similarly, lower reliability may sometimes be chosen during design stages to facilitate a fail-safe state in the event of component failure, thus introducing a trade-off between system reliability and safety [6].

The rapid proliferation of computerized, software-based controls and interfaces in engineering systems continues to increase complexity to a level well beyond that which can be effectively analyzed by FTA methods. (Even if the investment were made to conduct a comprehensive FTA for a highly software-intensive system, who will have the time and ability to read it in its entirety and then make actionable sense of its output?) Finally, human factors are difficult to model in a fault tree framework.

2.4.2 Event Tree Analysis

The previous section discussed some of the difficulties encountered when applying FTA to complex systems. Event Tree Analysis (ETA) deconstructs the problem into smaller parts and then applies FTA to each of these parts. As opposed to the backward-looking process employed by FTA, ETA is an inductive, forward-looking procedure that begins with an initiating event and explores possible outcomes stemming from this event. Throughout this process, the analyst takes into account whether installed safety barriers are properly functioning. Protective systems are illustrated from left to right across the top of the diagram in the order they would be encountered. For this analysis technique to be useful, relevant accidental events need to have been identified by a preliminary hazard analysis (perhaps informed by industry experience). Beginning with the results of the preliminary hazard analysis, ETA can be used to identify potential accident scenarios involving the complex system under consideration. Upon developing these scenarios, weaknesses in procedures, control structures, and system design can be more readily identified.

The event tree is drawn to depict a progression from left to right, starting with the initiating event (with its frequency (i.e., occurrences per year) written under the line that the event is written on). Progressing to the right (beneath the left to right progression of protective systems at the top of the diagram), two alternative events are given: 1) success of the protective system, and 2) failure of the protective system. The probabilities of success or failure are also estimated and recorded below each named alternative event. This sequence continues through all of the protective systems listed, resulting in a horizontal "tree," with each path corresponding to a sequence of events leading to an accident. The probability of a particular path occurring is computed by multiplying the probabilities of each event that would occur along the path. An example of an event tree is shown in Figure 2.9.

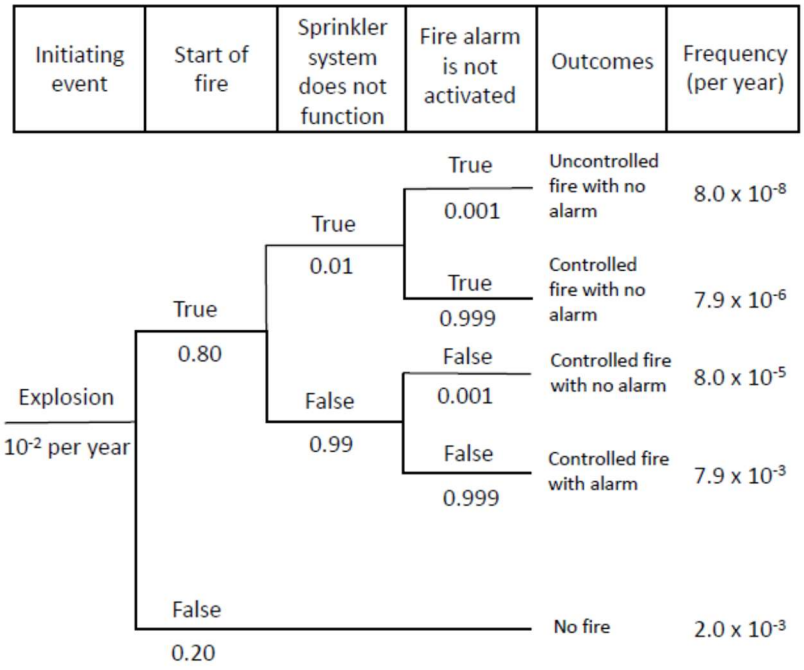


Figure 2.9 – Example Event Tree Analysis [15]

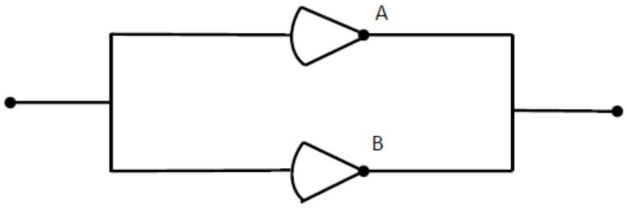
The forward-looking nature of ETA is a valuable property that enables its use in predicting the probability of loss event outcomes (i.e., accidents) that stem from initiating events (or "minor" accidents). This technique is often used in applications such as nuclear power plants, where single initiating events, if not sufficiently addressed by successive safety protection systems, could cause catastrophic damage. The graphic representation used for ETA facilitates a logical visualization of the progression from initiating event to major accident, and it is thus a good basis for evaluating the need for new or improved safety procedures or functions. However, only one initiating event can be studied in each event tree. This fact leads to a potentially voluminous final product, particularly if multiple states (i.e., other than binary) exist for each branch, as in the case of a partial failure of a protective system. It is also easy to overlook subtle system dependencies while conducting the analysis; as a result, ETA is not well suited for handling common-cause failures [15]. ETA is not appropriately sensitive to timing issues and thus may not yield accurate results in instances where failure logic depends on when specific events take place [6]. Finally, ETA and the use of probabilities do not apply to systems that contain software in them; this includes most systems built today, even nuclear power plants (for which ETA was invented).

2.4.3 Failure Modes and Effects Analysis

The method of Failure Modes and Effects Analysis (FMEA) is, like FTA, fundamentally a reliability analysis. However, it is occasionally used as a substitute for a complete system safety analysis in some organizations. The underlying assumption is that reliability of the component(s) in question roughly equates to system safety – a misunderstanding already explained earlier in this chapter. Because it has been applied to system safety evaluations, a brief discussion of FMEA is warranted here.

The first step in FMEA is identification of all system components. As was mentioned in the description of FTA, the level of abstraction at this point in the process will inform all downstream results. Too high a level of abstraction will lead to oversimplification and increase the possibility of overlooking potential subassembly failures that may be economically preventable. Too low a level of abstraction can result in an analysis that is too time and resource consuming to be valuable to the sponsoring organization. Statistical properties (mean, median, mode, and distribution) related to hardware component failure time are often known with reasonable accuracy and precision as a result of manufacturer testing and, in some cases, data gleaned from extensive field use.

Similar to ETA, FMEA is forward-looking and takes a probabilistic approach. Once values are established for component reliability, the effects of component failure on the system are explored. The results are recorded in a table with column headings of component name, failure probability, failure mode, percent failures by mode, and effects (which may be categorized as critical, non-critical, etc.). The probabilities listed under the "critical" effects category (those component failures that are assumed to cause a major malfunction of the larger inclusive system) are then added to compute the failure probability for the entire system [6]. An example of a simple FMEA is shown in Figure 2.10.



Critical	Failure Probability	Failure Mode	% failures by mode	Effects	
				Critical	Noncritical
A	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	
B	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	

Figure 2.10 – Simple Example of Application of Failure Modes and Effects Analysis [6]

FMEA is a relatively straightforward and effective tool to use in determining system reliability. It allows designers to envision paths to critical system level failures far upstream of such a problem occurring. If completed early enough in the systems engineering process, significant downstream time and resources can be saved by promptly addressing a potential problem that could affect overall system reliability. In many cases (assuming a well-engineered system), safety and reliability are complementary properties. Given this, FMEA may supplement pure hazard analysis techniques. However, high component reliability can actually run counter to the goals of system safety, as in the pressure vessel example presented earlier in this chapter. Thus, the FMEA tool must be wielded judiciously when being used to inform decisions with system safety implications. Additionally, the analysis does not typically involve exploration of any potential loss caused by failure of multiple components. Finally, human error and system environment are not typically significantly taken into account when conducting an FMEA [6].

2.4.4 Management Oversight and Risk Tree Analysis

Management Oversight and Risk Tree (MORT) analysis was developed in the 1970s for the U.S. Nuclear Regulatory Agency by William Johnson. MORT is predicated on the belief that all accidental losses are caused by undesired and uncontrolled transfers of energy due to mishandled system changes. Because unwanted energy transfers can be harmful and wasteful, Johnson suggests a number of strategies, barriers, and managerial systems for systematic energy control. Johnson states that accidents result from lengthy sequences of planning and operational error that do not sufficiently adapt to human or environmental changes. He asserts that any organization has two natural tendencies that need to be countered: (1) critical messages tend to flow downward, and (2) commendatory messages tend to flow upward. His MORT approach is intended to reverse these propensities. Through its focus on controlling energy transfers, MORT analysis places emphasis on management responsibility, thus leading to more productive analysis of human factors compared what Johnson calls the “jackass fallacy” of simply blaming someone below management [16].

MORT analysis may be presented as either an accident model or a hazard analysis technique. It is useful when analyzing a specific accident or evaluating a safety program. In contributing to safety program management, MORT is not only intended to prevent safety-related oversights and manage risk, but also assists in optimizing allocation of resources toward safety programs and specific controls [16].

A MORT is a logic tree which contains high-level ideals for a safety program and provides a format for program evaluation. It connects risk factors with logic gates ("and" or "or" gates) and essentially operates as an extensive checklist to review in determining the accident risk. In fact, the MORT describes over 1,500 factors, which are related to 98 generic problems (Figure 2.11) [16].

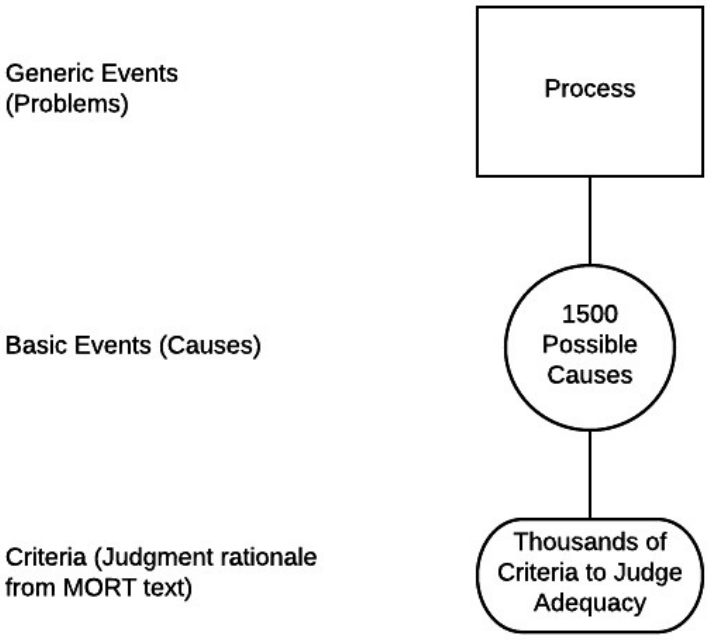


Figure 2.11 – MORT Structure [16]

MORT analysis focus on three primary areas: (1) specific oversights and omissions, (2) assumed risks, and (3) general management system weaknesses. In a MORT analysis, losses stem from: (1) specific job oversights and omissions, and (2) the management judgment system in control of the job. MORT analysis has significant similarity to FTA, but additionally includes an analysis of management, human behavior, and environmental factors. Figure 2.12 shows an excerpt from a MORT.

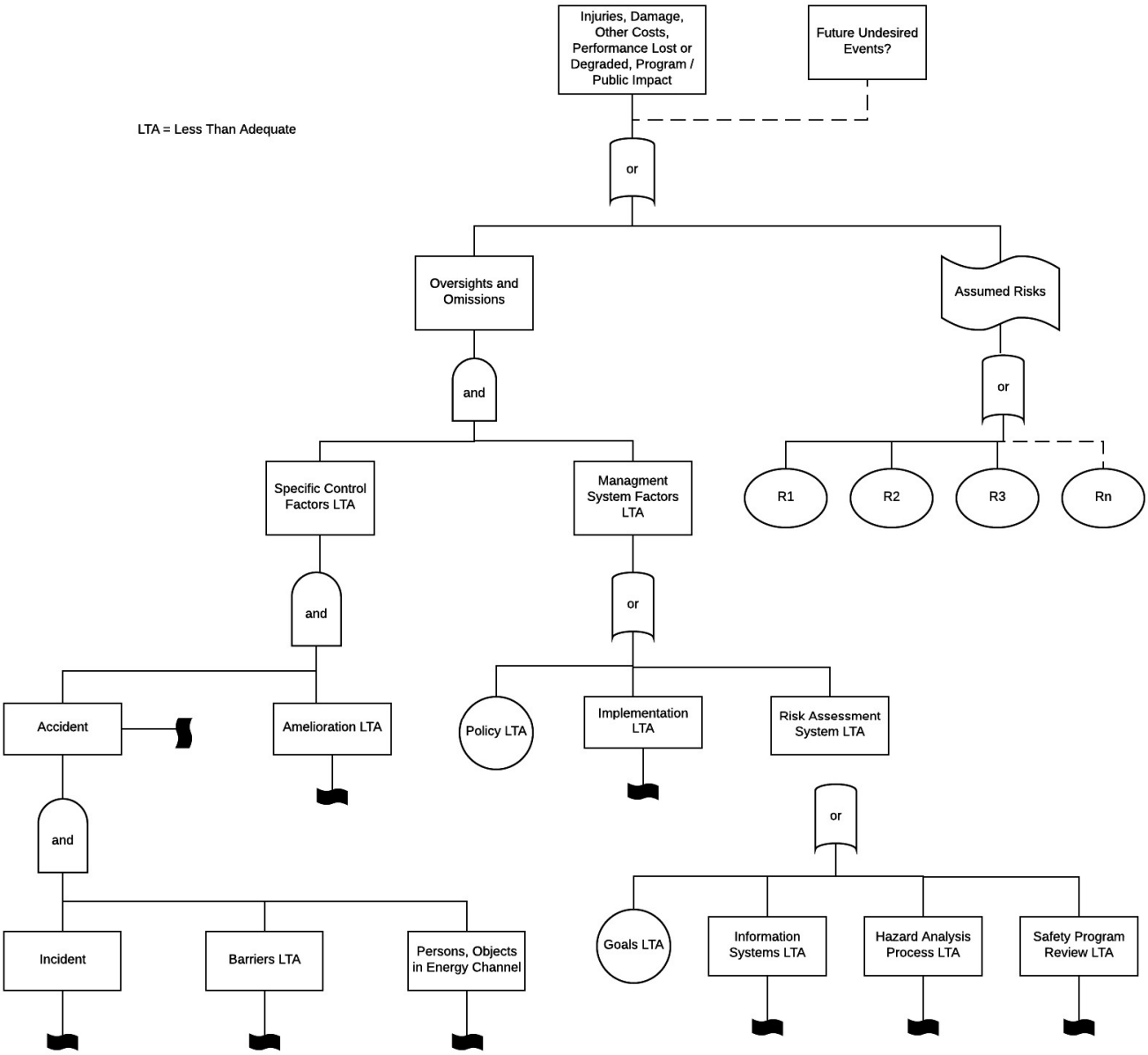


Figure 2.12 – Management Oversight and Risk Tree (excerpt) [16]

One distinction of MORT is the emphasis it places on the role of change in accidents, particularly a non-routine operating mode (e.g., the Chernobyl nuclear disaster) or routine operations in an unfamiliar environment. MORT does not presume that a root cause exists for an accident; in fact, strengths of the technique are its ability to break down an accident sequence into discrete events and its consideration of additional factors such as training, maintenance, planning, supervision, organization, environment, and policy. The goal of MORT analysis is to detect system problems (defects and/or oversights) that either create hazards or prevent early identification of hazards. Unfortunately, MORT takes the form of

a very large checklist (perhaps impractically so, for most applications) with rather vague statements included in it [6].

2.5 The Need for a New Approach

A common thread that runs through many of the "classical" approaches to safety analysis discussed in the preceding sections is the tendency to oversimplify. The models discussed up to this point all assume that accidents are caused by human or component failures. However, accidents can occur when nothing fails, but when interactions among components – operating as designed – lead to a hazardous system state. As was described in this chapter, there are often a large number of conditions that are necessary to make an accident a possibility; however, most time-tested approaches tend to focus on isolating a single root cause, despite the fact that other factors necessarily existed for the accident to occur.

A personal example of such a scenario is a collision between a bus and bicycle at the intersection of Cambridge's Ames Street and Memorial Drive (a busy road bordering the MIT campus), as was experienced by this author. There were many factors involved: the bus stopping in an intersection's crosswalk rather than behind it, the lack of a dedicated bike lane along Memorial Drive, a bus driver who likely felt pressured to maintain/regain his schedule, lack of a traffic signal at the intersection of Ames St. and Memorial Drive (thus leading to the bus driver to "edge out" into the intersection prior to accelerating into a right turn and merging onto Memorial Drive), the bus driver's focused attention on oncoming traffic to his *left* (prior to making a *right* turn) vice also paying attention to pedestrian and bicycle traffic approaching on the sidewalk to his *right*, and the bicyclist hurrying down the sidewalk between consecutive classes that met on opposite sides of the MIT campus. Not one of these conditions was likely sufficient to lead to an incident by itself. However, the incident did occur – the bicyclist approached from the bus's right and bowed his route around the front of the bus that was in the crosswalk; the bus driver accelerated into his right turn onto Memorial Drive while still looking to his left. The element of chance (Reason might refer to it as a hole in the Swiss cheese slice of "unsafe acts") was the most proximate factor that allowed the accident to occur; the driver accelerated from a stop at the same instant the bicyclist was directly in front of the bus.

Depending on one's perspective, it is tempting to single out a single factor as *the* cause of the accident. The bus driver might say that the bicyclist did not stop at the intersection and wait for the bus to pass. The bicyclist might (and does!) say that the bus driver should have stopped behind the crosswalk and yielded the right-of-way to pedestrian and bicycle traffic associated with a bustling college campus. Had a formal investigation been conducted (there was no investigation, since (fortunately) no loss occurred), it is likely that many of the aforementioned factors would have been touched upon. However, it is even more likely that there would have been an ascription of primary blame for the incident. The finding of a primary cause in this case could vary the incident postscript significantly. If the bus driver were found at fault, he could be placed on probation. If the bicyclist were found to be primarily at fault, he could be ticketed by law enforcement (adding insult to injury, had it occurred). If the root cause were determined to be the lack of a traffic signal at the intersection (or the lack of a bus lane on Memorial Drive, the lack of a bicycle lane on Memorial Drive, or a poorly designed bus route), it is possible that physical improvements to the environment (e.g., a traffic signal) may have been recommended. As described earlier in this chapter, many liability analyses are left to one's opinion regarding only what was the most proximate cause. (For the record – in my somewhat biased opinion, "the tie goes to the runner" – or in this case, to the bicyclist.)

The bicyclist in this example escaped injury (though, as he later discovered, his laptop computer did not), and he lived to author a thesis related to system safety. He chose not to pursue any further action related to the incident (he was late to class already), so we will never know what the "root cause" of the accident was, at least in the opinion of an investigating officer conducting such an analysis. The point of this anecdote, of course, is that there was no "root cause." An incident or accident must be examined within the context of a system functioning in its present environment. What is needed to properly analyze a scenario such as the one just described is a holistic systems safety approach. Techniques to conduct such an analysis are detailed in the next chapter.

Chapter 3 – Systems-Theoretic Processes and Analysis

"A systems approach begins when first you see the world through the eyes of another."

- C. West Churchman, American philosopher and systems scientist

"That means that our whole solar system could be, like, one tiny atom in the fingernail of some other giant being…. This is too much! That means one tiny atom in my fingernail could be…"

"Could be one little tiny universe."

- Larry Kroger (Tom Hulce) and Professor Dave Jennings (Donald Sutherland) in *Animal House*

3.1 Chapter Overview

Continuing the discussion that was begun in Chapter 2 regarding the importance of a complete systems-based safety approach, this chapter describes essential characteristics of systems, with a particular focus on complex systems. Systems are categorized into regions of organized simplicity, unorganized complexity, and organized complexity – each of which is best handled using different modeling and analysis methods. Systems-Theoretic Accident Model and Processes (STAMP) is introduced as an accident causality model for systems exhibiting organized complexity. Two particular analysis methods based on STAMP are described in detail: CAST (a backward-looking accident analysis approach) and STPA (a forward-looking hazard analysis technique). This discussion provides the necessary foundation for the analyses that occur in later chapters.

3.2 What is System Safety?

Chapter 2 described several accident models and hazard analysis techniques, most of which were developed more than a half century ago. Like all models and processes, they each have their particular strengths and shortcomings. Chapter 2 concluded with a nod to systems approaches, particularly for complex systems that involve interactions between various subsystems, components, human operators, and the environment. Many of today's computer controlled systems are necessarily included in this category of complex system. The WLB ISCS certainly qualifies as such a system.

Approaches to both backward and forward looking safety management have largely converged on the concept of system safety. At its essence, systems thinking is a manner of analysis that describes all activities involving a process, an operand, and an instrument object and/or a human agent are systems. The term "system" may be defined as follows:

> A system is a construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents; that is, all things required to produce systems-level results. The results include system level qualities, properties, characteristics, functions, behavior and performance. The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is, how they are interconnected [17].

Complicated systems are classified as such based on the number of system components and the combinations and permutations that may arise when analyzing them. A complicated system is difficult for the human brain to holistically consider. Such systems exhibit combinatorial complexity.

Complex systems have several interrelated entities and relationships. The nature of these many interactions, which may change over time, are the essence of complex systems. Such systems may exhibit behavior that is nonlinear, governed by feedback, adaptive, and tightly coupled. Their performance may be counterintuitive, history-dependent, and policy resistant. Complex systems exhibit the property of dynamic complexity [18]. Most modern automated control systems fit into this category.

An "open system" is one that has inputs and outputs from its environment. This communication is an essential property of an open system, such as the WLB ISCS. Feedback loops that communicate information (from sensors) and control commands are at the heart of the system. For any controlled process, four conditions are required:

(1) Goal Condition: The controller must have a goal or goals (for example, to maintain the setpoint).
(2) Action Condition: The controller must be able to affect the state of the system. In engineering, control actions are implemented by actuators.
(3) Model Condition: The controller must be (or contain) a model of the system.
(4) Observability Condition: The controller must be able to ascertain the state of the system. In engineering terminology, observation of the state of the system is provided by sensors [19].

A generic control loop for a system is shown in Figure 3.1, while Figure 3.2 explicitly depicts a controlling computer in the loop. The generic high-level schematic presented in Figure 3.2 is typical of many control systems in operation today.

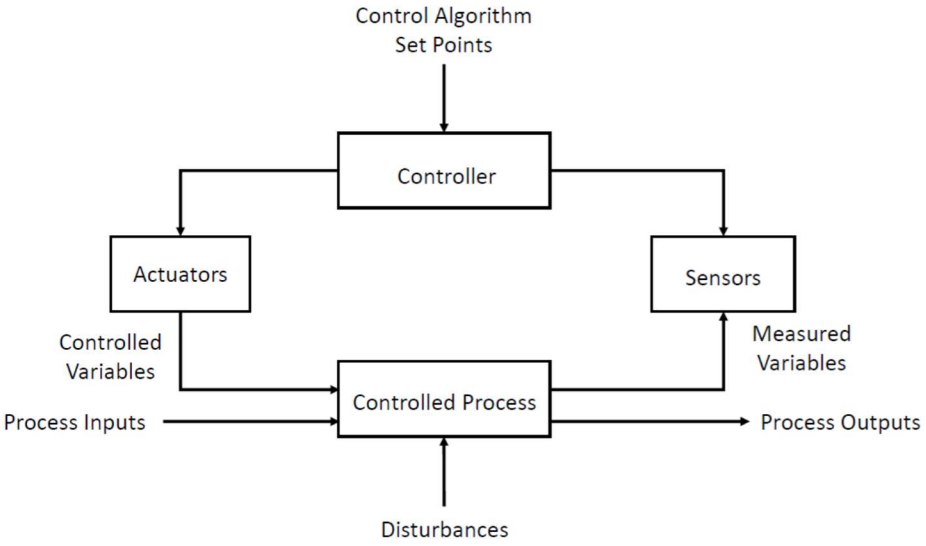


Figure 3.1 – Generic Open System Control Loop [20]

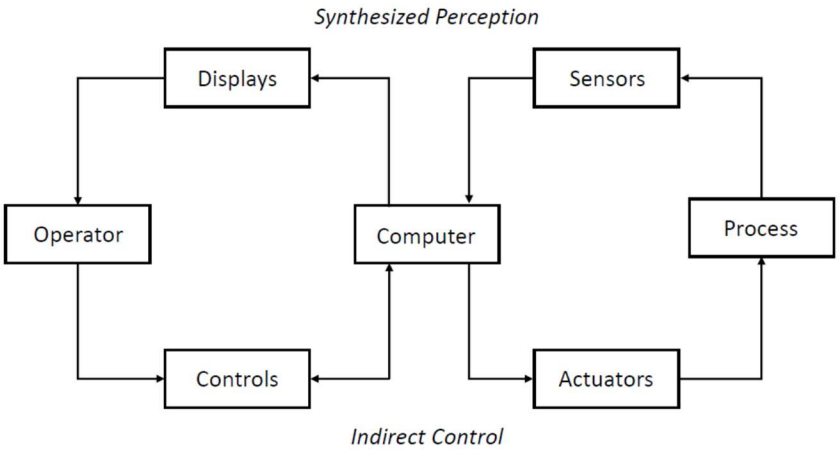


Figure 3.2 – Two Control Loops Linked Together [20]

While Figures 3.1 and 3.2 present the basic elements of system control loops, one should not imply from their contents that all potential system safety influences are depicted therein. System safety looks beyond the control loops and even beyond primary influences such as operational environment and use context; rather, it takes a much broader look at risk management. Pertaining to this topic, Lederer states:

> System safety covers the total spectrum of risk management. It goes *beyond the hardware* and associated procedures of system safety *engineering*. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored [21].

Weinberg used the terms "unorganized complexity," "organized complexity," and "organized simplicity" to aid in explaining system analysis. On an abstract level, Weinberg describes how the Law of Large Numbers enables the observer to make predictions based on statistical analysis when dealing with a system that exhibits both complexity and "sufficiently random" behavior to be analyzed statistically (region II of Figure 3.3). While an Ebola outbreak may be an example of such an "unorganized complex" system (e.g., dealing with a population), engineered systems typically do not exhibit such random behavior, nor do they have a sufficient number of components to be analyzed through statistics alone. Small populations that exhibit highly ordered and structured behavior (region I of Figure 3.3) are not ideally suited for statistical treatment, but may be explored through purely analytical means This category often includes individual machines or mechanisms. The remaining area in Figure 3.3, region III, represents the region of "organized complexity" – too complex to be treated analytically, but too organized for statistics. Weinberg portrays it thusly: "this is the region of *systems*." It is in this region where the Law of Medium Numbers holds, which Weinberg describes as follows: "For medium number systems, we can expect that large fluctuation, irregularities, and discrepancy with any theory will occur

more or less regularly [22]." The WLB ISCS – through its many interacting sensors, actuators, and subsystems – exhibits the property of organized complexity, and is thus best suited to be analyzed via systems theory. This is also the case for the majority of today's engineered systems.

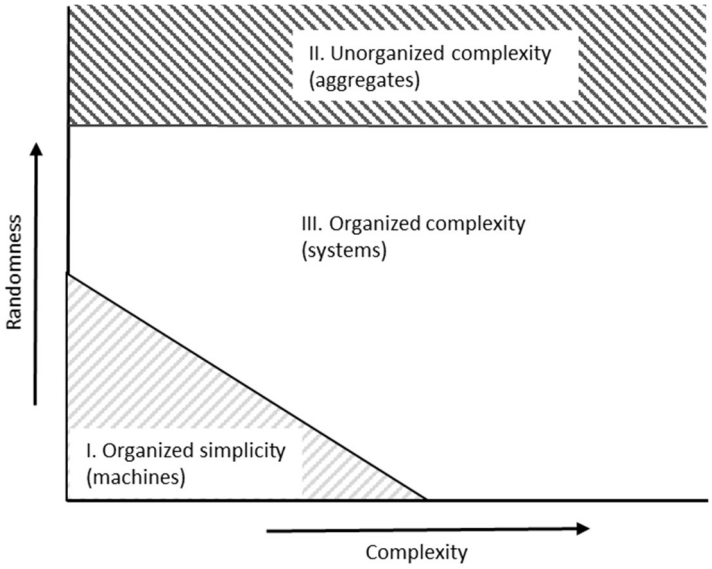


Figure 3.3 – Categorization of Systems by Complexity and Randomness [22]

It may be inferred that system safety techniques must be usable by professionals who represent multiple disciplines and specialties. Furthermore, such methods should be applicable to early system design, facilitating the consideration of safety as a primary "ility" alongside reliability, maintainability, durability, manufacturability, etc. in preliminary design reviews.

3.3 Systems-Theoretic Accident Model and Processes (STAMP)

"A good idea should not be allowed to migrate; it should be propelled."

- Jerome Lederer, former NASA safety director

In her 2011 book "Engineering a Safer World," Dr. Nancy Leveson introduces a new causality model called Systems-Theoretic Accident Model and Processes (STAMP). This model, based on system theory, represents a paradigm shift in accident modeling and hazard analysis. STAMP shifts emphasis from failure prevention to identification and enforcement of constraints on system behavior and component interactions. Of course, accidents arising from component failure are included in the analysis, but attention is paid to component and environmental *interactions*. These go beyond mechanical, electrical, and chemical constraints; management, policy, environmental, societal, and other constraints are also considered.

STAMP leverages its power from system concepts discussed earlier in this chapter: safety constraints, hierarchical control structures, and process models. In this way, it fundamentally differs from the event-based models discussed in Chapter 2. When viewed through the lens of STAMP, events leading to losses occur as a result of ineffective enforcement of safety constraints. In complex systems, these constraints are most often enforced by active controls which detect, measure, interpret, and respond to hazardous conditions. While some controls may be mechanical in nature (e.g., a centrifugal flyweight governor),

most newer active controls used in today's complex systems involve computers to control process outputs. When analyzing an actively controlled complex system, STAMP often attributes accidents to inadequate handling of external disturbances, component failures, or dysfunctional interactions among system components. Very often, this analysis sheds light on incomplete, incorrect, or ambiguous system requirements.

STAMP can be applied in either accident analysis or hazard analysis. Use of STAMP to determine accident causation (backward-looking analysis) requires the analyst to identify ineffective (or missing) control action(s). In a forward-looking analysis, emphasis is placed on identifying and designing controls that will enforce the necessary system safety constraints.

In STAMP, the broader system is viewed as a series of hierarchical control structures that impose constraints from high levels to low levels. Control processes reside between the levels of hierarchy. Thus, constraints govern lower-level behavior by enforcing control processes on the next lower level. To do so, effective communications are needed between levels in the hierarchy – not only a downward directed reference channel, but also an upward directed feedback channel which describes how effectively the constraints are satisfied. Inadequate control can be the result of missing constraints, insufficient control commands, control commands that were not properly executed at a lower level, or inadequate feedback regarding enforcement of constraints.

Finally, STAMP requires understanding and application of process models. As described in Section 3.2, a control process contains a goal condition, an action condition, an observability condition, and a model condition. Any controller – human or machine – requires a model of the process to be controlled in order to be effective. Leveson describes the function of a process model using the example of a simple thermostat:

> Whether the model is embedded in the control logic of an automated controller or in the mental model maintained by a human controller, it must contain the same type of information: the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state. This model is used to determine what control actions are needed, and it is updated through various forms of feedback. If the model of the room temperature shows that the ambient temperature is less than the setpoint, then the thermostat issues a control command to start a heating element. Temperature sensors provide feedback about the (hopefully rising) temperature. This feedback is used to update the thermostat's model of the current room temperature. When the setpoint is reached, the thermostat turns off the heating element. In the same way, human operators also require accurate process or mental models to provide safe control actions [20].

Leveson asserts that accidents often occur when the controller's process model does not match the controlled system, leading to the controller issuing unsafe commands. A generic model showing the process model embedded within the controller is included in Figure 3.4.

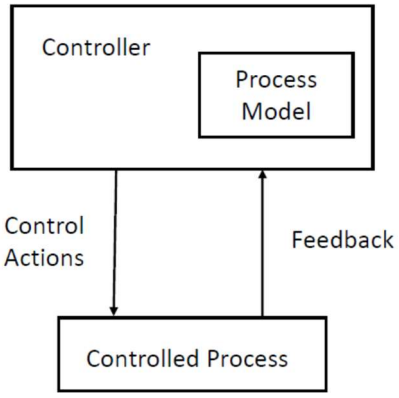


Figure 3.4 – Process Model Governing Controller Behavior [20]

As explained by Leveson, for an accident to happen, one or more of the following must have occurred:

1. The safety constraints were not enforced by the controller.

    a. The control actions necessary to enforce the associated safety constraint at each level of the sociotechnical control structure for the system were not provided.

    b. The necessary control actions were provided but at the wrong time (too early or too late) or stopped too soon or applied too long.

    c. Unsafe control actions were provided that caused a violation of the safety constraints.

2. Appropriate control actions were provided but not followed [20].

There are often multiple paths that lead to one or more of these accident conditions for a complex system. Unsafe control inputs may be entered by the human user. Control algorithms may be inadequately designed. Controller process models may be flawed (as was seen in the loss of the Mars Polar Lander, where the controller interpreted sensor feedback as indicating that the spacecraft had landed on the surface of the Red Planet, thus leading to shutdown of the descent engines and ultimately the crash landing of the spacecraft). Control commands may not be carried out by controlled processes, perhaps due to communication problems. Inadequate coordination between controllers (human and/or machine) could lead to negative system outcomes. Finally, system components may be affected in different ways, and to differing extents, by environmental factors, thus leading to unpredicted (or undesired) system behavior.

A final important factor regarding in-service complex systems, noted by Jacques Leplat, is that of asynchronous evolution [23]. This phenomenon occurs when one part of a system changes without the requisite related changes in other system components or subsystems. In complex systems, it is difficult to predict the system-wide consequences of a change in one component. This phenomenon can prove confounding to system engineers, logisticians, and operators alike when technology refreshes are made during a system's lifecycle to preserve supportability and maintainability against the pressures presented by obsolescence of manufactured components and/or their underlying technologies. Asynchronous evolution may also be the result of deterioration over time of a component or subsystem in its ability to control a process. Any substantial change to a system component or process can "upset

the apple cart" and transform a safely operating system to an accident waiting to happen. As we shall see in Chapter 5, asynchronous evolution likely played a part in the issues associated with the WLB ISCS.

3.3.1 Causal Analysis Based on STAMP (CAST)

Accident reports are typically written from an event-based perspective. Such a format flows naturally – the events leading up to and including the accident are related in chronological order, and often a root cause is ascribed arbitrarily to one of the events in the chain. This is the case when using several of the accident models discussed in Chapter 2. Some analyses, such as those conducted by the NTSB, also account for some systemic factors. Like a zealous prosecutor, however, an accident investigator may be tempted to stop his or her analysis (or continue half-heartedly with significantly reduced rigor) as soon as a blameworthy target is identified as the root cause.

To better ensure completeness in accident analysis, Leveson introduced a new accident analysis technique known as Causal Analysis Based on STAMP (CAST). One of the powerful properties of CAST is that it is a process geared not toward assignment of blame, but rather toward determining *why* an accident occurred. To use an analogy to American football, CAST does not primarily seek to establish who dropped the ball, but rather why the ball was dropped. (Was it slippery? Over-inflated? Under-inflated? Assigned to an exhausted or injured ball carrier? Carried in the wrong hand due to ignorance of technique (inadequate coaching)? Jarred out by a tackler that was unaccounted for in the play's blocking scheme? Carried by the ball carrier in an incorrect direction due to poor communication of the play in the huddle? All of these would be considered in the context of controls and constraints when using CAST.) With CAST, the entire system is examined, including all components, controllers, processes, and the larger control structure in which they reside. Application of CAST shines a bright spotlight onto even the remote corners of accident details where gremlins may still be lurking, ready to rear their ugly heads at the next opportunity to precipitate an accident.

The elegance of the CAST process is in its formulaic approach that yields superior completeness to many other accident analysis techniques. The procedure prescribed by Leveson is detailed below:

1. Identify the system(s) and hazard(s) involved in the accident.
2. Identify the system safety constraints and system requirements associated with that hazard(s).
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsibilities of each component in the structure as well as the controls through which they execute their responsibilities.
4. Determine the proximate events leading to the accident. (This step is similar to event based models, but note that it is not conducted until the fourth step of CAST.)
5. Analyze the loss at the physical system level. (In the case of the WLB ISCS, this consists of the ISCS, its interfacing systems/sensors, and the human controllers.) Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level in the system's hierarchy allowed or contributed to the inadequate control at the hierarchy level currently being analyzed. For each system safety constraint, either the responsibility for enforcing it was never assigned to a component in the safety control structure or a component or components did not exercise adequate control to ensure their safety

constraints were enforced on lower levels of the system hierarchy. Any human decisions or flawed control actions must be understood in terms of: information available to the decision maker (as well as any required information that was not available), behavior-shaping mechanisms (such as those exerted on decision makers), the value structures underlying the decision, and any flaws in the process models of those making the decisions (and what caused the flaws to exist).

7. Examine how overall coordination and communication contributed to the accident.
8. Determine if changes in the system and its hierarchical control structure over time contributed to the migration of the system to a less safe condition.
9. Generate recommendations [20].

The CAST process is particularly effective at "pulling the string" – typically several strings – to determine what inadequate controls were exercised on a system that allowed it to migrate to an unsafe state and, ultimately, result in an accident. Of course, such an approach presumes that an accident has already occurred. The next section explores how STAMP and systems thinking principles may be applied well in advance of any would-be accident.

3.3.2 System-Theoretic Process Analysis (STPA)

Chapter 2 included a discussion of hazard analysis techniques that have been widely used for some years, including Fault Tree Analysis, Event Tree Analysis, Failure Mode and Effects Analysis, and Management Oversight and Risk Tree analysis. While each aforementioned method is effective in its own niche, several of these techniques take a probabilistic view, treating reliability as somewhat of a proxy for safety. While designing reliability into a system may possibly contribute to its overall safety, it is evident that failures from unforeseen failure modes due to either outside influences or a changing system environment may render moot any apparent gains in safety due to increases in reliability. In fact, a system possessing more component or subsystem redundancy (and, ostensibly, more reliability) may actually contribute to operator and management complacency regarding the possibility of system failure. Accidents are not exclusively caused by component failures. Indeed, some accidents are the result of dysfunctional component interactions without a single failure occurring (i.e., the components all function exactly as designed, but their individual functions interact in such a way that a hazardous condition is created).

System-Theoretic Process Analysis (STPA) was developed by Professor Nancy Leveson as a hazard analysis technique to expose and treat potential hazards that may not be addressed by other methods. As a STAMP-based tool, it is a systems-based approach that takes a broader view to include accidents arising from dysfunctional component interaction, complex human decision-making, software flaws, and underlying organizational or social factors that may contribute to an accident [20]. STPA looks not only at electromechanical system components and human operators; it is intended to lead the analyst to build potential hazard scenarios that include all system influences. As a result, requirements may be stated and implemented to design controls that will prevent these hazards from occurring. Crafting scenarios based on system models enables "what if" scenarios to be evaluated before a system is built, thus enabling architects and system engineers to incorporate more robust safety features into its design.

Leveson describes the two main steps of STPA as follows:

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:

a. A control action required for safety is not provided or not followed.

b. An unsafe control action is provided.

c. A potentially safe control action is provided too early or too late; that is, at the wrong time or in the wrong sequence.

d. A control action required for safety is stopped too soon or applied too long.

2. Determine how each potentially hazardous control action identified in step 1 could occur.

a. For each unsafe control action, examine the parts of the control loop to see if they could cause it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.

b. Consider how the designed controls could degrade over time and build in protection, including:

i. Management of change procedures to ensure safety constraints are enforced in planned changes.

ii. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that violate the safety constraints can be detected.

iii. Accident and incident analysis to trace anomalies to the hazards and to the system design [20].

Human controllers can be treated similarly to electromechanical or computer system controllers when conducting STPA. While a cursory review of a highly automated system may lead one to believe that there is less understanding required by human controllers, this is not typically the case. Training and operational procedures must be followed due to the need for the human controller to have an accurate process model. If control algorithms employed by automated controllers are not understood by the human supervising system operation, this lack of understanding can lead to increased likelihood of human error should intervention become necessary [20]. Step 2 of an STPA is designed to determine ways in which the human controller, in addition to the automated controller, may have a flawed process model. If humans tasked with supervising an automated process receive active indication of a system failure or otherwise suspect that a failure has occurred, they may resort to responding with experimentation in the absence of adequate training and procedural guidance. Additionally, process models embedded in automated controllers are typically static in nature. It is most often up to the human controller to manage any environmental cues that are unknown to the automated controller's process model and adjust the controlled process as necessary. Without proper understanding of the

automated controller's process model and associated algorithms, the human supervisor may take insufficient or incorrect action when intervening in an attempt to direct the previously automated process. Figure 3.5 depicts the importance of including human controllers within the bounds of an STPA.

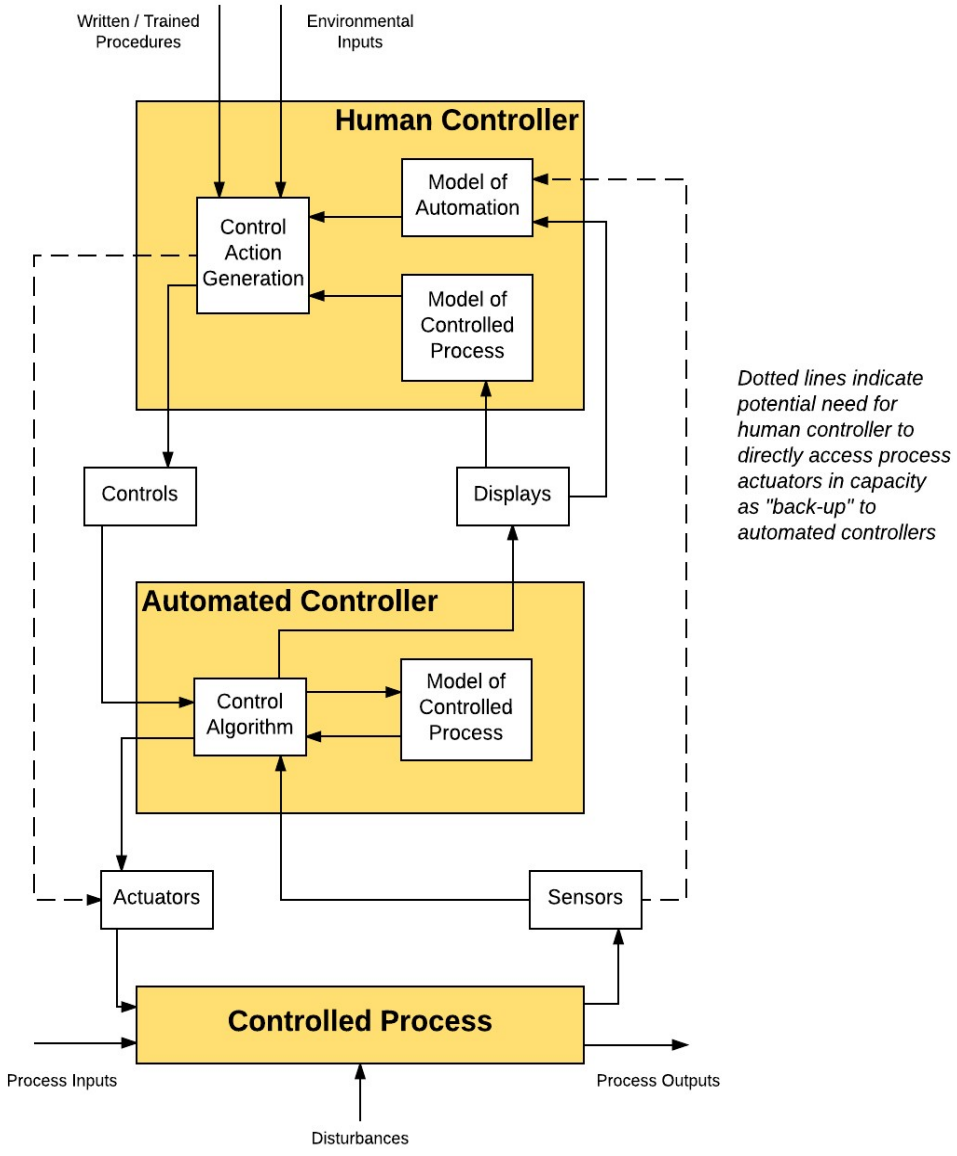


Figure 3.5 – Example of Control Model Where a Human Controller Is Controlling an Automated Controller, Which in Turn Is Controlling a Physical Process [20]

STPA is an accessible methodology. One of its advantages is that it does not require the analyst to be intimately familiar with the system being analyzed, nor must he/she be an expert regarding the technology it employs. STPA is also versatile in its use; it may be applied to a system that has been in existence for many years as easily as a system that is in the early stages of design. While it may be easier and significantly less costly to incorporate the outputs of an STPA into a system that is still being

designed, STPA can also reveal steps that may be taken to protect mature systems from migrating to a hazardous state (or draw them out from a hazardous state that they may have already entered).

3.4 Chapter Summary

This chapter presented some basic tenets of systems theory and described how systems thinking may be applied to the system property of safety. STAMP theory was described in detail, and two processes that draw upon STAMP methods were introduced: CAST and STPA. CAST was described as a backward-looking accident analysis method, and STPA was shown to be a powerful forward-looking hazard identification and elimination tool. Chapters 5 and 7 will apply CAST and STPA, respectively, to the WLB ISCS.

Chapter 4 – WLB ISCS System Overview

4.1 Chapter Overview

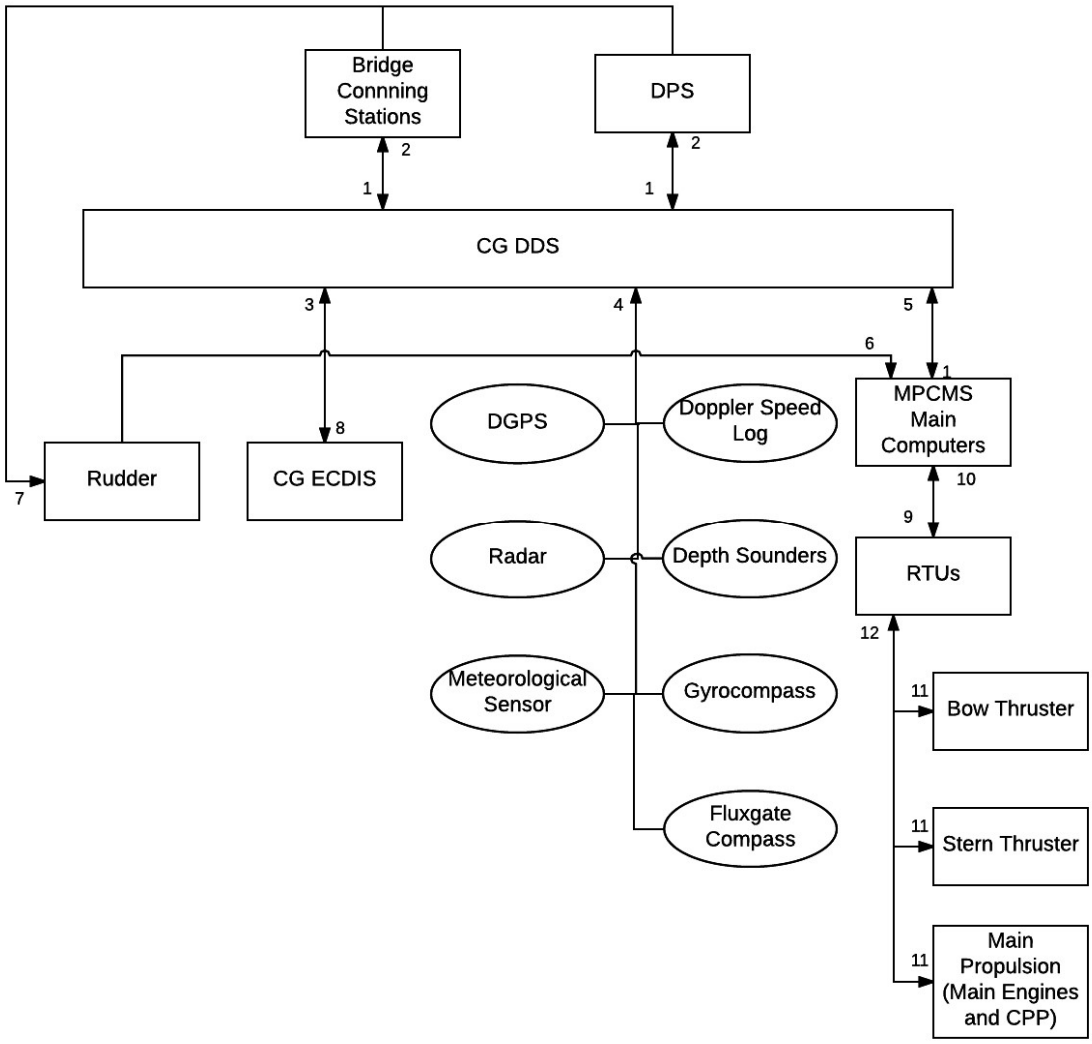
In order to conduct accident and hazard analysis on the WLB ISCS, a brief but adequately thorough description of the system is necessary. This chapter provides a description of the ISCS from a broad system standpoint, as well as the operation of each of its major component subsystems and the interactions between the subsystems. A basic understanding of the properties and functionalities described in this chapter is assumed in the succeeding chapters.

4.2 ISCS Architecture Details

Prior to acquisition of the *Juniper* class WLBs, an Operational Requirements Document (ORD) was approved to document the capabilities required of the new vessels. This document was later modified to reflect lessons learned from operation of the first 225s, as well as some slight changes in operational requirements for these cutters. The current ORD, approved by the Coast Guard's Chief of Staff in June 2000, requires the cutters to service standard buoys (including lifting them from the water, securing them to the deck, and setting them in the water) in winds up to 30 knots, seas up to 8 feet in height, and currents up to 3 knots. It also clearly states that the dynamic positioning system (DPS) shall have the capability to operate in manual position/heading and automatic position/heading modes. Additionally, the ORD specifies:

> Automated systems shall be used wherever possible to minimize manning requirements and maximize unattended operation, with the specific caveat that manual overrides or reasonable delay warning alarms be integrated so that under no circumstances will the propulsion plan be taken off the line "automatically" without the consent of the Conning Officer during buoy handling or other close quarter maneuvering situation. The hazardous nature of buoy work requires this caveat [24].

An abstracted schematic representation of the ISCS and the directions of information flow (commands, status feedback, and alarms) is shown in Figure 4.1. The remaining subsections of this chapter provide a subsystem by subsystem description of the ISCS that was installed onboard the WLB class cutters when they were delivered from the shipbuilder, beginning with *USCGC Juniper* in 1995.



Legend	
Number	Description
1	Propulsion Commands
2	Cutter Status, System Status
3	Chart / Surface Situation Display
4	Sensor Data
5	Feedback from Monitored and Conrolled Systems
6	Feedback from Steering System
7	Rudder Commands
8	DGPS, Compass, Radar Data
9	Commands to Propulsor RTUs
10	Feedback from Propulsors RTUs
11	Commands to Propulsor Acuators
12	Feedback from Propulsor Sensors

Figure 4.1 – Abstracted Schematic Diagram of WLB ISCS

4.2.1 MPCMS

The Machinery Plant Control and Monitoring System (MPCMS) provides remote control, monitoring, and alarm annunciation of ship propulsion machinery, propulsion auxiliaries, and independent auxiliaries.

The MPCMS includes a primary computer and a secondary computer (providing system redundancy) with one computer on line at any given time. An uninterruptable power supply (UPS) located in the Engineering Control Center (ECC) provides regulated power to the computers. In the event of loss of shipboard AC power (provided by one of the ship's service generators or the emergency generator), the MPCMS has an internal battery that can provide approximately 30 minutes of system operation.

The active MPCMS main computer performs the following tasks:

- Controls serial communications with controlled equipment
- Processes external inputs
- Annunciates alarms
- Controls ship propulsion machinery
- Relays data to the passive (stand-by) MPCMS main computer

Because data is continuously provided to the passive main computer, it has an up-to-date database of historical commands issued and feedback received that provides it with a current situational model in the event of active MPCMS main computer failure. The system also contains a separate "watchdog" processor that receives a "health" message from each MPCMS main computer at specified intervals. If a health message is not received from a main computer within the required interval, the watchdog determines that computer to be in a "failed" state, resulting in placing the computer off-line and annunciation of an alarm. Should this happen to the active MPCMS main computer, propulsion control will immediately shift to the passive unit.

A separate data logging computer records log data onto its local hard drive. Logs may be retrieved from the data logger for display or printing.

A user interface is provided at both the Main Ship Control Console (MSCC) on the bridge and at the Engineering Control Center Console (ECCC), which is located in ECC. When control resides with the MSCC, propulsion and thruster control can be further delegated to either the port or starboard secondary conning station. The MPCMS computers (including the data logger) and three video display terminals are located in the ECCC. The system is designed so that the ECCC controls may override the MSCC controls.

As its name implies, the Machinery Plant Control and Monitoring System interfaces with numerous subsystems and equipment throughout the ship. These include:

- Main Diesel Engines
- Propulsion Reduction Gears
- Controllable Pitch Propeller (CPP)
- Ship Service Diesel Generators
- Switchboards
- Steering (receiving system feedback only)
- Maneuvering Thrusters
- Other Shipboard Systems (e.g., fuel tank level indicators, firefighting water pumps, fire/smoke detectors, bilge flooding sensors, etc.)

Interfacing between the MPCMS and shipboard systems is accomplished through 10 remote terminal units (RTUs), which are located throughout the ship. Each RTU consists of a single processor and up to 31 individual analog or digital input/output modules [25].

Operator interface is provided via five video display terminals (VDTs), with user inputs made by keyboard and mouse. VDTs used for underway operations are located in both the ECCC and MSCC [25].

While the MPCMS passively monitors numerous ship systems, this thesis considers its functions in the context of propulsion control. The 225' WLB main propulsion plant consists of a single controllable pitch propeller and two diesel engines, which deliver rotational energy to the propeller via a reduction gear. A power take-off from the reduction gear drives a thruster generator; when operating with MPCMS in maneuvering mode, this provides the necessary AC line voltage to rectifiers that deliver DC voltage to motors that drive a bow thruster and a stern thruster, both of which are oriented athwartships. Under normal operating conditions, the speed of each main engine is controlled by command signals transmitted to the engine governors via the MPCMS. Similarly, propeller pitch is controlled by commands relayed from the MPCMS. Engine load is monitored by the MPCMS, with feedback signals relayed to the associated RTUs by the fuel rack position indicators. If load becomes too great for the engine(s), propeller pitch is reduced via a command from the MPCMS main computer.

Two basic modes of MPCMS operation are examined in this thesis: transit mode and maneuvering mode. Under transit mode, input commands to the engines and CPP produce increased/decreased forward/reverse thrust by initially modifying propeller pitch (ahead or astern) while the clutched in engine(s) remain(s) at idle (350 rpm). Should the input command signal increase to order more thrust, engine rpm and pitch increase in accordance with the programmed engine speed/CPP pitch schedule. When maneuvering mode is selected, engine speed is held constant at 720 rpm to provide a constant 60 Hz to the thruster generator via the reduction gear power take-off. As a result of this constant engine rpm, varying fore/aft thrust input commands results in only propeller pitch response while in maneuvering mode.

In addition to receiving thrust commands from propulsors (thrusters and main engines) and conveying their status feedback to the (human or automated) controller, the MPCMS relays related alarms, issues automatic engine shutdown commands if programmed conditions are encountered, enforces propulsion interlocks and permissives, and engages/disengages clutch controls.

The MPCMS main computers communicate with the RTUs through a network known by its proprietary name, TANOnet. The RTUs, in turn, interact with various ship systems' actuators and sensors. A representation of the MPCMS communication network is shown in Figure 4.2.

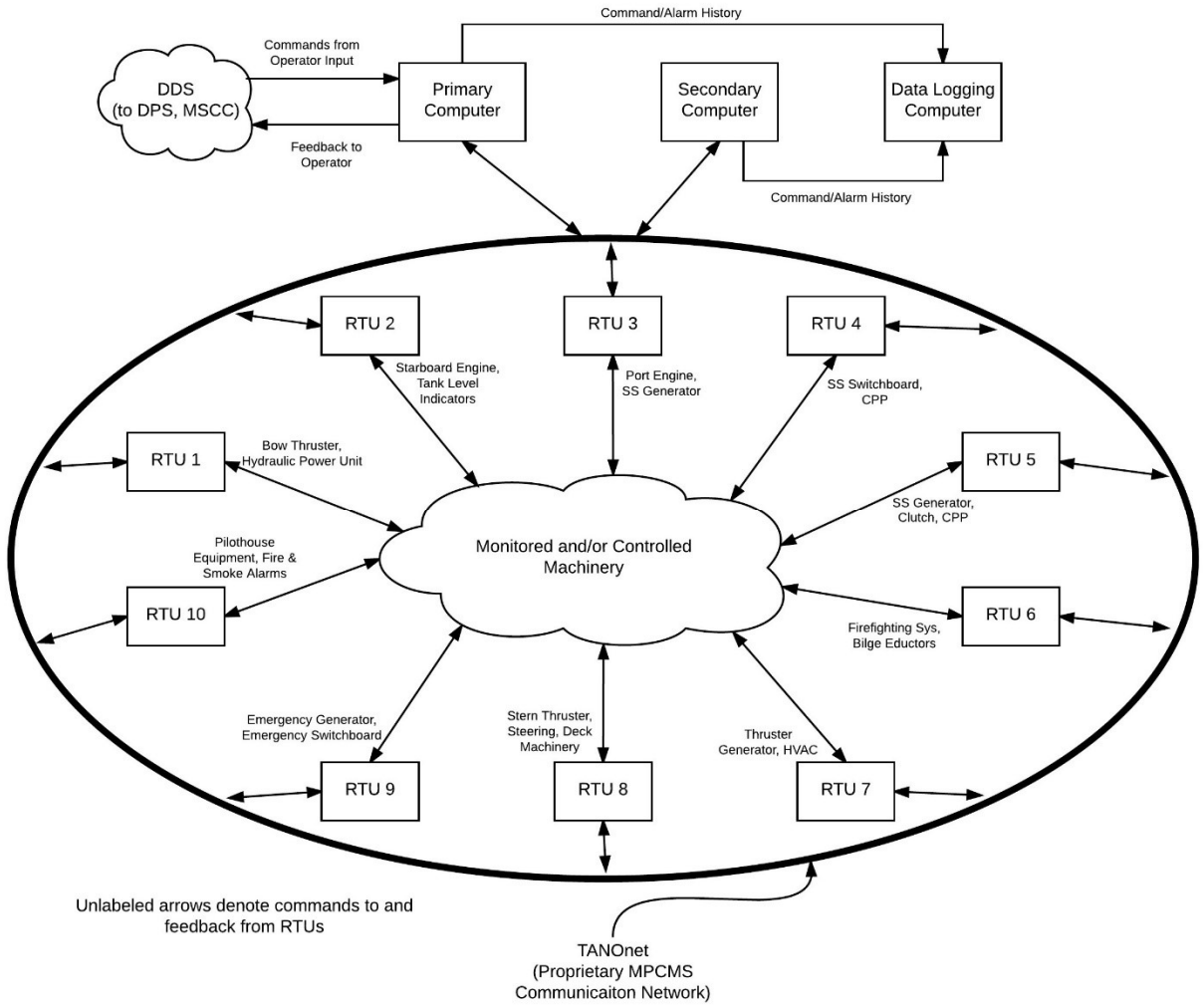


Figure 4.2 – Schematic Representation of MPCMS Communication Network

4.2.2 DPS

The installed dynamic positioning system (DPS) consists of an industrial computer, main control console, two secondary conning station consoles (SCSCs), a power supply/signal processing unit, three joystick assemblies (one at each SCSC and a portable assembly for use on the bridge wings), and a bulkhead mounted vertical reference unit (corrects errors in vessel position measurements induced by pitch and roll). Backup power for the DPS is available through an uninterruptable power supply (UPS) located in the pilothouse. The DPS main control console is mounted in the MSCC in the pilothouse. The DPS control selector switch has three positions: “Joystick/DP,” “Autopilot,” and “Bridge” (see Figure 4.3). The first two positions reflect DPS control modes that are selected by the user according to mission requirements. “Bridge” mode is chosen when direct operator control is desired, and its selection initiates transfer of control from DPS.

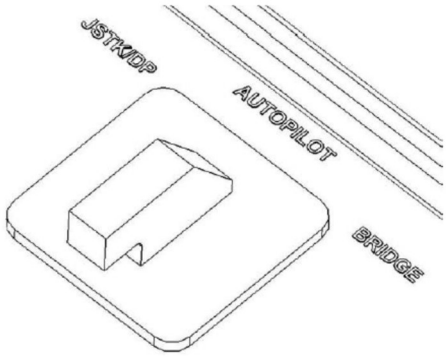


Figure 4.3 – DPS Control Select Switch [26]

The system interfaces with sensors and the MPCMS via a fiber-optic LAN, known as CG DDS. The DPS interfaces with the steering control system (rudder positioning) via a dedicated Ethernet connection.

The DPS receives inputs from various sensors, including the Weatherpak (wind speed and direction), ship speed log, gyrocompass, fluxgate compass, differential global positioning system (DGPS), and the electronic chart display information system (CG ECDIS). DPS can control the ship's movement via Dynamic Positioning (DP) or Autopilot modes. With the MPCMS set to maneuvering mode (with thrusters available and at least one main engine clutched in), DPS can be used in DP mode to hold the ship's current position ("hold position" command) and/or hold the ship's current compass heading ("hold heading" command) using the main engine(s), CPP, and thrusters. When MPCMS is set to transit mode, DPS can be employed in Autopilot mode to control the main engine(s), CPP, and rudder (not thrusters) to follow a pre-determined trackline or consecutive series of tracklines ("high speed track follow" command) that are provided via CG ECDIS. A vertical reference unit (VRU) measures ship pitch and roll angles which are used to correct the errors they induce in position measurements. Additionally, the DPS corrects for the forces of wind and ocean currents to maintain the desired position, heading, or track. While the DPS controls the propulsors and/or steering, the operator is required to monitor system operation by means of system indicators and initiate corrective actions in the event of alarm occurrences. Some manual operation is available in DP mode through joystick controls, allowing the user to position the vessel upon reaching the vicinity of the work site (prior to engaging "hold heading" and/or "hold position") [26].

A basic architectural representation of the DPS and its interfaced systems is shown in Figure 4.4. Representations of the "hold heading" and "hold position" commands are shown in Figures 4.5 and 4.6, respectively.

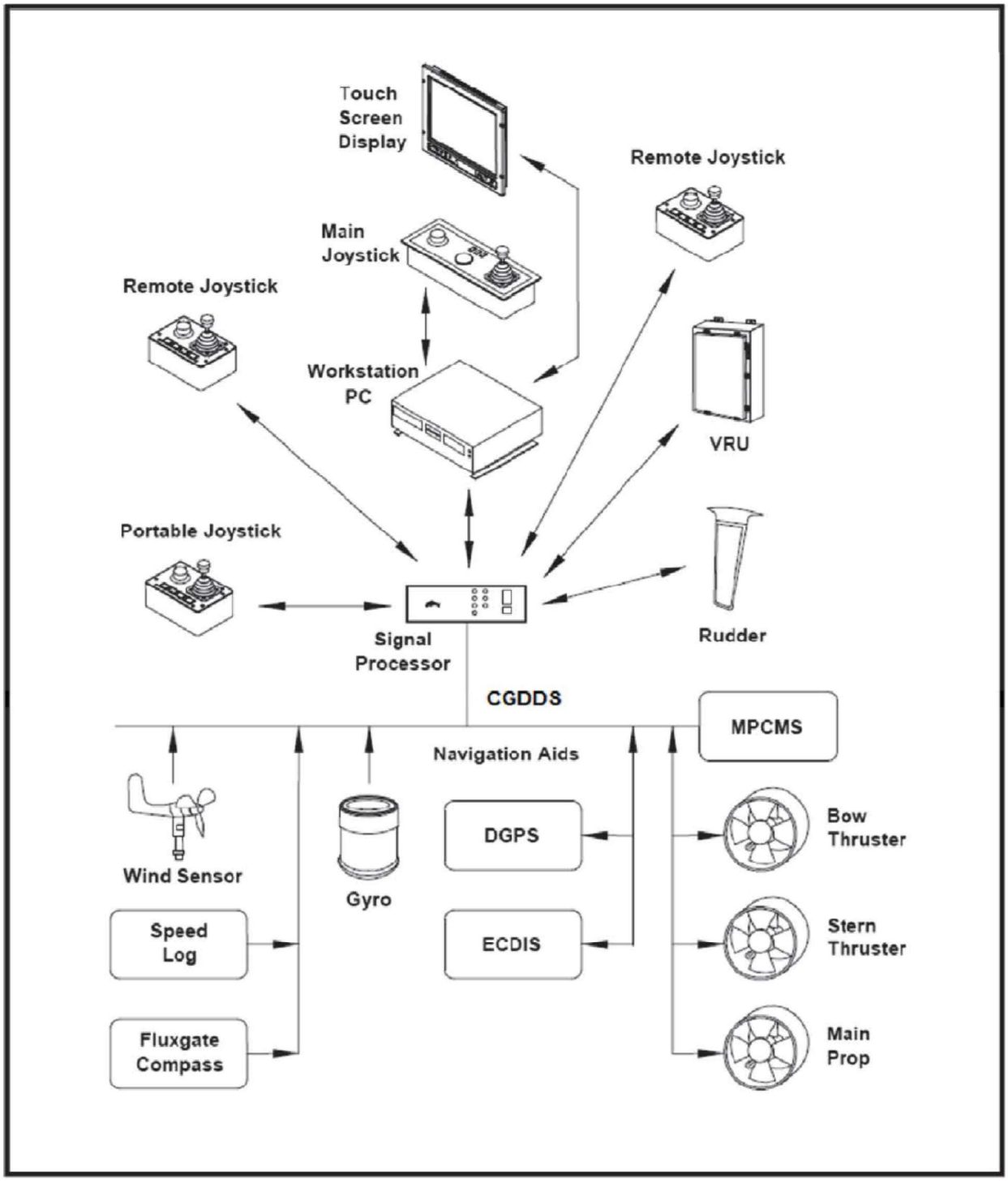


Figure 4.4 – Dynamic Positioning System Overview [27]

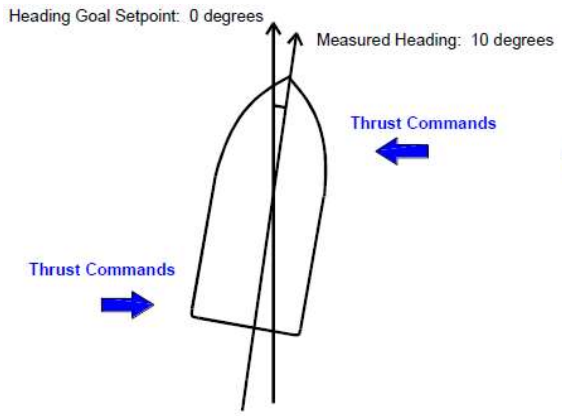


Figure 4.5 Hold Heading Illustration [26]

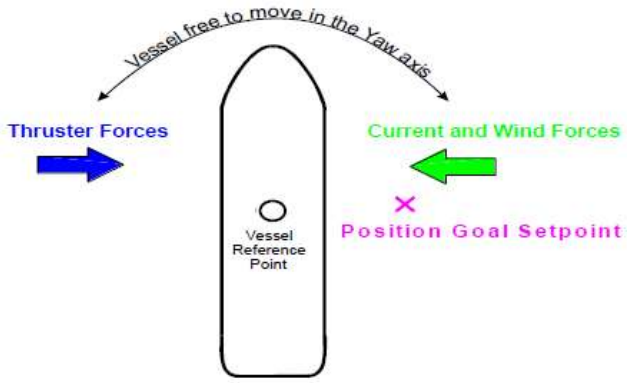


Figure 4.6 Hold Position Illustration [26]

4.2.3 CG ECDIS

The Electronic Chart Display Information System (CG ECDIS) incorporates a marine class industrial computer with display monitors. CG ECDIS is used for shipboard navigation and collision avoidance, and is a combination of an electronic chart, current DGPS coordinates, and surface radar picture on a single display, providing the user with a real-time assessment of current navigational conditions. Necessary inputs come via the Data Distribution System (CG DDS) from the DGPS, gyrocompass, radar, and Doppler speed log. CG ECDIS is also interfaced with the Automatic Identification System (AIS), which provides the cutter's navigational information to other ships and vessel traffic services. Backup power for CG ECDIS is available through a UPS located in the pilothouse. CG ECDIS is used in voyage planning, allowing the navigator to enter waypoints and tracklines from the cutter's current position to a desired future position [27].

4.2.4 CG DDS

The Data Distribution System (CG DDS) provides the communications interface between the MPCMS, ECDIS, and DPS. It also interfaces with related sensors, including the radar, DGPS, compasses, Doppler speed log, weather sensors, and shallow water depth sounder. CG DDS consists of two computers (one online, one standby), three managed Ethernet switches, six serial device servers, a laptop computer (for system configuration and troubleshooting only) and ancillary equipment (Ethernet cabling, gyrocompass synchro digital converter, etc.). Back-up power for CG DDS is available via a UPS. Connected systems (such as MPCMS) transmit and receive serial data to/from a serial device server, which coverts serial data to internet protocol data and vice-versa. During normal operations, data is sent to the primary CG DDS computer via a managed switch, and this computer then routes the data to the appropriate serial device server, while also translating the data to proprietary messaging formats required by CG ECDIS, DPS, and MPCMS. In effect, the CG DDS acts as both "traffic cop" and "highway"; it translates, reformats, and routes messages to/from connected systems after verifying the correct message type and format.

The primary CG DDS computer sends a status message to the secondary computer once per second. If this status message is not received, CG DDS cycles power to the primary computer and places the secondary computer on line, at which time the primary computer assumes the back-up functionality previously performed by the secondary computer.

A maintenance interface is provided to technicians via a semi-rugged laptop computer, which is connected through Ethernet switches in the cutter's chart room and allows monitoring of status of

communications to and from sensors and subsystems. The laptop also stores CG DDS message data and system status information in an SQL database [28].

The CG DDS is a USCG architected system that uses commercial off-the shelf products. It was installed in the WLB fleet beginning in 2010 to replace the Survivable Adoptable Fiber Optic Embedded Network (SAFEnet) LAN, which was installed on each cutter upon initial delivery from the shipbuilder.

Chapter 5 – CAST Analysis of *USCGC Elm* Incident of August 16, 2013

"The owl of Minerva spreads its wings only with the falling of dusk."

- Georg Wilhelm Friedrich Hegel, German philosopher

5.1 Chapter Overview

This chapter is devoted to a Causal Analysis using STAMP (CAST) of a "near-miss" incident onboard *UCGCG Elm* that occurred in 2013. A step-by-by step methodology is used, following the approach introduced in Dr. Nancy Leveson's book *Engineering a Safer World*. While shortcomings in performance of the WLB ISCS as an electromechanical system are readily apparent through use of other accident analysis techniques, deficiencies in the system's hierarchical control structure are uncovered only through exercise of the CAST method. Recommendations pursuant to the CAST are made at the end of the chapter.

5.2 Overall context of *USCSC Elm* Incident

The near-miss event involving *USCGC Elm* described in Chapter 1 was not the only one of its kind.

On July 17, 2013 – only a month prior to *Elm's* incident – *USCGC Alder* was transiting the Sault Sainte Marie locks between Lake Superior and Lake Huron. The cutter was within a lock, operating in maneuvering mode and holding position via DPS, when an MPCMS secondary computer failure alarm was noted (the secondary computer was online as the active computer prior to the alarm). MPCMS control was lost while the bow thruster was executing a command to push the cutter's bow to port (left). With the control loop broken, the MPCMS continued to execute its last command from the DPS – the thrust to port. The Conning Officer (human controller) was unable to regain control of the ship's propulsion in time to arrest the yawing motion created by the bow thruster, and the starboard quarter (right rear) of the cutter contacted the lock wall. Fortunately, no damage occurred to the cutter or the lock. The primary MPCMS computer (which had been the passive computer in the pre-casualty configuration) came on line approximately 20 seconds after the loss of propulsion control. The shift from active to passive (standby) computer should have been nearly instantaneous if the system were operating as designed and intended.

The first level reviewer comments in *Alder's* official mishap report indicated that there was a delay between the loss of MPCMS control and the time when the associated alarm was received. As a result, the Conning Officer unsuccessfully attempted to use the stern thruster to push the cutter's stern to port in an effort to avoid an allision with the lock wall. The mishap report's "command reviewer" comments included the following:

> The MPCMS VME [Versa Module Europa] computers are obsolete and need replacement. Every day we operate with this system our chances of a more serious casualty are increased. We will reload the software package and continue to monitor closely. Thankfully no one was injured and we only suffered cosmetic damage.

Absent any rigorous analysis, how did *Alder's* command draw the conclusion that obsolescence of the MPCMS computers caused the loss of control that led to the allision? What was hoped to be accomplished by reloading the MPCMS software? Was a corrupt version of the software suspected? If

so, why? Was the source of the reloaded software the same as that from which the software had been previously loaded? These and other questions are unanswered in the mishap report.

A second incident involved *USCGC Hollyhock,* another WLB homeported in the Great Lakes. On May 2, 2013, *Hollyhock's* buoy crane and cross-deck winch were both hooked into a winter mark buoy. Control was being exercised through the port DPS joystick, and the DPS was in "hold heading" mode. A "transfer control" alarm sounded, indicating loss of control by the port conning station. Despite attempts to transfer control to Bridge mode, nearly a minute elapsed before the shift in control was executed. Once control was regained in Bridge mode, the Conning Officer noted a lengthy lag (approximately 45 seconds) in response to thruster and engine/pitch commands. Due to the poor control situation, the Officer of the Deck deployed the port anchor and attempted to shift propulsion control to ECC so that the engines could be de-clutched. The Engineer of the Watch (EOW) was unable to acknowledge control of the plant in ECC due to sluggish control system response, and he proceeded to switch to emergency manual mode to gain control of and declutch both main diesel propulsion engines.

Similar to *Elm's* mishap report, *Hollyhock's* narrative stated the cause as "failure" – ostensibly failure of both MPCMS computers. The mishap report's "command reviewer" comments stated:

> This near miss depicts just how dangerous our daily work can be and how our aging systems are prone to mechanical failures. The MPCMS VME computers are obsolete and need to be replaced…

The first sentence in the above passage references mechanical failure – but computer obsolescence is mentioned in the second sentence. Are these separate thoughts, or does the mishap's command reviewer feel that mechanical failure is related to obsolescence? How much did *Hollyhock's* mishap report influence the content of *Elm's*, which was issued roughly a month later?

A loss of propulsion control casualty with a considerably clearer proximate cause occurred onboard *USCGC Maple* on November 19, 2013. The cutter was actively engaged in a buoy servicing evolution in Southeast Alaska when propulsion control was lost. Casualty control procedures were followed, and attempts to regain control in ECC and in emergency manual mode were both unsuccessful. In desperation, the EOW directed a junior watchstander to locally take local control of the main diesel engine and the controllable pitch propeller. Positive propulsion control was regained in local control, the buoy deck team disengaged from the buoy being serviced, and the cutter proceeded to safe water to troubleshoot the casualty. Further investigation by technicians isolated the "cause" of the casualty to be liquid intrusion into the UPS, which resulted in a short circuit that secured power to both MPCMS computers. The culprit liquid was coffee, which spilled from a cup that had been placed on top of the UPS. The corrective action noted in *Maple's* mishap report was as follows: "Unit safety training was conducted in the Engineering Department and a piece of rubber matting was placed over the UPS cover to prevent future casualties." The lack of an adequate constraint (e.g., "watchstanders must not put open beverages on top of MPCMS UPS") can be seen as a causal factor of *Maple's* incident.

Similar propulsion control mishaps were reported by other cutters in the 2013 – 2014 timeframe, including instances of computer "failure" and uncontrolled/unexplained pitch increases (resulting in undesired ship acceleration). It is apparent why operators were losing confidence in the installed propulsion controls that fell under the ISCS suite. These controls provide the framework for safe mission

execution within the WLB concept of operations by allowing a minimal crew to operate the ship with high precision at the margin of a navigable waterway.

It is noteworthy that the mishap reports summarized above not only did not delve deeply into control structure hierarchies (to say nothing of safety constraints and process models), but did not recognize many factors outside proximate causes that led to the casualties. In fact, some of the mishap causes were characterized as "failure" or "design." It is also interesting to observe a common thread emerge in the reports – casualties tended to be attributed to failure of the MPCMS which, as described in Chapter 1, is one component subsystem of the Integrated Ship Control System (controlling the ship's position in conjunction with, most notably, the DPS and CG DDS). Perhaps this illustrates a type of networking effect phenomenon, since it is reasonable to assume that commanding officers of WLBs that experienced propulsion control casualties readily shared their experiences (and their opinions regarding the cause of the symptoms that their ISCS exhibited) with their peers.

The remainder of this chapter will be devoted to analyzing one of these incidents – the *Elm* mishap – using CAST.

5.3 *USCGC Elm* CAST

5.3.1 Step 1 – Define System and Hazards

The system being analyzed is the WLB Integrated Ship Control System. The purpose of the ISCS is to facilitate safe, efficient transit and buoy operations for the WLB. "Hazard" was defined earlier in Chapter 2 as "a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident." The potential accident being considered in this case is grounding of *USCGC Elm*. While an accident (loss event) did not occur as a result of the mishap, the incident involving *Elm's* loss of propulsion control in very close proximity to shoal water clearly had potential to be a rather significant accident.

The primary system hazard encountered by *Elm* in this incident was the *cutter not maintaining safe distance from a shoal*.

5.3.2 Step 2 – Define System Safety Constraints and Requirements

Possible system safety constraints include:

1. The cutter must maintain safe distance from other ships.
2. The cutter must maintain safe distance from stationary objects (e.g., piers, bridges).
3. The cutter must be positively controlled while servicing buoys.
4. The cutter must maintain safe distance from shoals.

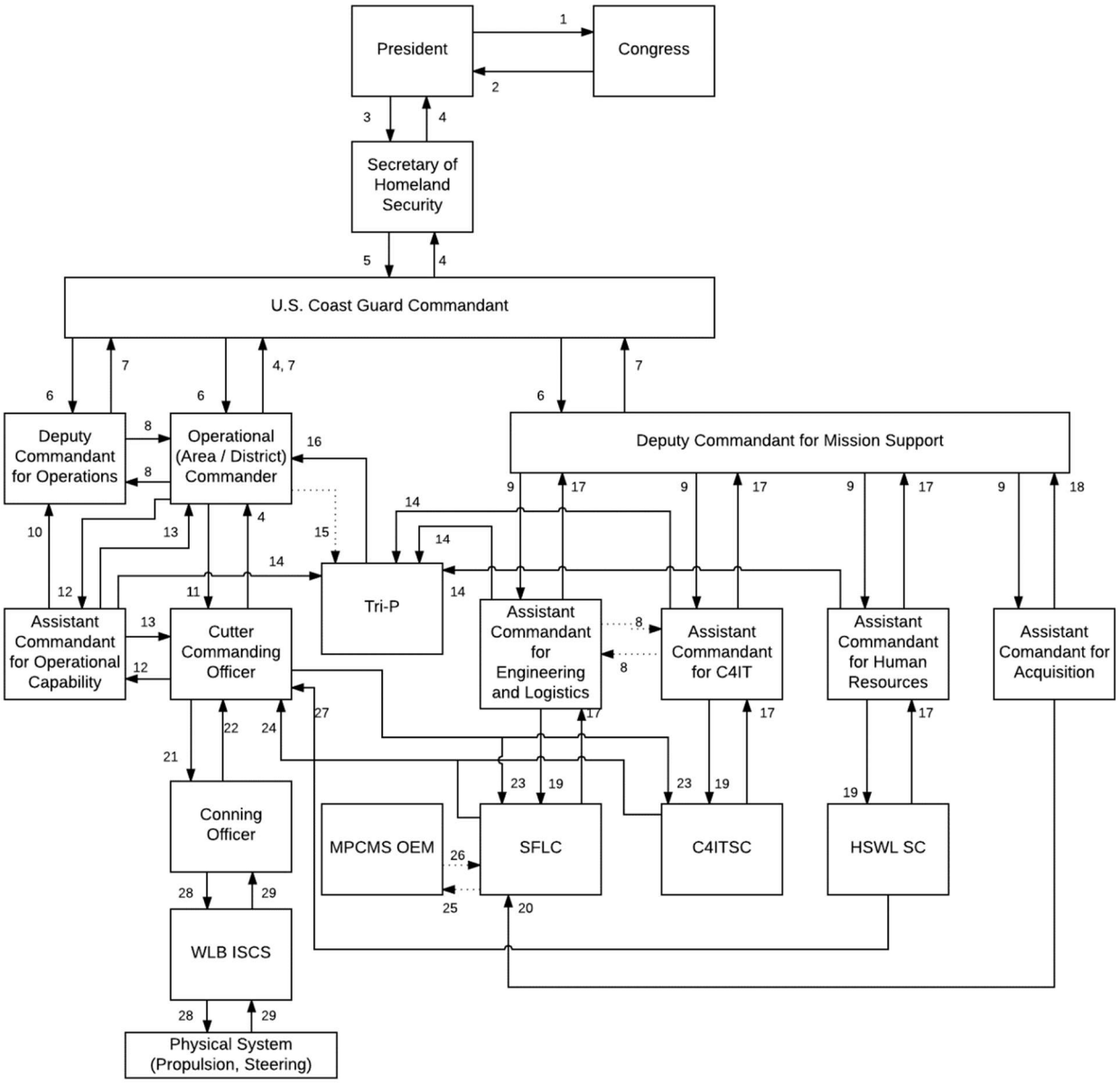
Possible system requirements include:

1. The system must be capable of maintaining the cutter's heading within X degrees of desired heading.
2. The system must be capable of maintaining the cutter's position within Y meters of desired coordinates.
3. The Conning Officer or DPS must not position the cutter at an unsafe distance from ships, stationary objects, or shoals.
4. The Conning Officer must receive clear and immediate indication of the loss of current mode of propulsion and/or steering control, should a loss of control occur.

5. The Conning Officer must receive clear and immediate indication of an unacceptable lag in propulsion and/or steering control, should a lag in control occur.
6. If the current mode of propulsion and/or steering control is lost, it must be fully regained (in the same mode or an alternate mode) within X seconds.

5.3.3 Step 3 – Document Safety Control Structure

The WLB, as an operational asset in the U.S. Coast Guard's surface fleet, provides mission execution. While the primary mission discussed in this thesis is Aids to Navigation, WLBs frequently perform other missions, including marine environmental protection, law enforcement, protection of living marine resources, and ice breaking operations. Mission assignments come from operational commanders who, in turn, receive their tasking via the chain of command in support of the Commandant's strategic direction. Figure 5.1 represents the hierarchical system safety control structure for the WLB ISCS. A clear vertical delivery of mission execution from the WLB all the way up the operational chain of command is depicted in the control structure. The mission support organization provides integrated mission support, which is delivered via specialized logistics and service centers. These logistics and service centers report to their supervisory assistant commandants. The dotted lines in Figure 5.1 represent areas of communication/control that were identified during the CAST as specific areas to consider in directing future improvement efforts.



Legend			
Number	Meaning	Number	Meaning
1	Budgets and Priorities	15	Fleet Concerns
2	Authorizations and Appropriations	16	Prioritization and Resolution of Fleet Concerns and Policy Issues
3	Mission Prioritization, Funding	17	Execution of Mission Support
4	Mission Execution	18	Asset Recapitalization
5	Mission Goals & Requirements, Funding	19	Policy, Funding
6	Strategic Direction, Funding	20	Initial Technical Publications and Sparing
7	Execution of Strategic Direction	21	Leadership and Oversight
8	Alignment of Goals and Information	22	Personnel and Equipment Status, Execution of Orders
9	High Level Policy, Performance Targets, Funding	23	Requests for Maintenance, Technical, and/or Logistics Assistance
10	Appropriate Operational Capabilities	24	Maintenance, Technical, and/or Logistics Assistance
11	Mission Assignment, Command and Control	25	Requests for Technical Assistance
12	Requests for Headquarters Advocacy	26	Technical Assistance
13	Policy, Advocacy	27	Safety Procedures, Inspections, Mishap Review
14	Resource and Policy Issues	28	Control Actions
		29	System Status Feedback

Figure 5.1 – Hierarchical System Safety Control Structure and Legend

A “zoom in” of the functional control structure of the WLB is detailed in Figure 5.2

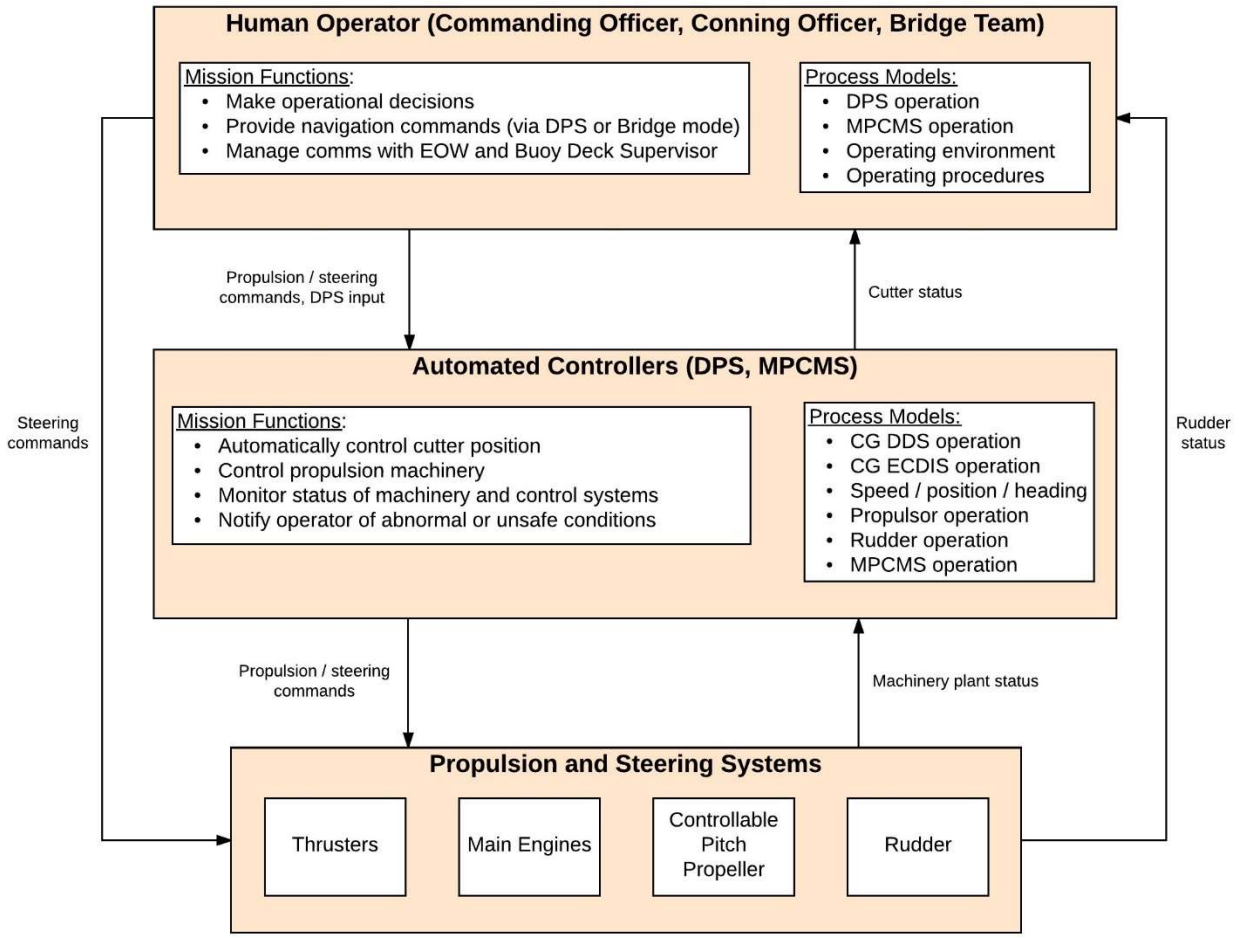


Figure 5.2 – WLB High-Level Functional Control Structure

5.3.4 Step 4 – Determine the Proximate Events Leading to Accident

A truncated account of proximal events already narratively described in Chapter 1 is repeated here, both for the readers’ convenience and to illustrate the full CAST process.

1. A new electronic charting system and radar were installed on *USCGC Elm* at the cutter’s homeport by Coast Guard technicians from the Coast Guard’s Surface Forces Logistics Center (SFLC) and Command, Control, Communications, Computers and Information Technology Service Center (C4IT SC).
2. *USCGC Elm* departed homeport after completing all normal pre-underway checks without incident or noted anomaly.
3. At 10:23 local time, *Elm* entered the Morehead City turning basin.
4. The Conning Officer placed *Elm’s* DPS in “hold position” mode.
5. The Conning Officer tested the DPS console by ordering a twist to port.
6. DPS relinquished control of propulsion and steering.
7. Both the Conning Officer and the Officer of the Deck attempted to transfer control to Bridge mode, with negative results.

8. The Officer of the Deck ordered the Boatswain to let go the starboard anchor, which was accomplished.
9. The Conning Officer placed the Bridge controls into the neutral position.
10. Propeller pitch moved to 60% astern, causing *Elm* to back down under power while at anchor.
11. The Conning Officer depressed the main engine emergency shutdown button on the bridge.
12. Alarms annunciated on the bridge indicating loss of both MPCMS computers.
13. The port anchor was lowered.
14. At 10:34, a toxic gas leak alarm annunciated on the bridge
15. The Officer of the Deck set the General Emergency Bill, and a damage control team was dispatched to the scene of the toxic gas leak.
16. Tugs arrived on scene and mated up to *Elm*.
17. *Elm's* Commanding Officer ordered the engines restarted, clutched in, and passed to pilothouse control. Propulsion checks were unsatisfactory, as thrusters did not remain energized.
18. *Elm* was towed by tug and safely moored at her home pier in Fort Macon, NC.

5.3.5 Step 5 – Analyze the Physical Process

The purpose of this step is to identify physical and operational controls and any potential failures, unsafe interactions, flaws in coordination and communication, and unhandled system disturbances originating from external sources. The goal of this step is to determine why the physical controls that were in place at the time of the incident were not effective in preventing the hazard [20].

Safety Requirements and Constraints Violated:

- The cutter must maintain safe distance from shoals

Emergency and Safety Equipment (Controls):

- Loss of primary MPCMS computer alarm
- Loss of both MPCMS computers alarm
- Loss of DPS control alarm
- MPCMS UPS
- Emergency diesel generator
- Casualty control procedures
- MPCMS technical publication
- WLB Ship's Information Book (SIB)
- General Emergency Bill
- Commanding Officer's Standing Orders
- Anchors (port and starboard)
- Emergency manual propulsion control

Failures and unsafe interactions:

- DPS relinquished control of the propulsion systems (engines, thrusters, CPP)
- Both MPCMS computers dropped off line
- Propeller pitch moved to 60% astern while MSCC controllers were in neutral position
- Refrigeration piping developed a leak, activating the toxic gas alarm

Physical Contextual Factors:

- *USCGC Elm* had just received a new primary radar and electronic chart display system (CG ECDIS), as well as an upgrade to her DGPS receiver.
- *USCGC Elm* was operating in vicinity of her homeport and was under the command of an experienced Commanding Officer who was familiar with both the area of geographic operations as well as the practical operation of the cutter's ISCS.
- The current generation CG DDS was installed on the WLB fleet starting in 2010. CG DDS is a Coast Guard product, built by technicians at the U.S. Coast Guard's C4IT SC. It replaced the previous network (known as "SAFEnet LAN"), which was had been installed by the shipbuilder during construction.
- WLB crewmembers who are ISCS operators and maintainers are required to attend ISCS operator or ISCS maintainer classes prior to transferring to a WLB as part of pre-arrival "pipeline" training. The precise status of training completion for *Elm's* crew at the time of the incident is unknown; for the purpose of this CAST, it is assumed that all designated crewmembers had completed the requisite formal training for their positions.
- Previous documented mishap incidents involving some aspect of the WLB ISCS had occurred within the previous nine months on *USCGC Alder*, *USCGC Hollyhock*, and *USCGC Maple*.
- After the *Elm* incident, conversations with fleet commanding officers indicated that irregularities with system operation were not unusual, though typically not documented and reported to maintenance and safety personnel.

Several actions occur during operation of the ISCS to control the position and heading of the cutter. Any of a number of physical failures within the ISCS could have precipitated a loss of propulsion and/or steering control, thus leading to violation of system safety constraints and ultimately hazarding the cutter.

The physical system – that is, the steering, CPP, thrusters, and main engines – did not experience component failure during *Elm's* incident. However, the system experienced functional failure due to inappropriate actions of the computer controllers. The most noteworthy functional failure in this case occurred when DPS relinquished control of both propulsion and steering and when the MPCMS computers dropped off line. Sufficient data does not exist for a component-by-component analysis of this incident. However, improved data logging capabilities to determine the rate and sufficiency of command messages and system status feedback would improve the ability of technicians to not only look back on incidents to determine areas of equipment failure, but would assist their efforts in diagnosing overall system health in order to avoid future incidents. Additionally, active notification of command latency and impending major system malfunction (e.g., alarms) would improve operator awareness of the current status of the DPS, CG DDS, and MPCMS. In this sense, inadequate feedback existed for *Elm's* ISCS.

5.3.6 Step 6 – Move Up Levels of Safety Control Structure

This portion of the analysis looks beyond the elements covered by most event-chain analyses. Inadequacies in actual physical controls are usually relatively apparent to any analyst. However, analysis of higher levels of the control structure is necessary to understand why physical failures or design inadequacies existed. Specifically, fully understanding behavior at any level of the sociotechnical safety control structure necessitates explanation of how the control at the next higher level allowed (or perhaps even contributed to) inadequate control at the current level [20]. As described in Chapter 2,

many accident models have evolved to include factors outside of the event chain proximal to the accident. For example, the NTSB model includes systemic factors and contributing factors that have the capacity to influence the direct factors of the accident event chain. Even when such models are employed, however, less experienced practitioners may be tempted to find a donkey to pin the blame "tail" onto, and then cease any further analysis – particularly when blame can be plausibly assigned to a human operator. In addition, as no model of the system is part of the analysis, the selection of systemic factors to consider is usually arbitrary and incomplete. In addition, as previously indicated, an accident involving a complex system likely has more than one primary contributing factor.

In the CAST analysis it is assumed that all human operators wish to prevent accidents and do a good job. While this assumption rules out direct gross negligence, such willful carelessness would be apparent to any analyst, regardless of the methodology used. When it comes to human operators, CAST seeks to discover why they did what they did in a given situation. As was discussed in Chapter 3, assignment of blame is not an objective of CAST; rather, CAST is concerned with future accident prevention.

5.3.6.1 ISCS Automated Controllers

As described in Chapter 4, the WLB ISCS relies on computer controllers to control the ship's movements. While in DP or Autopilot modes of operation, the DPS computer issues commands to the propulsion machinery (via the MPCMS) and rudder commands to the steering system. While in the Bridge mode of operation, propulsion commands are relayed to the propulsors by the online MPCMS computer. Propulsion commands travel to the MPCMS via the CG DDS network, and decision-making is influenced by various sensors (e.g., radar, weather sensors) and systems (e.g., CG ECDIS). The section below summarizes the ISCS Automated Controls' safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Maintain awareness of ship's position relative to charted shoals, fixed structures (e.g., piers and bridges), floating structures (e.g., buoys), and other vessel traffic
- Maintain a steady course and/or position, depending on commands selected in DPS
- Maintain the appropriately ordered cutter speed
- Maintain active communication with CG ECDIS to ensure that the ship stays in "good water" (i.e., safe distance from shoals) at all times
- Ensure commands are issued and that feedback messages from controlled machinery are received within specified time periods
- Monitor both the controlled processes and the computers themselves; notify human controllers of abnormal or unsafe conditions

Context:

- Computer-controlled propulsion response was sluggish on the day of the mishap
- Sluggish computer-controlled propulsion response had been previously noted
- The evolution of the integrated computer control systems had been somewhat asynchronous during the cutter's life cycle; numerous upgrades and updates had been made to the DPS, CG ECDIS, CG DDS, and sensors while the MPCMS architecture and components had remained the same

Unsafe Decisions and Control Actions:

- DPS relinquished control of propulsion and steering
- MPCMS did not provide commands to propulsors in a timely manner
- MPCMS carried out last command issued (60% astern pitch) despite significant time delay

Process Model Flaws:

- MPCMS did not formally "recognize" a significant delay in processing commands and did not notify Conning Officer of this significant delay, resulting in Conning Officer thinking that propulsion systems were not controlled
- DPS did not provide Conning Officer with warning of imminent loss of DPS control
- No "push" notification of extent CG DDS memory usage was provided to or displayed for human controllers
- An apparent messaging issue existed between CG DDS and MPCMS, which was evidenced by the need to secure the CG DDS prior to re-booting the MPCMS to temporarily alleviate issues with sluggish MPCMS performance; this was discovered after the incident

5.3.6.2 Conning Officer

The Conning Officer is the person on watch who is in charge of driving and maneuvering the ship. He or she stands watch on the bridge and is assisted by a bridge watch team. The Conning Officer is required to be intimately familiar with all of the cutter's modes of navigation and propulsion, as well as an expert on navigation "rules of the road" as defined by the International Regulations for Preventing Collisions at Sea.

The section below summarizes the Conning Officer's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws. Amplifying information (beyond the contents of the actual mishap report) was obtained via email interview with the officer who was in command of *USCGC Elm* at the time of the incident (he provided details to the best of his recollection).

Safety-Related Responsibilities:

- Maintain awareness of ship's position relative to shoals, fixed structures (e.g., piers and bridges), floating structures (e.g., buoys), and other vessel traffic
- Maintain a safe speed for the ambient environmental conditions
- Ensure that the ship stays in "good water" (i.e., safe distance from shoals) at all times
- Request assistance from Commanding Officer if ever in doubt
- Take bridge initial actions in accordance with the WLB casualty control manual in the event of a casualty to/malfunction of the ISCS

Context:

- Had over one year of WLB conning experience
- Had completed required pipeline ISCS operator training prior to reporting to *Elm*
- Was not adversely affected by weather, as the sea state in the vicinity was unremarkable on the day of the incident
- Had participated in an Operational Risk Management (ORM) brief prior to getting underway on the day of the incident

Unsafe Decisions and Control Actions:

- The command was given to back down hard when propulsion control was first lost; this command was executed by the MPCMS only after the starboard anchor had been deployed, thus causing severe vibration that ultimately resulted in the toxic gas leak

Process Model Flaws:

- Did not recognize a potential for a lag in execution in last ordered command to MPCMS (i.e., 60% reverse pitch) during system malfunction
- Did not realize that MPCMS would carry out any time-lagged commands stored in the CG DDS "buffer" if MSCC controls were in neutral position
- Initially assumed that loss of DPS control was due to a failure within the DPS, and that the MPCMS and CG DDS were both working properly

5.3.6.3 Commanding Officer

The Commanding Officer (CO) is overall accountable for the safety of the cutter and every person onboard. He or she is also responsible for execution of the cutter's assigned missions. These responsibilities are accompanied by an inherent requirement to maintain a "big picture" view of all shipboard evolutions and situations. It is for this reason that a Conning Officer is assigned to navigate the ship while the CO maintains overall responsibility for the operation and safety of the ship within its operating context.

The section below summarizes the Commanding Officer's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety Responsibilities:

- Incorporate risk management into daily operations
- Develop, implement and maintain a mishap response plan
- Establish a safety and environmental health committee which identifies and reviews hazardous conditions, tracks abatement and control actions, and reviews unit mishap reports and mishap messages from similar units to review and implement lessons learned
- Conduct a safety stand down at least annually
- Ensure all personnel are qualified for the watch stations to which they are assigned
- Ensure ORM briefing is conducted prior to any major evolution
- Maintain awareness of ship's position relative to shoals, fixed structures (e.g., piers and bridges), floating structures (e.g., buoys), and other vessel traffic
- Establish clear CO's Standing Orders for the bridge watch team
- Take no unnecessary risks with the cutter or its crew
- Foster a climate of trust and open communication within the cutter crew
- Report any safety related concerns to the responsible U.S. Coast Guard Logistics or Service Center; request specific support as necessary
- Maintain approved equipment configuration onboard cutter
- Ensure all planned maintenance is conducted a prescribed by SFLC and C4IT SC policies
- Ensure necessary unit-level training teams are established and active

- Ensure required drills and training are conducted per Assistant Commandant for Operational Capability policy

Context:

- Experienced officer/leader with high level of ship handling skill
- Cutter was operating after a planned three week inport period, during which major upgrades were made to important navigation subsystems
- Was well aware of other ISCS related incidents that had occurred throughout the WLB fleet in recent months
- During preparations for getting underway on the day of the mishap, the bridge team noticed sluggishness in transition when shifting between propulsion controls at the different consoles
- After getting underway, thrusters were sluggish in response to command inputs from DPS, DPS experienced difficulty controlling the ship's heading in "hold position" mode, and transitions between control modes were slow; these symptoms were known to be leading indicators of an impending loss of MPCMS, but there were no alarms from either MPCMS or DPS before the loss of control occurred

Unsafe Decisions and Control Actions:

- Continued to operate without conducting an updated ORM despite the fact that symptoms of impending loss of MPCMS control being present

Process Model Flaws:

- Incorrectly presumed, with recent work completed by U.S. Coast Guard (USCG) shore-based technicians on the navigation systems and the onboard presence of USCG system experts for the DPS, CG DDS, MPCMS, and CG ECDIS during shake-down testing, that the possibility of an ISCS related accident was relatively small
- Incorrectly presumed that technicians onboard had equal knowledge of all interacting ISCS subsystems
- Did not realize the potential for miscommunication or mistrust between SFLC and C4IT SC technicians and their supported systems (and the potential effect on cutter ISCS discrepancy resolution)
- Attributed the casualty to failure of MPCMS without fully considering other potential factors, leading to "information momentum" through the fleet COs' network regarding the belief that MPCMS "failure" could be imminent on any WLB
  Assumed that MPCMS upgrades could wait until *Elm's* extended shipyard MMA period, which was scheduled for 2018

5.3.6.4 Operational Commander (USCG District Five)

The operational commander (in this case, the Commander of the Fifth Coast Guard District) exercises operational and administrative control over shore-based units and maritime patrol units within his or her area of operations. Administratively, the operational commander is responsible for ensuring positive command climates as well as good order and discipline are maintained at units under his or her control. The operational commander prioritizes and directs resources and assets in accomplishing mission execution.

The section below summarizes the District Commander's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Ensure that the provisions of the afloat safety program (as described by the Coast Guard Safety and Environmental Health Manual) are implemented
- Review mishap reports of subordinate commands
- Ensure an atmosphere of trust and open communication exists with cutter Commanding Officers
- Ensure periodic Cutter Assessments for Readiness and Training (CART) inspections are conducted
- Ensure positive command climate exist onboard all cutters under span of control
- Advocate on behalf of cutter to headquarters or logistics/service centers for needed resource, policy, maintenance, and/or supply support

Context:

- The WLB Major Midlife Availability (MMA) project was due to start in 2015; *Elm* was scheduled to enter its MMA in 2018
- Desired all upgrades and testing on navigation systems to be completed in advance of Fall seasonal buoy operations in September/October
- *Elm* was the only WLB assigned to the Fifth District (which spans the coastal area from Central New Jersey to the North Carolina/South Carolina border); it is highly plausible – even likely – that the District Five Commander was not aware of the pervasiveness of ISCS related issues throughout the rest of the WLB fleet

Unsafe Decisions and Control Actions:

- N/A

Process Model Flaws:

- Presumed that ISCS issues in the fleet were well known in the support community and were being addressed

5.3.6.5 MPCMS Original Equipment Manufacturer (OEM)

The MPCMS OEM was subcontracted by the shipbuilder to architect and integrate the propulsion control system. The section below summarizes the MPCMS OEM's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Provide knowledgeable technical support whenever when contracted to do so
- Overhaul proprietary circuit cards for the MPCMS VME computers and RTUs when contracted to do so

Context:

- The MPCMS operated on an OEM-developed, proprietary messaging syntax and was coded in the Ada programming language

- The USCG did not have a standing technical support contract with the MPCMS OEM
- The USCG had a standing contract with the MPCMS OEM for inspection/repair of MPCMS computer circuit cards
- The OEM was the only authorized repair facility for the MPCMS circuit cards due to their proprietary nature
- The ability of the OEM to repair failed circuit cards was diminishing due to component obsolescence
- The OEM had been acquired by another company since initial WLB delivery
- Only one programmer who worked on developing the original MPCMS code was still employed by the OEM

Unsafe Decisions and Control Actions:

- The OEM did not proactively inform the USCG of component obsolescence concerns
- The OEM made a business decision to not maintain a high level of system knowledge regarding the WLB MPCMS operation or underlying computer code

Process Model Flaws:

- The OEM assumed the USCG was not interested in OEM technical support due to the existence of the USCG's separate ISCS groom contract (not contracted to the OEM)

5.3.6.6 Assistant Commandant for Operational Capability

The Assistant Commandant for Operational Capability (CG-7) exists to set operational requirements for USCG assets and strategically manage Service capital assets to execute assigned and emerging missions. Along with aviation asset and small boat responsibilities, CG-7 oversees several activities related to the planning, acquisition, and management of cutter capabilities while formulating and administering strategies for integration of new assets into the cutter fleet. CG-7 collaborates with support directorates organized under the Deputy Commandant for Mission Support to develop and implement material solutions to meet operational requirements.

With regard to the WLBs, CG-7 was intimately involved in generating and prioritizing requirements for the WLB Major Midlife Availability (MMA), which was scheduled to begin in 2015 and end in 2024. A high priority work item in this midlife renovation package was the upgrade or renewal of the MPCMS system.

The section below summarizes CG-7's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Publish and maintain the USCG Cutter Training and Qualification Manual (Commandant Instruction M3502.4 (series))
- Publish and maintain the WLB Master Training List
- Establish and communicate policy related to cutter operations and employment
- Provide headquarters-level advocacy for the cutter commanding officers and crews
- Provide Office Chief (O6) level representation to the cutter Tripartite (Tri-P) – comprised of representatives from CG-7, the Assistant Commandant for Human Resources (CG-1), and the

Assistant Commandant for Engineering and Logistics (CG-4) – to discuss cutter related safety and environmental health issues and determine corrective action

Context:

- All headquarters directorates were feeling extreme budget pressures from the 2013 budget sequestration and the ensuing debt ceiling crisis, which ultimately led to a partial shutdown of the federal government that lasted for over two weeks
- CG-7 leadership was highly supportive of capital investments for planned new cutters, including both the in-production National Security Cutter and Fast Response Cutter as well as the planned Offshore Patrol Cutter and Heavy Icebreaker; however, funding streams for these new construction projects competed with one another, as well as with major rehabilitation/retrofit project on in-service cutters, such as the WLBs

Unsafe Decisions and Control Actions:

- N/A

Process Model Flaws:

- Assumed any issues with the WLB ISCS could wait to be addressed in the planned WLB MMA

5.3.6.7 Deputy Commandant for Operations

The Deputy Commandant for Operations (DCO) – a three-star admiral – is charged with developing and overseeing execution of operational planning, policy, and international engagement at the strategic level. CG-7 is among DCO's direct-report subordinates (which also include the Assistant Commandant for Intelligence and Criminal Investigations, the Assistant Commandant for Prevention Policy, the Assistant Commandant for Response Policy, and the Director of International Affairs and Foreign Policy). The DCO ensures alignment within mission areas to optimize mission execution as the recognized international leader of maritime safety, security and stewardship. At the time of *Elm's* incident, a primary DCO focus was development of the USCG's Western Hemisphere Strategy, a cornerstone of the USCG Commandant's Strategic Intent.

Safety-Related Responsibilities:

- Provide high-level advocacy for CG-7 interests

Context:

- High level of emphasis and resource priority placed on the Commandant's Western Hemisphere strategy (combatting criminal networks, securing borders, safeguarding commerce)

Unsafe Decisions and Control Actions:

- N/A

Process Model Flaws:

- Was largely unaware of any systemic issues in the WLB fleet affecting safety of navigation

5.3.6.8 Surface Forces Logistics Center

The mission of the Surface Forces Logistics Center (SFLC) is to provide the surface fleet with depot level maintenance, engineering, supply, logistics, and information services to support Coast Guard mission execution. In doing so, SFLC is the primary technical advisor to DCMS, CG-7, and operational commanders regarding cutter and boat engineering and logistics matters. In addition to providing maintenance and material support for all USCG surface assets, SFLC analyzes maintenance data to improve reliability, processes, and procedures. SFLC provides "24x7" customer service to the fleet, including technical advice, logistics management, and casualty response. Product line managers within the SFLC determine asset maintenance requirements and oversee the conduct of depot level maintenance – either through organic personnel or contracted resources – on their portfolios of managed assets.

The section below summarizes SFLC's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Originate maintenance standards for ISCS subsystems managed by SFLC (e.g., MPCMS, DPS)
- Catalogue and distribute all ISCS maintenance standards
- Coordinate and track completion of all prescribed planned maintenance and necessary corrective maintenance onboard supported surface assets
- Specify maintenance periodicity and policy (e.g., whether planned or corrective maintenance items are to be accomplished by crew, shore-based USCG technicians, or contractors)
- Create and maintain procedural guidance for the content and conduct of engineering analysis boards and/or root cause failure analyses
- Convene engineering analysis boards and/or root cause failure analyses as deemed appropriate under procedural guidance

Context:

- 31 MPCMS related casualty reports (system outages/degradations) were initiated by cutter-based WLB technicians from January 2001 – December 2009; a rate of 3.4 casualty reports per year during this period
- 75 MPCMS related casualty reports (system outages/degradations) were initiated by cutter-based WLB technicians from January 2010 – August 2013; a rate of 20.5 casualty reports per year during this period
- ISCS system grooms were outsourced to a contractor; there was no guarantee that the same contractor (with a knowledge base borne of system experience) would be awarded the next contract when it came time to re-compete
- The Contracting Officer's Representative for groom contract had neither system specific knowledge of the ISCS nor immediate access to a designated, knowledgeable Contracting Officer's Technical Representative
- The SFLC product line responsible for maintaining the WLBs was also responsible for maintaining 11 other asset classes

- The SFLC product line responsible for maintaining the WLBs placed its strategic recapitalization focus on planning for the WLB MMA, as well as two other major in-service cutter class recapitalization projects

Unsafe Decisions and Control Actions:

- Did not maintain support or knowledge link with MPCMS OEM via contract
- Several USCG maintenance procedures for the WLB ISCS were out-sourced to the groom contractor, resulting in further erosion of system knowledge possessed by WLB crewmember technicians
- Did not maintain depth of system technical knowledge within the responsible product line
- Did not establish clear ownership of the ISCS suite for systems integration and upgrade purposes

Process Model Flaws:

- Presumed that OEM would maintain technical competence regarding the MPCMS and that knowledgeable and reliable technical assistance would be available for contracting to the government on an "as needed" basis
- Assumed that the contractor hired to complete grooms and recurring maintenance would have consistent knowledge regarding ISCS subsystems
- Assumed that all adjustments/recommendations made by the groom contractor would be in accordance with technical publications and USCG maintenance policies/procedures
- Key SFLC support personnel lacked specific knowledge of C4IT SC supported subsystems (e.g., CG DDS, CG ECDIS) and harbored some mistrust of these subsystems and their interaction with the MPCMS
- Key SFLC support personnel lacked full understanding of system boundary management between MPCMS and CG DDS
- De-emphasized Integrated Logistics Support Management Team (ILSMT) obligations of former after reorganization of USCG naval engineering support commands
- Lacked depth of expertise in ISCS; the most knowledgeable SFLC technical expert was detailed ~50% of time to work on requirements definition and review of contractor submittals pertaining to the USCG's Offshore Patrol Cutter acquisition program
- Presumed that the planned MPCMS upgrade could wait to be performed during each WLB's respective MMA dry-dock maintenance period, with the first cutter entering MMA in 2015 and the last cutter completing MMA in 2024

5.3.6.9 Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC)

The C4IT SC enables USCG mission execution by providing IT and electronic systems and services to the field. It designs, develops, tests, fields, trains, maintains, and disposes of USCG C4IT systems and capabilities. This includes both planned maintenance and unplanned repair of systems. C4IT SC is the field delivery agent of the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (CG-6), and acts as a broker of information and technology services across all USCG units by managing the USCG's technical infrastructure as a strategic asset. This includes managing configuration and cybersecurity aspects of all supported systems.

Specific to WLB system management, the C4IT SC maintains and manages the WLB Land Based Support Facility (LBSF) in Chesapeake, VA and oversees the specialty pipeline training given to ISCS operators and maintainers. The C4IT SC is the primary support facility for CG ECDIS and CG DDS, as well as the surface search radar and DGPS.

The section below summarizes C4IT SC's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Originate maintenance standards for certain ISCS subsystems (e.g., CG DDS, CG ECDIS, radar)
- Maintain LBSF
- Coordinate and host ISCS (including MPCMS, CG EDCIS, and CG DDS) operations and maintenance training courses at Chesapeake, VA facility (location of LBSF)
- Originate and/or process engineering changes pertaining to C4IT SC-managed portions of the ISCS (e.g., CG DDS, CG ECDIS, radar, DGPS)
- Enforce cybersecurity policies on fielded systems
- Manage all phases of the lifecycle for C4IT SC supported systems

Context:

- Technicians and managers lacked specific knowledge of SFLC supported subsystems (e.g., MPCMS, DPS) and harbored some mistrust of these subsystems
- Highest level of emphasis of C4IT SC command was placed on Commandant's cybersecurity strategy, which involved detailing certain managers and technicians with ISCS knowledge to temporarily serve full-time on cybersecurity strategy working groups

Unsafe Decisions and Control Actions:

- Did not maintain configuration management of LBSF
- Did not maintain personnel on staff who adequately understood the inner workings (e.g., programming, hardware deviations from drawings) of the LBSF
- Did not maintain active engagement in ILSMT activities after reorganization of naval engineering support commands

Process Model Flaws:

- Lacked full understanding of system boundary management between MPCMS and CG DDS
- C4IT SC organization is divided into either Product Lines (e.g., DGPS, vessel tracking applications, enterprise networks) or Core Technologies (e.g., communications systems, navigation systems); ISCS is neither a Product Line nor a Core Technology within the current organizational structure
- The LBSF that houses the MPCMS simulator and MPCMS training classrooms is hosted by a C4IT SC facility, but SFLC maintains technical ownership of the MPCMS

5.3.6.10 Health, Safety, and Work-Life Service Center (HSWL SC)

The HSWL SC is CG-1's implementation organization for health, safety, and work-life programs in the field. In addition to providing supervision and standardization for the USCG's medical and dental clinics, HSWL SC provides field units with periodic health and safety inspections, procedures for mitigating

hazards, operational medicine policies and procedures, and case-by-case consultation regarding industrial hygiene matters. HSWL SC representatives are located at regional field offices and provide a local "touch point" for units located within their region. HSWL SC personnel review mishap reports and offer both best practices and suggestions for improvement.

The section below summarizes HSWL SC's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Provide field units with direct advice and service regarding afloat or ashore industrial hygiene matters
- Review mishap reports and provide feedback as deemed appropriate
- Assist units in developing safe work practices using job hazard analysis methods
- Develop tactics, techniques, and procedures to support risk management program assessment, hazard abatement, and reporting requirements
- Assist units with the integration of risk management concepts into the unit safety and environmental health program

Context:

- HSWL SC's limited personnel resources did not enable annual safety audits of cutters
- HSWL SC's involvement in the ATON fleet had been primarily directed toward lead dust and friable asbestos hazards present on the older construction tenders in the fleet; little to no emphasis was placed on the newer WLBs

Unsafe Decisions and Control Actions:

- Did not actively poll cutter fleet commanding officers to obtain their top safety concerns

Process Model Flaws:

- Due to insufficient resourcing to proactively gather first-hand data, HSWL SC largely assumed that "no news is good news" when it comes to safety of cutter systems

5.3.6.11 Assistant Commandant for Engineering and Logistics

The Assistant Commandant for Engineering and Logistics (CG-4) provides the maintenance and logistics elements and policies to sustain operational capabilities, including aircraft, cutters, boats, and shore facilities. This involves obtaining operational needs and priorities from CG-7 and partnering with other DCMS directorates (e.g., CG-6 and the Assistant Commandant for Acquisitions (CG-9)) to deliver the best life cycle engineering and logistics support possible subject to the availability of resources.

The section below summarizes CG-4's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Establish high-level policy governing USCG engineering (civil, aeronautical, naval, energy, and environmental) and logistics activities

- Obtain input from CG-7 regarding asset investment priorities for limited maintenance and sustainment funds
- Prioritize, submit, and defend budgets for asset maintenance and sustainment
- Address points of strategic emphasis for SFLC
- Coordinate asset operational availability targets with CG-7
- Participate as a member of the cutter Tripartite (Tri-P), made up of representatives from CG-1, CG-7, and CG-4 to discuss cutter related safety and environmental health issues and determine corrective action
- Provide Office Chief (O6) level representation to the cutter Tripartite (Tri-P) – comprised of representatives from CG-7, the Assistant Commandant for Human Resources (CG-1), an CG-4 – to discuss cutter related safety and environmental health issues and determine corrective action

Context:

- All headquarters directorates were feeling extreme budget pressures from the 2013 budget sequestration and the ensuing debt ceiling crisis, which ultimately led to a partial shutdown of the federal government that lasted for over two weeks
- CG-4 was providing extensive technical support for requirements generation and review of contractor submittals pertaining to the USCG's Offshore Patrol Cutter acquisition

Unsafe Decisions and Control Actions:

- Did not ensure the Integrated Logistics Support Management Team (ILSMT) was continued under the new SFLC organization
- Did not coordinate with CG-6 to take a systems approach to ISCS management

Process Model Flaws:

- Was largely unaware of the level of systemic issues in the WLB fleet affecting safety of navigation until multiple mishap reports were submitted by cutter COs in 2013

5.3.6.12 Assistant Commandant for Command, Control, Communications, Computers, and Information Technology

The Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (CG-6) is responsible for designing, developing, deploying, and maintaining C4IT systems and infrastructure. Systems governed by CG-6 touch each and every Coast Guard member and asset. In addition to facilitating mission execution through C4IT, CG-6 is responsible for the Service's cybersecurity posture and readiness. Creation and implementation of a Coast Guard Cyber Strategy was one of the USCG Commandant's highest priorities and was thus one of the primary focuses of CG-6 during this time period.

The section below summarizes CG-6's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Establish and promulgate high-level policy governing all USCG command, control, communications, computer, and information technology, including cybersecurity standards

- Prioritize C4IT projects for funding based on input from other assistant commandants and operational commanders
- Obtain input from CG-7 regarding asset investment priorities for limited C4IT maintenance and sustainment funds
- Prioritize, submit, and defend budgets for C4IT system maintenance and sustainment
- Address points of strategic emphasis for SFLC

Context:

- All headquarters directorates were feeling extreme budget pressures from the 2013 budget sequestration and the ensuing debt ceiling crisis, which ultimately led to a partial shutdown of the federal government that lasted for over two weeks
- Lacked full understanding of system boundary management between MPCMS and CG DDS
- Highest level of emphasis on Commandant's cyber strategy

Unsafe Decisions and Control Actions:

- Did not coordinate with CG-4 to take a systems approach to ISCS management

Process Model Flaws:

- Presumed that all ISCS interfaces were well understood and tested by logistics/service center personnel

5.3.6.13 Assistant Commandant for Human Resources

The Assistant Commandant for Human Resources (CG-1) is responsible for all aspects of USCG human resources policy (civilian, active duty, and reserve), including force planning, recruiting, training, administration, separation, and everything in between. These responsibilities encompass human-system integration and health/safety policy. In the context of health and safety, the Assistant Commandant for Health, Safety, and Work-Life (CG-11) – a direct subordinate of CG-1 – is responsible for policy pertaining to mishap reporting and investigation.

The section below summarizes CG-1's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Manage the planning and implementation of effective human systems integration for all facets of system acquisitions including cutters, aircraft, C4ISR, logistics systems, and the associated workforce
- Provide input for changes to crewing, performance support, system and asset configuration, research and development, and supportability
- Initiate, review and evaluate program-related analyses; participate in the establishment and approval of all entrance/exit criteria for all program phases; develop and update documentation to support the system acquisitions programs
- Develop, manage and execute a comprehensive Loss Control and Prevention Program to assess risks, identify trends and control risks associated with USCG operations
- Oversee and analyze Afloat Safety policy and program requirements and leverage scarce resources to produce afloat safety programs that are more effective

- Manage, direct, and coordinate all aspects of the USCG afloat mishap investigation process
- Monitor and evaluate afloat safety policy and program implementation by afloat units
- Manage Team Coordination Training, and coordinate Operational Risk Management and Crew Endurance Management training for fleet-wide afloat use
- Maintain liaison with other major operational and support programs especially Boat and Cutter Forces and Naval Engineering on all issues
- Provide system safety and occupational health inputs to systems engineering technical reviews during the capital acquisition process
- Participate as a member of the cutter Tripartite (Tri-P), made up of representatives from CG-1, CG-7, and CG-4 to discuss cutter related safety and environmental health issues and determine corrective action

Context:

- The USCG places high emphasis on personnel safety
- Although input method (e.g., Web-based) has changed, the basic USCG mishap reporting and investigation system has not changed appreciably in many years

Unsafe Decisions and Control Actions:

- N/A

Process Model Flaws:

- Presumed that command-level investigation into near-miss mishaps was sufficient to identify preventive measures
- Allocated the bulk of personnel resources to craft and review policy related to more tangible threats to health and safety (e.g., remediation of lead dust and friable asbestos on older cutters)
- Presumed that any issues related to safety of onboard control systems requiring CG-11 attention would be raised by CG-7, SFLC or C4IT SC

5.3.6.14 Assistant Commandant for Acquisition (CG-9)

The Assistant Commandant for Acquisition's primary mission is to efficiently and effectively deliver the capabilities needed to execute USCG missions. These capabilities are defined and communicated by CG-7, with input from CG-1, CG-4, and CG-6. In managing the acquisition portfolio, CG-9 applies risk-based decision making and analysis practices to balance factors that influence program cost, schedule, and performance constraints. Additionally, CG-9 is responsible for developing and delivering logistics support products for acquisition programs to best assure achievement of capability, readiness, and sustainability objectives over the assets' service life cycles.

The section below summarizes CG-9's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Oversee acquisition, integration and delivery of assets and systems
- Ensure development, maintenance, and/or compliance with all program-related plans and existing directives

- Provide direction and guidance for Acquisition Program Managers and Project Managers to define and best satisfy program cost, schedule, and performance objectives while identifying and managing risk throughout the acquisition life cycle
- Liaison with sponsors and technical authorities for their appropriate participation in: project management activities, systems engineering activities (including systems integration), logistics activities, test and evaluation activities, and enterprise architecture activities
- Coordinate with acquisition program sponsor (CG-7) to ensure specifications meet requirements
- Coordinate with CG-1 to produce a System Safety Management Plan for new capital acquisitions
- Coordinate with CG-1 to ensure contractor developed plans for human systems integration, human factors engineering, and the contractor's system safety program plan are incorporated as required deliverables into the acquisition contract
- Provide acquisition logistics products and services in support of the acquisition of new surface assets

Context:

- The 225' *Juniper* class WLBs were designed and built to meet a USCG objective of reduced crewing through increased use of computer-controlled automation, particularly for navigation and buoy positioning; per the Operational Requirements Document (ORD), the total crew compliment on each 225' WLB would be 40 personnel, compared to approximately 50 on the smaller, less-capable 180' WLBs they were replacing
- At the time of the mishap, CG-9's highest priority in the surface domain was active acquisition of planned new cutters, including both the in-production National Security Cutter and Fast Response Cutter as well as acquisition planning efforts for the Offshore Patrol Cutter and Heavy Icebreaker
- CG-9 owned project management responsibilities for the upcoming WLB MMA
- Appropriated funds for the WLB MMA would not be available until fiscal year 2015; this funding was programmed to begin the MMA for *USCGC Oak* (the lead ship for the MMA project)

Unsafe Decisions and Control Actions:

- The WLB integrated logistics support plan (ILSP) did not address lifecycle logistics updates for IT systems

Process Model Flaws:

- Presumed that the original WLB ILSP would be adhered to for the cutters' service lives
- Assumed MPCMS recapitalization would be best performed as part of each individual cutter's approximately one-year MMA shipyard period (beginning with *USCGC Oak* in 2015 and ending with completion of the final WLB's MMA in 2024)
- Did not explicitly account for ISCS system safety degradation over time due to wear-out, obsolescence, or asynchronous evolution

5.3.6.15 Tri-Partite (Tri-P)

A cross-functional headquarters body known as the "Tri-P" provides prioritization and resolution of current surface fleet issues. The group is co-chaired by the Office of Naval Engineering (under the Assistant Commandant for Engineering and Logistics) and the Office of Cutter Forces (under the Assistant Commandant for Operational Capability). The Office of Afloat Safety also provides primary

representation on behalf of CG-1. The weekly Tri-P meetings provide a forum to discuss multiple matters of interest pertaining to cutter fleet support, including safety issues in the context of operational and maintenance requirements. CG-6 provides representation at these meetings, as well. While the "principals" at the meetings are typically office chiefs (O6 level), staff members are expected to attend and brief out on their individual areas of responsibility when they believe they have items of interest to pass; the only restriction on attendance is physical room capacity. Each meeting is scheduled to last for 1.5 hours.

The section below summarizes the Tri-P's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Provide a forum for the informal sharing of concerns and conflict resolution within the engineering, operational, and safety communities
- Recommend budget priorities to senior leadership for allocation of operating and maintenance funds
- Recommend budget priorities to senior leadership for allocation of acquisition funds
- Provide a "one stop shop," direct forum for operational commanders to share concerns and requests for headquarters-level action when multiple directorates' involvement is required to resolve an issue

Context:

- The Tri-P meets every week, unless special meetings (in additional to regular meetings) are called
- The Tri-P has no formal charter – it is intended to be an informal body that presents unified positions and recommendations to senior executive decision makers
- Meetings typically have no formal agenda and are conducted in round-robin discussion format

Unsafe Decisions and Control Actions:

- Mishap reports that may have been appropriate to receive consideration/action from multiple headquarters directorates were not typically reviewed as part of recurring Tri-P agenda

Process Model Flaws:

- Tri-P members did not initially fully appreciate the pervasiveness of ship control issues due to a general sense of acceptance and resultant under-reporting from the fleet
- While the Tri-P intentionally has no charter and was designed to be an informal advisory and information sharing body, Tri-P principals frequently make fleet-wide policy and resource related decisions, such as prioritization of budgeting for engineering changes

5.3.6.16 Deputy Commandant for Mission Support (DCMS)

The Deputy Commandant for Mission Support – a three-star admiral – is responsible for life cycle management of USCG assets (including cutters, boats, shore facilities, and aircraft) from acquisition to disposal. Additionally, DCMS oversees all aspects of USCG human resources, including training and safety policy. As part of his/her responsibilities, DCMS supervises the Assistant Commandant for Human Resources (CG-1), the Assistant Commandant for Engineering and Logistics (CG-4), the Assistant

Commandant for C4IT (CG-6), and the Assistant Commandant for Acquisitions (CG-9). It is DCMS' responsibility to ensure that timely, standardized, and effective mission support services are delivered to operational commanders to facilitate mission execution.

Given his/her level in the organization, DCMS is the common denominator among support providers. Thus, it is incumbent upon DCMS to ensure that optimal levels of standardized processes and governance exist among his/her subordinate assistant commandants. Examples include minimizing any "seam" issues in policy and procedures that may arise between responsible directorates (e.g., CG-4 and CG-6), as well as establishing clear channels of engineering technical authority within the various DCMS disciplines. The USCG's Engineering Technical Authority instruction (signed by DCMS) defines engineering technical authority as "the authority, responsibility, and accountability to establish or assert engineering technical standards, tools, processes, and best practices; monitor compliance with or use of them; and certify conformance with statute, policy, requirements, architectures, and standards."

The section below summarizes DCMS's safety-related responsibilities, operational context, unsafe decisions and control actions, and process model flaws.

Safety-Related Responsibilities:

- Establish clear lines of formal engineering technical authority and enforce their application
- Lead and coordinate the USCG mission support community, including all USCG logistics/service centers, capital acquisition programs, human resources administration, formal training, and health and safety

Context:

- All headquarters directorates were feeling extreme budget pressures from the 2013 budget sequestration and the ensuing debt ceiling crisis, which ultimately led to a partial shutdown of the federal government that lasted for over two weeks
- Major issues facing DCMS at the time were the human resources impacts of sequestration and maintaining positive momentum in capital acquisition programs through the budget crisis.

Unsafe Decisions and Control Actions:

- Despite efforts that had been in place since 2010, a formal engineering technical authority program was not yet established, as required by the Coast Guard Authorization Act of 2010; a formal ETA governance structure would provide a clear set of checks and balances for asset lifecycle management and imbue authority in specific qualified, technically warranted personnel in technical decision making, thus avoiding conflicts of interest between project sponsors, acquisition program managers, and technical experts
- Did not promulgate or require a formal Integration, Test & Evaluation (IT&E) instruction for systems with potentially high safety impact

Process Model Flaws:

- Was largely unaware of any major systemic issues in the WLB fleet affecting safety of navigation

5.3.6.17 Step 6 Summary

Several entities within the physical system's hierarchical control structure were analyzed in this step. The analysis included not only the computer controllers (i.e., DPS and MPCMS) and the human controller (i.e., the Conning Officer), but also multiple levels within both the operational chain of command and the support chain of command.

Onboard the cutter, the physical controlled systems (i.e., steering, propulsion) did not malfunction. Similarly, it was not demonstrated that the ISCS computer controllers functioned counter to their programming. However, the time delays associated with processing and executing commands clearly led to loss of propulsion control. The system was designed for redundancy of MPCMS computers. It is very important to have one MPCMS computer online relaying control commands at all times. In this case, however, both computers ended up off line at the same time, and not due to coincidental component failures within both computers. The system design did not appropriately take into account external (to the MPCMS) reasons that could lead both MPCMS computers to be offline against the wishes of the operator. As was described in Section 5.3.6.1 and will also be seen in Chapter 6, timing issues precipitated by the characteristics and encoding of the messages between ISCS subsystems was likely a contributory factor in this incident. Similarly, memory persistence of the MPCMS (upon system reboot) was not well documented or understood. Compounding these system interface issues was the incomplete mental model of the human controller, who was unaware of the specifics of the interface issues.

The Conning Officer issued the command to back down away from shoal water after MPCMS responsiveness was severely compromised and DPS had dropped out of the loop. Due to the extreme sluggishness of propulsion response immediately before MPCMS dropped off-line, this command was eventually delivered to the CPP system several seconds later, after the anchor had already been let go. This inadequate control action led to backing down hard while at anchor, causing the vibration that led to the toxic gas leak.

Additionally, the Conning Officer assumed that the loss of propulsion control was caused by a DPS casualty when, in reality, DPS relinquished control due to lack of responsiveness on the part of the MPCMS. Due to this misperception, attempts were made to regain control in Bridge mode at the MSCC. This resulted in the cutter drifting for additional time without positive propulsion control. Because the actual casualty involved loss of MPCMS control, the only way to quickly regain control was via local control in the engine room while the MPCMS computers were rebooted.

Upon recognizing the symptoms that had typically precursed an MPCMS casualty, the Commanding Officer did not update the cutter's ORM status by halting operations to re-evaluate operational risk. While he did order a test of the DPS via a twist to port while in "hold position" mode to ensure the proper operation of the DPS prior to the making the final leg of the transit into port, it may be argued that the timing and location of this test assumed unnecessary risk given the symptoms that were present. With additional technicians and subject matter experts from the Surface Forces Logistics Center (SFLC) and the Command, Control, Communication, Computers, and Information Technology Service Center (C4IT SC) onboard for the shake-down cruise, the CO had a greater tolerance for risk in terms of the ISCS than he otherwise would have, despite knowing the recent history of fleet mishaps related to the MPCMS.

The USCG did not enter into a service/technical support contract with the OEM after delivery of the WLBs. Because the USCG did not purchase the data rights to the MPCMS, its details remained OEM proprietary technology. System grooms were possible via a knowledgeable third party contractor, but when it came to repairing components or analyzing programming code, the OEM was the only provider of services. Because the USCG did not seek a robust and recurring technical support contract with the OEM, the overall level of technical competence within the OEM was allowed to slowly diminish. This erosion accelerated when the company was acquired by a larger defense contractor in 1998.

The overall context surrounding the incident was multi-layered. The ISCS subsystems and controllers had evolved asynchronously. While upgrades and engineering changes were carefully integrated into the existing system, there remained unknown effects of these changes that grew over time. While the status of ISCS support (both from within the Coast Guard and from external entities) was known by those who routinely operated the system, the shortcomings in this support and their resultant effects were not readily known by decision makers who controlled budget allocation and priorities. Similarly, deficits in ISCS operating performance were well known among cutter Commanding Officers; however, the "routine" nature of system malfunctions (not relating in mishap incidents) was not known or fully appreciated by front-line support personnel. At higher levels of leadership and budget allocation, the Coast Guard's clear priorities fell in behind the Commandant's strategic goals (appropriately so), which included recapitalization of aging cutter classes, acquisition of a new heavy icebreaker, and hardening cyber security defenses. An unforeseen side effect of these higher priority projects was their involvement of personnel resources that would otherwise have had significant portions of their time and attention dedicated to supporting the ISCS and its constituent systems.

In addition to sustainment, CG-4 was highly involved in the acquisition of new cutter assets at the time of *Elm's* mishap. While the resourcing of the WLB MMA was a priority, higher acquisition priorities included partnering with CG-9 to ensure a smooth award of the Offshore Patrol Cutter project (the largest fleet recapitalization project in USCG history) and working with CG-7 in requirements definition for a new heavy icebreaker (a national security imperative). All of this activity was superimposed onto the bleak budgetary backdrop inflicted by sequestration limitations resulting from the Budget Control Act of 2011.

CG-4 exercises supervision of the SFLC, and oversaw the 2009 reorganization that resulted in the agglomeration of multiple surface fleet naval engineering support entities to form SFLC. This was a huge undertaking; with limited staff to tend to all the details, some standing bodies, such as the WLB Integrated Logistics Support Management Team (ILSMT), either lost effectiveness or silently disappeared during the reorganization. As a result, the assignment of ISCS support responsibilities was not clearly mapped to the current organizational structure. Arguably the most effective matrixed team involved in oversight of integrating engineering, safety, and operations – the Tri-partite – operated without the existence of a charter to provide clear expectations for the group.

Although a handful of mishaps and near-miss incidents involving WLB MPCMS had been reported leading up to *Elm's* incident, the reports were not effectively strung together to enable a purposeful and objective systemic look at the problem. Although internet tools allow mishap reports to be filed more quickly and easily, the onus to submit such a report was still on the affected unit, and the basic format of the mishap report (and its required contents) had remained unchanged for many years. Given the budget climate at the time of *Elm's* incident, HSWL SC had been forced to cut back on field unit visits

due to a lack of sufficient funding. The primary engagement between HSWL SC, SFLC, and the cutter community since 2011 had been with regard to lead dust and friable asbestos hazards on older buoy tenders and construction tenders; the focus was not on the "newer" cutters, such as the WLBs.

While the Coast Guard was moving toward establishment of a clear line of Engineering Technical Authority that had the signature approval of senior leadership, such a formal system was not yet in place at the time of *Elm's* incident. Those personnel and staffs that were aware of the nature of the ISCS system issues understood that the MPCMS would be recapitalized during each cutter's shipyard MMA period; however, the final cutter was not due to complete MMA until 2024.

Finally, a number of communications issues were present and contributed to the issues discussed above. These are discussed in detail in the next section.

5.3.7 Step 7 – Examine Overall Coordination and Communication

Step 6 looked at the responsibilities, process model flaws, and unsafe decisions and control actions associated with each relevant person and organization within the system's hierarchical control structure. It also provided the context for these actions, decisions, and mental models. The result is a more complete picture of who brought what to the table in terms of responsibilities, influences, perceptions, and actions. When any complex system operates, effective communication and coordination between the system and its operators is clearly necessary. What may be slightly less obvious is the importance of communication and coordination up and down the levels of the system's control structure.

This step explores coordination and communication among controllers, which is necessary to eliminate confusion. Regarding this topic, Leveson states:

> Each controller may have different responsibilities, but the control actions provided may conflict. The controllers may also control the same aspects of the controlled component's behavior, leading to confusion about who is responsible for providing control at any time [20].

Identification of key aspects of each controller in Step 6 allows the pieces to all be put together from a system perspective and determine if the controllers operated in conflict with one another, performed their tasks based on inaccurate or outdated information (or no information at all), or were unable to perform their tasks due to poor coordination or communication.

Step 6 of the *Elm* CAST analysis sheds light on the fact that multiple entities were involved in managing the maintenance and configuration of the ISCS and its related sensors. Some of the subsystems (e.g., CG DDS, CG ECDIS, radar, DGPS) were managed by the Coast Guard's C4IT Service Center. Others (e.g., MPCMS, DPS, MSCC interface) were managed by the Coast Guard's Surface Forces Logistics Center. While coordination was partially effective – for example, the CG ECDIS, DGPS, and radar were all upgraded at the same time after evaluating the anticipated effects the upgrades would have on one another – overall integration and maintenance of the ISCS suffered somewhat from want of a clear owner/integrator. Additionally, discussions with support personnel from both SFLC and C4IT SC around the time of *Elm's* incident revealed an underlying mistrust of the others' systems, along with a stated belief that the root causes of the issues that manifested themselves via loss of MPCMS control lay with the others' systems. For example, an SFLC MPCMS subject matter expert felt strongly that the problem resided in the CG DDS. In contrast, a C4IT SC CG DDS subject matter expert pointedly opined that the

MPCMS was the culprit. This sometimes not-so-subtle finger pointing was reminiscent of 1980s television commercials for Reese's peanut butter cups™ ("You put your chocolate in my peanut butter!" "You put peanut butter on my chocolate!"), only without the tasty treat at the end. In conversations, personnel from SFLC and C4IT SC clearly demonstrated both defensiveness toward their own systems and mistrust/lack of complete understanding of the others' systems (MPCMS and CG DDS, in particular).

Communication and coordination onboard *Elm* during the actual incident appears to have been reasonably smooth, considering the circumstances. The Conning Officer took appropriate action to try to regain Bridge control at the MSCC when DPS relinquished control. When control was not regained, the starboard anchor was ordered to let go to stop the cutter from drifting into shoal water. According to the mishap report, the anchor detail was quick to respond and "averted catastrophe." There is no indication that the response to the ensuing toxic gas alarm was anything but orderly and effective.

Elm's mishap report stated that "clear" symptoms that were known to be indicators of impending MPCMS loss were present during sea trials on the day of the mishap. It is not clear how this information was disseminated to the bridge watch team, the engineering watch team, the anchor detail, or the shore-based technicians who were on board for sea trials. The pre-underway operational risk management brief included shore-based technicians, each of whom explicitly stated during the brief which piece of equipment he/she would be directly monitoring while underway. An updated operational risk management brief was not conducted when the "sluggishness" symptoms began to manifest themselves in an underway environment. The first mention of these symptoms are in the "first level reviewer comments" of the mishap report. Given that notice of these symptoms is not explicitly mentioned in the chain of events detailed in the mishap report, it is reasonable to infer that some level of the phenomenon known as "hindsight bias" is at work. It becomes apparent after the incident that these symptoms (sluggishness of ISCS response) "should have" been a harbinger of bad things to come, and that preventive and diagnostic actions "should have" been taken as soon as the symptoms appeared. However, no alarms were received and ISCS system experts were onboard during sea trials. Both of these factors gave *Elm's* commanding officer a degree of comfort that he likely otherwise would not have had, despite what his bridge team was experiencing in terms of propulsion control response.

Communication between SFLC and cutter commanding officers and cutter engineer officers regarding the pervasiveness of ISCS issues within the WLB fleet was clearly not effective. This was evidenced by the mishaps that, in addition to *Elm*, occurred on *Hollyhock*, *Alder*, and *Maple* and the fact that no holistic response was immediately generated by the USCG mission support enterprise (specifically, SFLC and C4IT SC) to explore systemic issues. Additionally, several other instances of improper functioning of the ISCS occurred on other WLBs but went unreported – this was discovered later when questionnaires asking for specific data were circulated to WLB engineer officers by the SFLC. Information concerning those incidents that were reported was shared in accordance with USCG procedures for mishap reporting, but the true level of urgency did not appropriately register outside the cutter community until *Elm's* incident. This may have been partially attributable to the fact that senior technicians from both SFLC and C4IT SC were onboard at the time of the incident and observed the gravity of the situation firsthand. The Coast Guard "cutterman" community has a general reputation for self-reliance and getting the job done without complaint. The fact that none of the previous reported incidents mentioned above resulted in any actual damage or injury may have also contributed to the lack of a strong demand signal from the cutter commanding officers and their operational commanders (or, conversely, the lack of reception of a clear demand signal on the part of the mission support

community). As the saying goes, communication is a two-way street; it requires both sending and receiving. At the time of *Elm's* incident, the strategic focus of the responsible SFLC product line was on multiple larger recapitalization projects, including the anticipated WLB MMA (which was scoped and budgeted to include upgrades to the MPCMS over a multi-year period). Until *Elm's* incident, the response to ISCS issues had been one at a time and tactical in nature. This lack of overall strategic coordination to examine the ISCS issues as a fleet-wide system resulted in treating only the symptoms of the problems.

The Coast Guard's mishap reporting system is the fleet's official conduit for reporting a loss event or a near-miss incident. While the existing reporting system sufficed for this purpose in *Elm's* case, it appears to have been used primarily as an administrative notification tool and not to provide the information to identify common and pervasive problems. Multiple near-miss incidents had occurred in the previous two years, involving a number of cutters. While some mishaps were reported, it is unclear if more than a cursory effort was expended in analyzing and correlating the data between the reports. Lack of clear, publicized correlation may have raised the profile of the WLB ISCS issues sooner.

Finally, the coordination of initial and follow-up actions in the event of a safety-threatening casualty to any ship system is governed by the WLB casualty control manual (CCM). This publication provides the steps to be followed by the bridge and ECC watch teams in the event of a casualty. Given the evolving nature of the ISCS issues and the static nature of the CCM, it appears that a revision to the CCM may have been in order to better coordinate crew response to known symptoms of an ISCS casualty.

5.3.8 Step 8 – Dynamics of System and Migration to High Risk State

The 225' WLBs began their service with the commissioning of *USCGC Juniper* in 1995. A total of 16 WLBs were eventually delivered by the shipbuilder and placed into service. Severe issues with the ISCS (such as loss of DPS control or loss of MPCMS control) were infrequent for several years. Casualty report data describes a significant uptick in both the number and severity of casualties that began in roughly 2010. Specifically, 31 MPCMS related casualty reports (system outages/degradations) were initiated by cutter-based WLB technicians from January 2001 – December 2009 (nine years), whereas 75 MPCMS related casualty reports (system outages/degradations) were initiated by cutter-based WLB technicians from January 2010 – August 2013 (less than four years). This phenomenon may be described as a system migration to an unsafe (or at least less safe) state.

A number of contributory factors revealed themselves in Step 6 of this CAST, particularly in the categories of context, unsafe control actions and decisions, and process model flaws. Tangible indications of this movement to a higher risk state were present in the form of documented recent mishaps on *USCGCs Alder, Hollyhock, and Maple*. Additionally, *USCGC Willow* experienced a loss of MPCMS that resulted in a pier allision in August 2009. In April 2009, CG DDS was installed on *Willow* as a form, fit, and functional replacement for the SAFEnet LAN, and it interfaced with the original versions of the MPCMS and DPS, as well as ECPINS (an electronic chart display system that was the pre-cursor to CG ECDIS). This was the first major update to a primary ISCS subsystem. In the investigation following the allision, failure of CG DDS was ruled out as a cause of the accident. The primary cause was officially attributed to loss of MPCMS control in close proximity to the pier, which was determined to have been caused by a faulty (intermittent) relay, a faulty circuit card, and numerous loose connections in various RTUs [29]. Despite this finding, SFLC's primary MPCMS subject matter expert remained vocal that he believed the new CG DDS was a causal factor in the accident, noting that newly updated CG DDS

software was provided to the *Willow* following the accident that resulted while operating with the CG DDS prototype software.

The 2009 accident onboard *Willow* highlights at least four broader (not specific *Willow* or CG DDS) factors that contributed to migration to a higher risk state. The first is the issue of asynchronous system evolution. Although CG DDS was "officially" eliminated as a potential causal factor in the *Willow* investigation report, its installation was the first of a series of ISCS upgrades. In the three years that followed, CG DDS was updated throughout the fleet, ECPINS was replaced by CG ECDIS, DPS was updated, the DGPS receiver was updated, and the AN/SPS-73(V) surface search radar was replaced by the AN/SPS-50(V) radar. As described in Chapter 1, each of these subsystems directly or indirectly interacts with the MPCMS, which remained largely unchanged since its original delivery. While due diligence was performed to document and prototype engineering changes to ISCS subsystems, design errors were likely introduced over time. Without direct access to OEM-level MPCMS expertise, it was difficult for the Coast Guard support community to effectively eliminate these design errors.

A second factor was the numerous loose connections that were found in *Willow's* MPCMS RTUs. In hindsight, this is not surprising. Homeported in Newport, RI, *Willow's* ice-capable hull was routinely used for winter ice breaking operations in New England, Long Island Sound, and the Hudson River. The vibrations caused by repetitive stress cycles associated with ice breaking are now known to loosen these connections. However, when the loose connections were discovered in 2009, no new fleet-wide maintenance procedures to check the tightness of the connections on a periodic basis were implemented. Internal SFLC emails to which the author had access indicated that loose connections were later found to be potential causal factors in "loss of MPCMS control" incidents that occurred in Fall 2013. Failure to implement maintenance procedures directing technicians to check/tighten these connections contributed to the migration to an unsafe state, particularly for those WLB that routinely engaged in icebreaking operations.

The 2008 update to the WLB Integrated Logistics Support Plan (ILSP) created a cross-functional Integrated Logistics Support Management Team (ILSMT) to annually review the ILSP and coordinate/monitor logistics support. A member of an SFLC precursor organization was designated as the ILSMT chairperson, and team members were selected from the human resources (CG-1), naval engineering (CG-4), electronics engineering (CG-6), and cutter management (CG-7) communities to manage "logistics elements" consisting of everything from training support and technical data to design interface and maintenance planning.

The updated WLB ILSP also called for creation of an Integrated System Management Team (ISMT) and an Integrated System Support Team (ISST) to guide life cycle logistics for the WLBs. The ISMT's mission was to provide resources, management, and technical oversight to the ISST. The office chiefs from the two applicable offices in CG-4 and CG-6 (specifically, the Office of Naval Engineering (CG-45) and the Office of Enterprise Infrastructure Management (CG-64)) were designated as ISMT co-chairs, with membership provided by CG-751 (the Office of Cutter Forces) and commanders of the precursor organizations to the SFLC and the C4IT SC. The ISST was a matrixed organization, including subject matter experts from the precursor organizations to the SFLC and the C4IT SC as well as contractors (for ISCS groom support). The mission of the ISST was, among other things, to provide systems support and management for navigation and propulsion control to ensure optimized "throttle to propeller"

performance. Additionally, the LBSF was established in Chesapeake, VA. The support concept was as follows:

> C2CEN [C4IT SC precursor] was designated as the SMEF [System Management Engineering Facility] for ECPINS and SAFEnet LAN and ELC [SFLC precursor] was designated as the equipment manager for DPS and MPCMS [30].

Despite the inevitable confusion that undoubtedly arose from having three related teams with very similar acronyms, indications are that the support plan, which relied heavily on ISCS grooms and assessments conducted by knowledgeable contractors, provided an additional depth of support that was needed for the ISCS and other systems. Over the next 3 years, however, major restructuring took place within the Coast Guard's support community. The former Engineering Logistics Center (ELC) was deconstructed and was absorbed in the stand-up of the SFLC. Likewise, the creation of the C4IT SC subsumed staff elements that were represented on the ILSMT and ISST. Supervisory chains and priorities shifted; military members transferred to new assignments. While the contracted ISST grooms remained in place (although the contract term expired and was subsequently re-competed and awarded to a different prime contractor), regular ISST and ILSMT meetings became a thing of the past.

This devolution of the cross-functional support concept resulted in less frequent dialogue and information sharing regarding the WLB ISCS between CG-7, SFLC, and C4IT SC personnel who would have otherwise been brought together by team meetings. This likely contributed to the lack of recognition of serious ISCS-related issues that could hazard the WLBs. Furthermore, the "split support" concept (ECPINS/CG ECDIS, DGPS, radar, and CG DDS are supported by C4ITSC; MPCMS and DPS are supported by SFLC) became more difficult to coordinate without the benefit of dedicated periodic team meetings.

Finally, the lack of an actively managed ISCS technology management plan resulted in not only asynchronous evolution, but an erosion of specific technical knowledge – both within the USCG and external to the Service. The handful of Coast Guard shore support subject matter experts were split between SFLC and C4IT SC, and the lack of ILSMT and ISST meetings led to independent evolution of opinions regarding the efficacy of the various subsystems. While the Coast Guard maintained an ISCS assessment/groom contract with a non-OEM contractor, no active relationship was pursued with the MPCMS OEM. As a result, SFLC and C4IT SC were unaware of the onset of obsolescence issues. Additionally, the OEM did not maintain a strong working technical knowledge of the system and the proprietary software running on it; maintaining this level of knowledge was not profitable in the absence of a support contract offered by the government. At least one corporate merger occurred, and some of the MPCMS OEM's most knowledgeable technicians moved on to other employment. It is possible that a recurring support contract between the USCG and the OEM could have retained a sufficient base of knowledge within the OEM's capabilities to meet the USCG's needs over the MPCMS' lifecycle.

5.4 Recommendations Pursuant to CAST of *Elm* incident

The mishap report released by *USCGC Elm's* command was brief and to the point. Sufficient details were included to follow the chain of events. Personal knowledge of the situation and follow-up interviews filled in the gaps that existed in formal documentation, enabling this CAST analysis to be conducted. By

following the step-by-step process prescribed for the CAST method, numerous shortcomings in controls were discovered. These were summarized in Sections 5.3.6.17, 5.3.7, and 5.3.8.

Final recommendations are made below.

ISCS Computer Controllers:

- Incorporate active monitoring of message timing between DPS, CG DDS, and MPCMS.
- Notify Conning Officer when message latency exceeds some threshold.
- Incorporate system diagnostic self-checks for DPS, CG DDS, and MPCMS based on criteria critical for uninterrupted operation.
- Ensure ISCS provides clear, unambiguous indication to the bridge team of current mode of operation at all times.

Operational Chain of Command:

- Notify appropriate logistics and service centers in the event of any incident calling into question the safe control of a cutter.
- Actively request Tri-P involvement with issues related to system safety.
- Emphasize the importance of re-evaluating operational risk management for an evolution in the event of significant changes in environment, equipment, or personnel.

DCMS Organization:

- SFLC publish standardized ISCS casualty control procedures, incorporating fleet input and feedback.
- HSWL SC provide correlation between mishap reports to find common themes.
- HSWL SC notify CG-11 of these correlations for discussion at Tri-P.
- HSWL SC notify SFLC/C4IT SC of mishap correlations involving their respectively supported systems.
- SFLC engage in support contracts with OEMs/licensed service providers or develop enduring, certified in-house expertise with adequate capacity to maintain and repair critical systems.
- SFLC/C4IT SC evaluate balance of contracted vs. organic maintenance capability/capacity; establish long-term plan to ensure adequate knowledge management regarding ISCS and related subsystems.
- CG-4 re-evaluate WLB lifecycle logistics management infrastructure and re-invigorate cross-directorate logistics management organizations (e.g., ILSMT), as deemed appropriate; directly involve logistics and service center subject matter experts in dialogue.
- CG-4/CG-6/SFLC/C4IT SC obtain/train and dedicate sufficient subject matter experts to manage both existing ship control systems and requirements generation and contract deliverable reviews for new acquisitions.
- C4IT SC baseline configuration of ISCS LBSF and ensure it is well-documented and is as similar as possible to shipboard installation.
- SFLC/C4IT SC re-evaluate current pseudo-stovepipe “split” of ISCS subsystem lifecycle management between SFLC and C4IT SC; consider creation of and ISCS/MPCMS product line to reduce ISCS interface issues generated/exacerbated by duality in support organizations.

- DCMS publish and promulgate clear Engineering Technical Authority instruction (note – this completed in May 2015).
- SFLC/C4IT SC review engineering change procedures to ensure adequate protections are in place (modeling, LBSF prototyping) to protect against encountering negative effects of asynchronous evolution of computer-intensive systems.
- SFLC create fleet-wide recurring maintenance procedures based on vetted "best practices" from the cutter fleet (e.g., periodic tightening of RTU connections).
- SFLC ensure a subject matter expert highly knowledgeable in ISCS architecture is readily available to assist the Contracting Officer's Technical Representative for all ISCS-related maintenance and supply contracts.
- SFLC/C4IT SC dedicate increased efforts to forward-looking supportability review tools, vice reacting to finding solutions once technology obsolescence or non-supportability by OEM becomes an issue.
- SFLC implement more granular configuration control methods, such as serial number tracking for repairable components (e.g., circuit cards).
- CG-9/CG-4/CG-6 improve transition from acquisition activities to lifecycle support activities for new assets to ensure sustainable regimes are in place to support systems with comparatively short technology refresh cycles.
- CG-1 benchmark mishap reporting system and infrastructure against organizations with particularly high-performing safety programs to identify potential improvements to the USCG surface vessel mishap reporting system.
- CG-4/CG-6/CG-1 formalize and codify standardized interface testing and evaluation requirements and procedures for cutter navigation control system updates, as well as other major shipboard systems.

DCO Organization:

- Emphasize the importance of re-evaluating operational risk management for an evolution in the event of significant changes in environment, equipment, or personnel.
- Work with DCMS to evaluate ability to budget/program for major safety-related as soon as possible, rather than programming their completion as part of larger out-year maintenance packages strictly out of convenience and economic decisions.
- Proactively encourage and facilitate information sharing forums among cutter operators, operational commanders, and support organizations where operational capabilities and safety are concerned.

Other:

- Formally charter the Tri-Partite and define the group's composition, function, and decision-making authority.
- Set aside scheduled time during Tri-P meetings (e.g., bi-weekly or in one meeting per month) to present a summary of mishap trends.

Chapter 6 – Comparison of *Elm* CAST and RCFA Results

"The only people who see the whole picture are the ones who step outside the frame."

- Salman Rushdie (from the novel *The Ground Beneath Her Feet)*

6.1 Chapter Overview

This chapter presents a comparison of the CAST completed in Chapter 5 with a Root Cause Failure Analysis (RCFA) that was contracted by the U.S. Coast Guard's Surface Forces Logistics Center (SFLC) to examine the same incident. The RCFA process is first described in the context of the SFLC's accident investigation procedures. The findings of the RCFA are presented and the assertions made in the RCFA's concluding statement are isolated and compared to the recommendations produced by the CAST. The significant contrasts between the recommendations of the two analyses are discussed in detail.

6.2 RCFA Overview

Following *USCGC Elm's* mishap involving loss of MPCMS control in August 2013, the SFLC initiated a root cause failure analysis (RCFA) in accordance with procedures detailed in the SFLC Engineering Investigation Process Guide. The intent of this chapter is to compare and contrast the output generated by the RCFA and the CAST completed in Chapter 5.

The applicable SFLC process guide *defines* an RCFA as follows:

> An RCFA is a structured, reactive investigation process aimed at addressing the problem rather than addressing the symptoms of the problem. The method produces recommendations that address equipment or personnel performance gaps and the management system deficiencies that are identified as root causes. Implementation of approved recommendations decreases recurrent equipment failures. The organizational objective is to solve the problem once, rather than addressing apparent causes multiple times (i.e., each time the casualty occurs) [31].

Furthermore, the stated goals of an RCFA are to ensure safeguards are in place and are functional to prevent accidents, as well as to identify root causes of an accident and allow these factors to be prioritized and addressed/resolved accordingly.

The process guide also states that the *purpose* of an RCFA is as follows:

> The purpose of an RCFA is to identify and evaluate every causal factor for an engineering incident to determine the true root cause of the failure. Causal factors are equipment performance gaps or front line personnel performance gaps that caused an incident, allowed an incident to occur, or allowed the consequences of the incident to be more severe than they might have been [31].

Finally, the SFLC Engineering Investigation Process Guide describes the *intent* of an RCFA as follows:

> The intent of an RCFA is to identify performance gaps. A performance gap is not a failure to perform as designed or directed, but a failure to perform as *desired*. Each causal factor is analyzed to determine its root cause. Root causes are deficiencies of management systems that allow the causal factors to occur or exist [31].

It is not difficult to see some of the apparent similarities and differences between a CAST and an RCFA (at least as defined by the SFLC process guide). The RCFA, like the CAST, identifies causal factors that allowed an incident to occur and/or not be well mitigated. Unlike CAST, however, RCFA focuses on equipment performance and front line personnel; this is derived from the stated purpose of RCFA quoted above. The statement about identifying the "*true* root cause" from all the causal factors further emphasizes that there is one root cause and the others are somehow less accurate or real. The stated purpose of an RCFA alludes to a root *cause* (emphasis added to accentuate the non-plural nature of the word). The definition of RCFA that is provided indicates more similarities with CAST in that it references "management system deficiencies." However, the same definition then moves away from this oblique reference to system control structures (to use STAMP terminology) and then refers to RCFA's benefit in preventing equipment "failures." As explained in Chapter 3, STAMP is not designed to primarily identify equipment failures (e.g., an overheated pump motor bearing causing the pump to go off-line due to thermal overload of the motor). STAMP focuses on constraints (organized via control structures) and the potential violation thereof, as opposed to primarily emphasizing equipment failure (such as the pump motor example). The stated *intent* of an RCFA (quoted in the preceding paragraph) is closer to the spirit and structure of a CAST. The SFLC process guide's emphasis of the word "desired" in the statement of intent suggests the existence of process models (to use STAMP terminology again). Also, the reference to "management systems that allow the causal factors to occur or exist" is rather STAMP-like, although the RCFA process guide does not seem to directly contemplate that the "causal factors" could be dysfunctional or unsafe management systems (control structures, in STAMP parlance) themselves.

6.3 Summary of *USCGC Elm* RCFA Results

The *USCGC Elm* incident explored in this thesis did not meet the criteria (loss magnitude) necessary to trigger a more formal investigation via an Engineering Analysis Board (an investigative body that is established to use DoD HFACS criteria to determine causal and contributing factors behind a specific equipment casualty). However, given the potential for severe damage and/or injury that could have resulted from a loss of MPCMS control – particularly during buoy retrieval/placement operations, an RCFA was ordered. Due to human resource constraints among appropriately trained civil service employees, the RCFA was completed by a consultant on contract to SFLC for such purposes. The consultant had in-depth system specific knowledge of neither the MPCMS nor the ISCS as a whole, and he relied heavily on interviews conducted with technicians, crewmembers, and subject matter experts in formulating his recommendations. As a result, the RCFA consisted of little more than a compendium of the results of these interviews, and the facts and opinions stated therein by the interviewees strongly influenced the RCFA's final content and recommendations.

The summary of findings and recommendations of the *USCGC Elm* RCFA is reproduced in Table 6.1 in its entirety.

Finding	Causal Factor	Supporting Data	Recommendation
MPCMS boots properly only after CG DDS LAN is secured.	1. Physical message characteristics are impeding proper MPCMS function.	Experiment shows that system functions properly after CG DDS LAN is secured. Prior DPS incident exhibiting	Review function after installing opto-isolators. Determine whether securing CG

	2. Logical message characteristic are impeding proper MPCMS	similar behavior was resolved by conditioning the electrical signal.	DDS LAN is required after installation.
Timestamp messaging from ECDIS to MPCMS interferes with alarm function.	The message encoding may instigate.	Securing timestamp messaging after initial booting restores alarm function.	Secure timestamp messaging following a successful boot. Investigate with (DPS and MPCMS OEMs) to expand the PNTX message to include the date and time data along with the propulsion data. Initial discussions with both OEMs say this is possible. This should serve to reduce the communication load between both systems, and may improve MPCMS operation.
Other hosts on serial bus produce clean logs.	The equipment is not impacted by the erratic MPCMS behavior. Equipment does not appear to interface well with legacy equipment.	C4ITSC investigation data shows message distribution from MPCMS became erratic.	Review MPCMS messaging to observe how messages are impacted at serial interface.
MPCS boots to prior state.	Memory is not cleared when power is cycled due to persistence of computer memory.	Capacitance requires time to discharge its charge. Quick power cycles do not provide sufficient time to release the charge.	Wait three minutes when rebooting computers to allow sufficient time to clear memory. This requires both computers to be down at the same time. This may be a moot point if the other recommendations eliminate the need for routine rebooting of MPCMS.
CG DDS LAN installation coincides with beginning of MPCMS reliability degradation.	Physical interface may not be within tolerance.	Inspection using oscilloscope or other signal analysis equipment required.	There may be physical layer faults with the signals to the MPCMS causing slowdown.

Measurement of serial bus impedance indicates mismatched levels.	There may be insufficient impedance to prevent signal reflection.	Low impedance can result in signal reflection and excessive current.	Send cards to factory to determine whether UART has been damaged and retest with validated VME.

Table 6.1 – Summary of Findings and Recommendations from *USCGC Elm* RCFA [32]

The conclusion of the RCFA was as follows:

> The cause of the loss of MPCMS reliability appears to be due to system noise and message defects related to retrofit upgrades of legacy system equipment. MPCMS performance degradation symptoms were coincidental to the installation of the CG DDS LAN. WLM/WLB continues [sic] to experience DDS LAN malfunction. Performance reliability may be restored at a low cost by adding opto-isolators in the serial connection to the serial bus.
>
> Personnel failed to identify high risk situations that placed crew and vessel in danger. Addressing frontline personnel performance gaps should be a first priority in resolving this casualty [32].

6.4 Discussion of *USCGC Elm* RCFA Conclusions

To both thoroughly and succinctly compare the recommendations of the USCG's RCFA with the results of the CAST completed in Chapter 5, the RCFA conclusion is dissected into parts for analysis in the paragraphs that follow (emphasis is added to some words/phrases via underlining for illustrative purposes).

6.4.1 RCFA Assertion 1

"The cause of the loss of MPCMS reliability appears to be due to system noise and message defects related to retrofit upgrades of legacy system equipment [32]*."*

The RCFA conclusions immediately hone in on reliability. The differences and interactions between reliability and safety were discussed in Chapters 2 and 3. While the term "reliability" does not appear to be inappropriately used in the RCFA conclusion, its mere presence in the opening sentence of the conclusion immediately colors the entire matter as an MPCMS reliability issue. At the component level, reliability concerns are certainly valid; the MPCMS main computer circuit cards appear to have been experiencing failures at a greater rate in recent years based on cutter casualty report data (summarized in Chapter 5). However, an executive looking for a concise summary of the *Elm's* incident and the larger MPCMS/ISCS affair would likely walk away from reading the opening sentence of the RCFA's conclusion with the clear mental model that the underlying issue is one of subsystem reliability. The second part of the conclusion's first sentence agrees with one of the key findings of the CAST. While the RCFA specifically refers to "system noise and message defects related to retrofit upgrades of legacy system equipment," this can be effectively summarized in two words: asynchronous evolution. As subsystems evolved separately and were re-integrated into the ISCS, the frequency of larger systematic functional issues increased.

6.4.2 RCFA Assertion 2

"MPCMS performance degradation symptoms were coincidental to the installation of the CG DDS LAN. WLM/WLB continues [sic] to experience DDS LAN malfunction. Performance reliability may be restored at a low cost by adding opto-isolators in the serial connection to the serial bus [32]*."*

The RCFA interestingly singles out the installation of the CG DDS (which replaced the SAFEnet LAN that was installed on the WLBs when they were delivered from the shipbuilder) as being "coincidental" to the degradation in ISCS performance (although MPCMS is specifically referred to in the text). Taken at face value, this appears to mean that MPCMS/ISCS exhibited degraded performance at the same time as the CG DDS installation. The reader is left to make his or her own deductions from this statement. Given the amount of controversy arising from the two "camps" (SFLC and C4IT SC technicians) at the time this analysis was conducted, one may infer that the language regarding a "coincidence" was not intended to be completely benign. The RCFA was contracted by SFLC and conducted by an individual with long and continuing business ties to the SFLC and its precursor organization. While multiple sources were interviewed by the contractor, the majority of attention was given to facts and opinions presented by SFLC subject matter experts. Chapter 5 discussed the suspicion/mistrust these individuals (MPCMS experts) harbored for the CG DDS (a C4IT SC supported system). It may be reasonably hypothesized that these circumstances affected the slant of the RCFA.

Additionally, the RCFA conclusion very directly states that the WLBs (and WLMs) continue to experience CG DDS malfunctions. This assertion prompted a very understandable "shields up" reaction from C4IT SC personnel. In fact, the responsible C4IT SC Division Chief provided a thorough rebuttal document in response to the SFLC's RCFA. The document (actually PowerPoint presentation slides) opens with the statement: "The (SFLC's) Root Cause Failure Analysis alleges CG DDS caused these MPCMS failures…[33]." Use of the word "alleges" clearly suggests both defensiveness and lack of agreement with the RCFA's conclusions. The rebuttal proceeds to state:

> This presentation will address each RCFA issue and prove that:
>
> - There is no correlation between fielding of CG DDS and the onset of MPCMS failures
> - There are no signal integrity issues on the serial cable between CG DDS and MPCMS
> - MPCMS software and hardware reliability issues must be addressed as specific isolated system issues [33]

The C4IT SC's response to the SFLC's RCFA goes into technical depth regarding analysis of computer logs and error messages, before concluding with the following bullet points:

- MPCMS issues do not correlate with CG DDS installation.
- There are no CG DDS signal integrity or grounding issues.
- CASREPS (Casualty Reports) point to an MPCMS hardware failure as root cause of issue.
- MPCMS reliability issues must to [sic] addressed as isolated system issue.
- MPCMS system is a VME system based on a 20-year-old M68040 CPU that has been exposed to harsh conditions of heat, humidity, and vibration for over 15 years – degradation is unavoidable.
- MPCMS software issues must be debugged and resolved in C3CEN lab & verified before fielding [33].

The C4IT SC report was accompanied by a thorough analysis of system messaging data and provided suspected alternative causes for the issues observed on *Elm* and other cutters. In conclusion, the RCFA presented somewhat "biased reporting" of the facts, similar to a news media outlet seeking to protect partisan interests. As a result, the C4IT SC CG DDS experts were somewhat piqued by the RCFA's conclusions and were cautious regarding immediate further engagement with SFLC MPCMS experts. As described in the CAST detailed in Chapter 5, barriers existed to properly constructive dialogue between the two responsible USCG logistics/service centers at the technical expert level in both organizations. This amounted to a more overt manifestation of the misunderstanding and mistrust (for lack of a better term) that appears to have existed for some time between certain highly knowledgeable personnel in both organizations. Such a dynamic is clearly not ideal for constructive cooperation. The RCFA served to widen this rift between key individuals.

6.4.3 RCFA Assertion 3

"Personnel failed to identify high risk situations that placed crew and vessel in danger. Addressing frontline personnel performance gaps should be a first priority in resolving this casualty."

The second to last sentence of the RCFA's conclusion matches a clear outcome of the CAST. While *Elm's* Commanding Officer had "absolute" responsibility for the cutter and its assigned personnel per USCG regulations [34], several people from multiple organizations had the opportunity to identify risk mitigation measures that could have been taken on the day of the incident. However, it is even more important to think back in time *before* the incident occurred. Asynchronous system evolution had been occurring for some time; in fact, it took on step-function behavior when concurrent upgrades were made to the ship's radar, DGPS receiver, and CG ECDIS. While the upgrades that occurred on *Elm* in early August 2013 were in no way implicated as causal factors for the incident that occurred on August 16, they provide a case-in-point of asynchronous sensor evolution. Over the years, DPS was periodically updated and the CG DDS replaced the SAFEnet LAN – but the MPCMS remained essentially static. Exceptions to this were some engineering changes made to MPCMS main computer processor cards – changes that were made during OEM-completed card repairs and were apparently not communicated to USCG SFLC configuration management personnel.

The *Elm* RCFA's concluding sentence stands out in direct contrast to the intent of a CAST. In fact, it is almost stereotypical as an example of how many accident analyses end when using non-STAMP methods. It not only obliquely assigns blame to a group of individuals, but it specifically calls out *frontline personnel performance gaps*. As Chapter 3 described in detail, the "blame game" provides a tidy termination point for an accident analysis. More often than not, such blame trickles down to frontline personnel (Johnson's "jackass fallacy," mentioned in Chapter 2). However, no direct indication was gleaned from *Elm's* mishap report or follow-on interviews that indicated a reason to assign blame to specific personnel, frontline or other.

6.5 Factors Identified by the CAST Analysis That Are Not in the RCFA's Conclusions

The RCFA provides only information regarding the physical system and its computer controllers. Based on the sources that were used to provide the bulk of the information considered by the RCFA, the report was likely biased toward certain "root causes." The hierarchical control structure was not considered in the RCFA report. As a result, numerous areas ripe for improvement were not

identified, perhaps leaving the door open for similar incidents in the future. While these areas were discussed in detail in Sections 5.3.6.17, 5.3.7, and 5.3.8, a summary of topics addressed by the CAST but not by the RCFA is provided here.

The Conning Officer and Commanding Officer recognized poor (sluggish) system performance, but pushed on with the day's evolutions. This is not a criticism of *Elm's* command and crew – rather, the overall hierarchical control structure (on both the operational side and the support side) was not fully aware or appreciative of the extent of the issues manifested in the ISCS. This stemmed from a range of issues, including crew self-reliance, incomplete understanding of system integration issues, and priority conflicts for key technicians.

A major reorganization of the USCG's surface asset engineering support structure increased efficiencies in maintenance management and greatly improved the effectiveness and standardization of fleet maintenance procedures, processes, and configuration management. While a detailed discussion of this reorganization is beyond the scope of this thesis, there were some unanticipated negative side effects. The WLB platform had been conceived, built, and crewed with a particular ILSP structure in mind. When the structure of the organizations providing primary support for the ISCS fundamentally changed, matrixed support teams largely dissolved. This lack of dedicated engagement across support commands, coupled with insufficient support contracted to the OEM or a licensed service provider, put ISCS technical and maintenance management on a downward slope. This effect was exacerbated by tensions and differences of opinion that existed between key technical personnel assigned to different support commands.

Some incidents involving the WLB ISCS were reported via formal mishap reports (as was *Elm's* in August 2013). It appears that those mishaps were largely addressed in a one-by-one fashion. Since they were not formally examined as a group by appropriate mission support leadership until after *Elm's* August 2013 incident, appropriate resources were not redirected earlier.

None of these factors involving the hierarchical control structure were addressed by the RCFA report.

6.6 Chapter Summary

The RCFA performed in the wake of *Elm's* incident shares some common ground with the CAST performed in Chapter 5. However, the greater hierarchical control structure is completely ignored by the RCFA, as may be reasonably expected given the RCFA analysis process. The comparison presented in this chapter clearly exhibits that CAST provides more complete recommendations for system improvement by enhancing controls and processes, while the RCFA largely focuses on component and subsystem failure.

Chapter 7 – STPA of WLB ISCS

"An ounce of prevention is worth a pound of cure."

"A stitch, in time, saves nine."

-Benjamin Franklin

7.1 Chapter Overview

This chapter examines the WLB ISCS by using the STPA hazard analysis technique. Potential accidents involving the WLB are considered, and hazards are determined and mapped to the accidents. Safety constraints for the system are then generated. Potential causal scenarios that can lead to the hazards are identified and design recommendations can be generated to prevent the scenarios. The functional control system is described, both at a high level and at the subsystem level.

In STPA Step 1, a table of unsafe control actions (UCAs) is created for both DPS modes of operation (Joystick/DP and Autopilot). Three of the most frequently used DPS commands are considered to build the UCAs – "hold heading," "hold position," and "high speed track follow." After determining UCAs and related safety constraints, an STPA Step 2 analysis is completed by constructing plausible scenarios that could lead to the identified UCAs. Finally, system requirements and design recommendations are suggested to prevent scenarios from cascading into accidents by mitigating the potentially hazardous nature of the UCAs.

7.2 System Accidents, Hazards, and High-Level Safety Constraints

Now that we have explored an actual near-miss incident involving the WLB ISCS, we have a better understanding of the dynamics exerted on the system operation by the broader high-level control structure. A number of recommendations emerged from the *USCGC Elm* CAST. Greater clarity was gained regarding unsafe control actions and process model flaws as they pertained to *Elm's* bad day. This chapter will apply STPA to look not at a particular *incident*, but at the ISCS itself as a *system*.

In the 12 months following *Elm's* incident, senior USCG leadership decided to pursue a partial system recapitalization of the MPCMS – specifically, a recapitalization of the MPMCS computers, upgrading them from Versa Module Europa computers to state-of-the-market industrial computers. In concert with the hardware updates, programmers changed the software from the original Ada code to the C++ programming language. Furthermore, the contract awarded for the partial system recapitalization stipulated that the USCG would have ownership of the software code for the purpose of making future improvements and/or upgrades. The requirements for this acquisition were relatively hastily written, and the contract was awarded to the MPCMS OEM (or, rather, the company that had acquired the OEM since original WLB delivery). This decision was made following considerable technical analysis; the MPCMS was identified as the weakest link in the system and the one from which the most problems (including component obsolescence and lack of supportability) were emanating. There was also a tremendous sense of urgency to increase the safety of the hardware/software – in which supportability plays a role – as soon as possible and within a limited budget.

Prior to embarking on an STPA, the analyst must decide what accidents/loss events to consider in the analysis. Chapter 2 of this thesis presented Leveson's definition of "accident": "an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss [6]." In the case of the WLB ISCS, the basic set of accidents evaluated are defined as follows:

A1: Cutter collides with another vessel

A2: Cutter strikes stationary object (e.g., pier, bridge)

A3: Personnel on cutter buoy deck are injured by buoy or related apparatus (buoy chain, sinker) during buoy servicing operations

A4: Cutter runs aground (e.g., on rocks, shoals)

These accidents are all potentially harmful to either the cutter, some portion of the crew, or both. It is these accidents that the STPA will seek to find ways to prevent.

As with other hazard analyses discussed earlier in this thesis, the basis for analyzing a system for safety is identifying hazards. Again, a hazard is defined as "a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident [6]." It is worth noting that the hazards considered in STPA should be within the boundaries of the system considered. For instance, submerged rocks or a sudden squall are not considered hazards to the WLB in this analysis, as the builders, maintainers, and operators of the WLBs have no control over where the rocks are located or what the weather may bring. In these cases, however, the hazards may be the cutter approaching too close to the rocks or servicing a buoy in an elevated sea state.

A hazard should be expressed as a statement regarding the entire system, rather than one component [35]. For example, "Failure of the primary and secondary MPCMS computers" is not considered a hazard. This is a statement regarding a subsystem – the MPCMS. Furthermore, what is meant by "failure?" This word introduces a level of vagueness that can and should be avoided in the analysis. A clearer statement would be: "the secondary MPCMS computer did not resume controlling propulsion machinery after the primary MPCMS computer went off line." This statement is clear and to the point; it expresses exactly what did and did not happen in terms that may be further analyzed. However, this statement should be further abstracted to become a statement of hazard. For example, such as statement could be: "cutter's propulsion machinery is not controlled by human or computer."

With this level of abstraction, it becomes apparent that the number of hazards will likely be fewer than one would originally think. In fact, Leveson states that the high-level (system) hazards identified for a system should number fewer than ten. Too high a number becomes overwhelming for the human brain to determine whether the list is complete or redundant. The high-level system hazards will be refined during the analysis using a tree-like structure to facilitate traceability to the detailed analysis. Top-level hazards identified for the WLB ISCS are as follows (with traceability to potential accidents shown within square brackets):

H1: Cutter does not maintain safe distance[1] from other ships [A1]

H2: Cutter does not maintain safe distance from stationary object (e.g., pier, bridge) [A2]

H3: Cutter maneuvering enters uncontrolled state while servicing a buoy [A1, A2, A3, A4]

H4: Cutter does not maintain safe distance from shoals [A4]

[1] The term "safe distance" is somewhat situationally subjective. It takes into account factors such as prevailing weather, sea state, current, visibility, time of day, crew selection, crew fatigue, and density, type, and proximity of vessel traffic.

Upon identification of hazards, system-level safety design constraints may be imposed to ensure the system "steers clear" of any hazards. In this case, the high level system safety constraints (mapped to their corresponding hazards) are as follows:

SC1: Cutter must maintain safe distance from other ships (H.1)

SC2: Cutter must maintain safe distance from stationary objects (H.2)

SC3: Cutter propulsion systems must be positively controlled while servicing buoys (H.3)

SC4: Cutter must maintain safe distance from shoals (H.4)

These are, of course, not particularly useful by themselves, but they serve as a starting point for the refinement steps to identify how these constraints could be violated.

7.3 Functional Control Structure

Figure 7.1 presents a high-level functional control structure diagram of the WLB. Within each primary system entity (human controller, automated controller, controlled process), the critical mission related functions are listed at a high level. Additionally, the necessary process models held by each controller are listed.

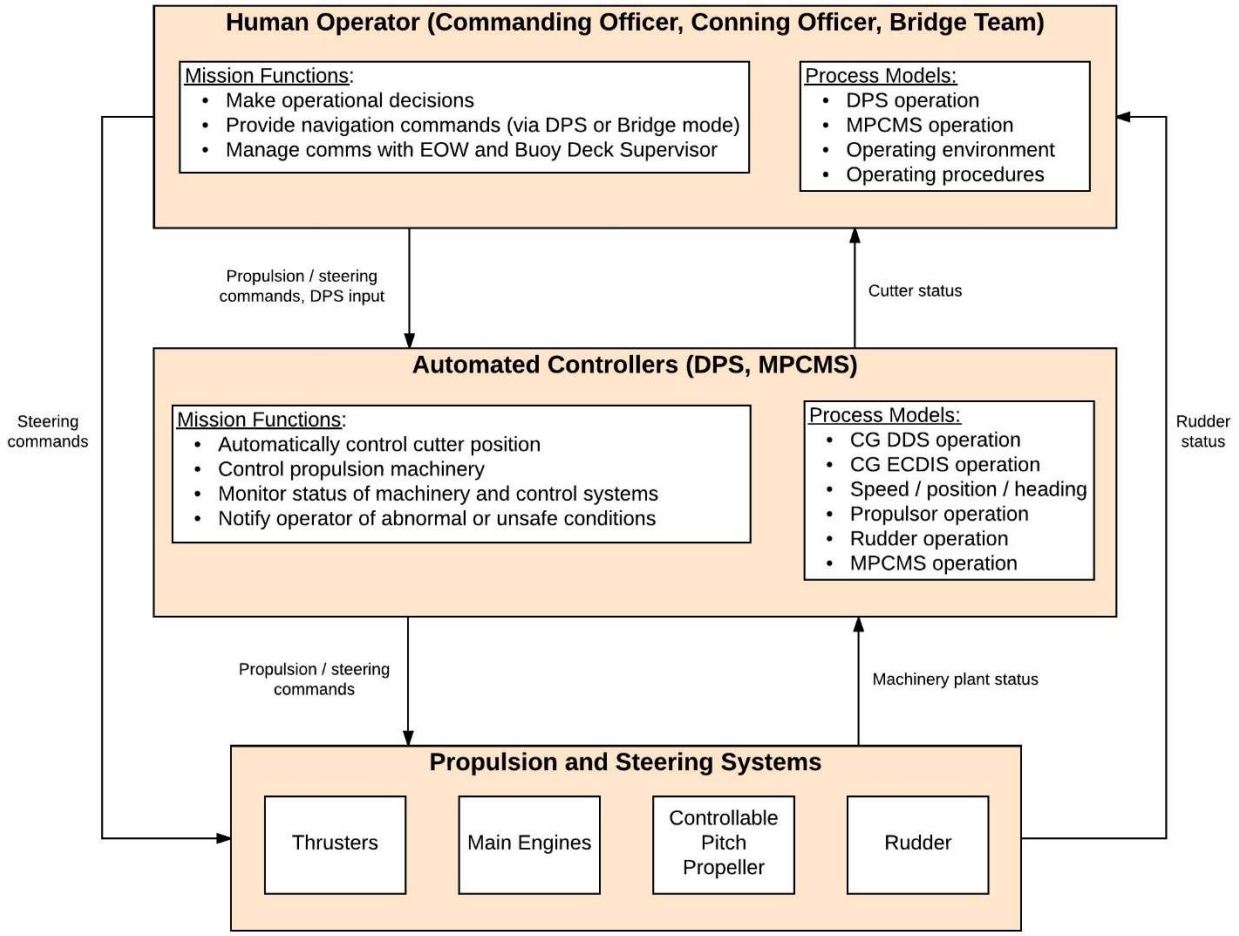


Figure 7.1 – WLB High-Level Functional Control Structure

Figure 7.2 is a more detailed functional control structure. In this figure, one is able to see that propulsion systems are controlled and monitored through the MPCMS, whereas steering is directly controlled by the Conning Officer or the DPS, depending on the mode selected. Both Bridge mode and DPS modes of operation are depicted in this diagram.

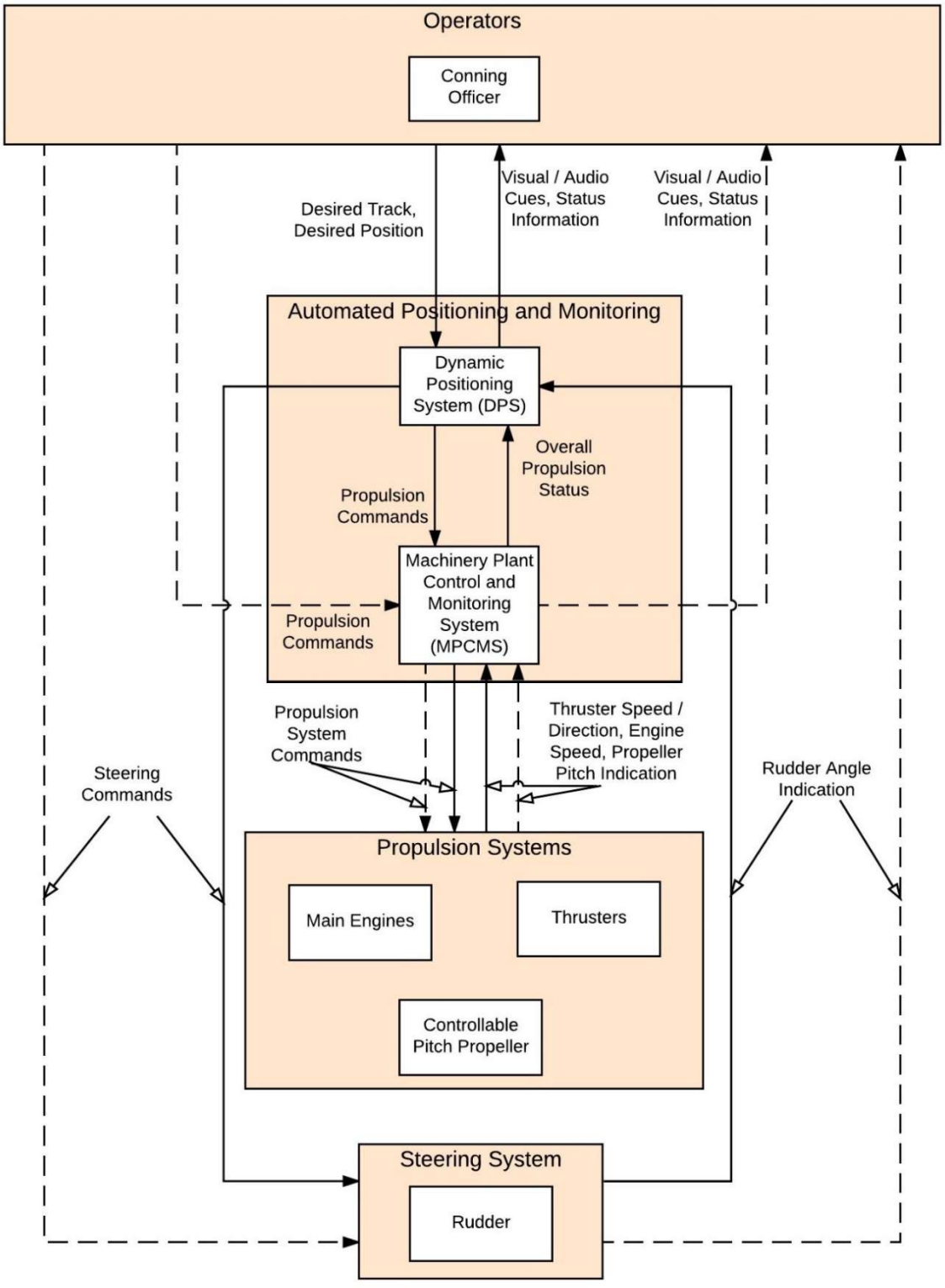


Figure 7.2 – WLB Functional Control Structure

7.4 STPA Step 1

Once potential accidents, hazards, and high level safety constraints have been identified and the control structure model created, the first step in conducting STPA is to assess the system's safety controls to determine the potential for inadequate control in particular contexts, thus enabling the presence of a hazard. This is best catalogued in a tabular format, with each identified control action evaluated with respect to each of the four potential causes of inadequate control that were described in Section 3.3.2 (i.e., not providing causes hazard, providing causes hazard, wrong timing or sequence causes hazard, and stopped too soon or applied too long causes hazard).

The formulation of unsafe control actions is important in conducting a rigorous analysis. Best practice dictates that an unsafe control action should begin by naming a source controller, the type (whether the control action was (or was not) provided), the control action that was provided (or is missing), and the context (system or environmental state) in which the command was (or was not) provided. To illustrate this construct, an unsafe control action for a circuit breaker controller is shown in Figure 7.3.

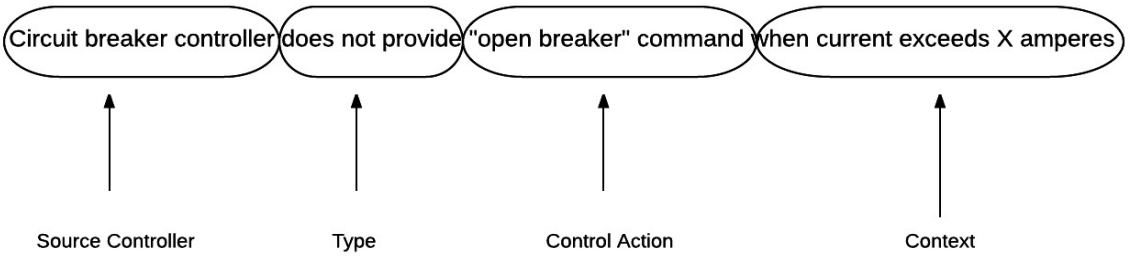


Figure 7.3 – Formulation of Unsafe Control Action – Circuit Breaker Controller Example

Use of this standard form ensures rigorous treatment of all identified states of the process models held by the controllers and controlled processes, and it assists the analyst in scenario development when completing STPA Step 2.

Additionally, traceability is provided for each unsafe control action, enabling the reader of the STPA to quickly ascertain which hazards are associated with each unsafe control action. This is similar to how hazards were traced to corresponding accidents in Section 7.2.

Finally, causal scenarios are created for each unsafe control action. These causal scenarios can be used to create system and component design requirements and recommendations.

As was described in Chapter 4, the cutter's propulsion and steering commands may be issued by a human operator (which we abstract to the Conning Officer in this analysis) or by the Dynamic Positioning System. For the purposes of this analysis, we will consider the cases when DPS operates under the following common commands: "high speed track follow," "hold position" and "hold heading." These modes were described in detail in Section 3.1.2.

Any human controller has a process model, and the Conning Officer is no different. Chapter 3 described how automated controllers maintain process models, as well, and this was depicted in the generic sense in Figure 3.4. In the case of the WLB ISCS, the process models are shown in Figure 7.1.

The controllers examined in this analysis are the Dynamic Positioning System and the Conning Officer. Identified Unsafe Control Actions (UCAs) are exhibited in Tables 7.1 – 7.3.

Dynamic Positioning System (DPS)				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide Propulsion Command to MPCMS	UCA-DPS-1: DPS does not provide propulsion command when cutter deviates by more than X meters from desired position while in "hold position" mode or when cutter deviates from desired heading by more than X degrees in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-2: DPS provides propulsion command when either insufficient thrust is produced to maintain station within X meters of desired position while in "hold position" mode or to maintain heading within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-3: DPS provides propulsion command more than X seconds after maneuver is required while in "hold position" mode or in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-4: DPS stops providing propulsion commands too soon before sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]
				UCA-DPS-5: DPS provides propulsion commands for too long after sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]

Table 7.1 – Unsafe Control Actions – DPS (Part 1)

Dynamic Positioning System (DPS)				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide Rudder Command to Steering System	UCA-DPS-6: DPS does not provide rudder command when cutter deviates more than X meters to the left or right of desired trackline or when cutter is within Y meters of calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-7: DPS provides rudder command when excessive or insufficient rudder force causes cutter to deviate more than X meters to the left or right of desired trackline or to overshoot/undershoot turn to join next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-8: DPS provides rudder command more than X seconds before or after reaching the calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-9: DPS stops providing rudder command too soon before sufficient maneuvering response is achieved to safely maintain ordered track or before sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]
				UCA-DPS-10: DPS provides rudder command for too long after sufficient maneuvering response is achieved for cutter to safely maintain ordered track or after sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]

Table 7.2 – Unsafe Control Actions – DPS (Part 2)

Conning Officer				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Transfer Propulsion and Steering Control from Bridge to DPS	UCA-Conn-1: Conning Officer does not shift propulsion control from Bridge to DPS while Commanding Officer and / or bridge team believe cutter propulsion was placed under DPS control [H1, H2, H3, H4]	UCA-Conn-2: Conning Officer shifts propulsion control from Bridge to DPS while Commanding Officer and / or bridge team believe cutter propulsion is still under Bridge control at MSCC [H1, H2, H4]		
Provide Hold Position or Hold Heading Command to DPS		UCA-Conn-3: Conning Officer provides "hold position" or "hold heading" command to DPS when chosen position or heading is unsafe [H1, H2, H4]	UCA-Conn-4: Buoy deck team begins servicing buoy before Conning Officer provides "hold position" and/or "hold heading" command [H3]	
Provide High Speed Track Follow Command to DPS		UCA-Conn-5: Conning Officer provides "high speed track follow" command to DPS when unsafe track is entered in CG ECDIS while cutter is controlled by DPS in Autopilot mode [H1, H2, H4]		
Transfer Propulsion and Steering Control from DPS to Bridge		UCA-Conn-6: Conning Officer transfers propulsion and steering control to Bridge mode while he/she has incorrect mental model of the operating environment [H1, H2, H4]	UCA-Conn-7: Conning Officer transfers propulsion control from DPS to Bridge mode before buoy servicing operation is complete [H3]	

Table 7.3 – Unsafe Control Actions – Conning Officer

The UCAs can be rewritten as safety constraints (with mapping to their corresponding UCAs in square brackets).

SC-DPS-1: DPS must provide necessary and sufficient propulsion commands for cutter to maintain position within X meters of desired position while in "hold position" or to maintain heading within Y degrees while in "hold heading." [UCA-DPS-1, UCA-DPS-2, UCA-DPS-4]

SC-DPS-2: DPS Must not provide propulsion command that will cause cutter to deviate more than X meters from desired position while in "hold position" mode or to maintain heading within Y degrees while in "hold heading" mode. [UCA-DPS-2]

SC-DPS-3: DPS must provide propulsion commands within X seconds of when maneuver is required (as determined by tolerance parameters programmed in DPS) while in either "hold position" or "hold heading" mode. [UCA-DPS-3]

SC-DPS-4: DPS must provide necessary and sufficient rudder commands for cutter to maintain course within X meters to the left or right of the desired trackline (as ordered via CG ECDIS) while in "high speed track follow" mode. [UCA-DPS-6, UCA-DPS-7, UCA-DPS-9]

SC-DPS-5: DPS must not provide rudder commands that will cause cutter to deviate more than X meters to the left or right of the desired trackline (as ordered via CG ECDIS) while in "high speed track follow" mode. [UCA-DPS-6, UCA-DPS-7, UCA-DPS-9]

SC-DPS-6: DPS must provide necessary and sufficient rudder commands for cutter to navigate from the current trackline to the next trackline (as ordered via CG ECDIS) while in "high speed track follow" mode. [UCA-DPS-6, UCA-DPS-7, UCA-DPS-9]

SC-DPS-7: DPS must provide computed rudder command for turn to navigate to next trackline (as ordered via CG ECDIS) within X seconds of reaching calculated starting point of turn. [UCA-DPS-8]

SC-Conn-1: Conning Officer must ensure awareness of Commanding Officer and Bridge Team of every shift in propulsion control between Bridge and DPS mode. [UCA-Conn-1, UCA-Conn-2, UCA-Conn-6, UCA-Conn-7]

SC-Conn-2: Conning Officer must not provide "hold position" command to DPS when cutter is in an unsafe position or "hold heading" command to DPS when cutter is at an unsafe heading. [UCA-Conn-3]

SC-Conn-3: Conning Officer must provide "hold position" and/or "hold heading" command before buoy deck team begins servicing buoy, as briefed to Commanding Officer prior to the evolution. [UCA-Conn-4]

SC-Conn-4: Conning Officer must not provide "high speed track follow" command to DPS when unsafe track is entered in CG ECDIS while cutter is controlled by DPS in Autopilot mode. [UCA-Conn-5]

SC-Conn-5: Conning Officer must not transfer propulsion control from DPS to Bridge before buoy servicing operation is complete. [UCA-Conn-7]

SC-Conn-6: Conning Officer must not transfer propulsion and steering control to Bridge while he/she has an incorrect mental model of the operating environment. [UCA-Conn-6]

The safety constraints derived from the list of UCAs provide a refinement of the original high-level system safety constraints and trace them to specific system components. Further refinement of safety constraints is accomplished in STPA Step 2.

7.5 STPA Step 2

Once UCAs are identified, we proceed to build accident scenarios that identify ways in which the identified unsafe control actions could occur.

The method employed in generating Step 2 scenarios for this thesis was first explicitly suggested in detail by Dr. John Thomas [36]. It employs a methodical, iterative approach to explore potential scenarios that may lead to identified UCAs. In Thomas' approach, the basic control system is regarded as depicted in Figure 7.4.

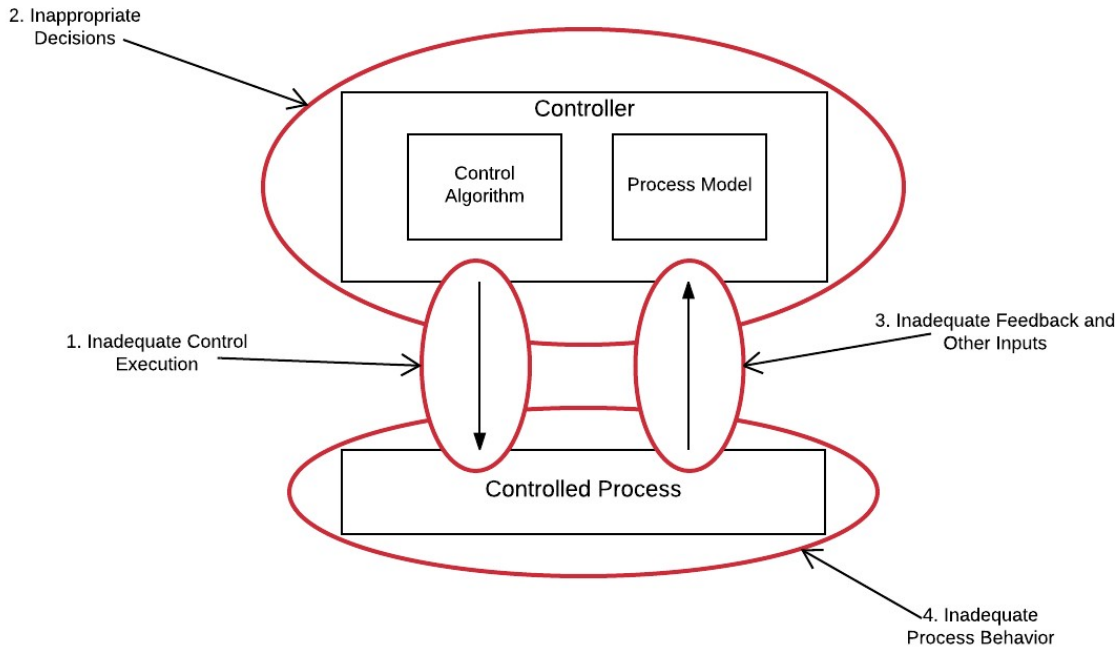


Figure 7.4 – The Four Categories of High-Level STPA Scenarios [36]

Starting on the left of Figure 7.4 and moving clockwise, the various geneses of scenarios are identified in four categories, or types – each of which is examined in detail for each UCA. The types are:

1) Inadequate control execution (command is provided by controller but not acted upon)

2) Inappropriate decisions by controller (inappropriate is command provided by controller despite controller receiving correct and adequate feedback/input)

3) Inadequate feedback and other inputs to controller (incorrect or incomplete input is provided to controller, resulting in controller providing inappropriate command)

4) Inadequate process behavior exhibited by controlled process (correct command is received from controller but not correctly followed by controlled process)

Separate analysis of each of these areas of the control loop provides sufficient information to develop high-level scenarios of each type by asking "why?" when considering each one. Once high-level scenarios of each type are identified, as applicable, a second iteration is performed. In this second iteration, the analyst again asks "why?" If more refinement is necessary, additional iterations may be

employed. Finally, system design requirements are suggested to institute controls that will prevent scenarios from leading to hazards.

For example, if a controller receives correct feedback yet makes an inappropriate decision (Type 2), we may ask: "Why could an inappropriate decision be made by the controller with correct feedback available to it?" One reason could be that the controller has an incorrect process model of the controlled process despite the feedback. On the second iteration, we ask: "Why could the controller's process model be incorrect?" A possible reason is that conflicting (and incorrect) feedback was received from another sensor that overrode the correct feedback that was initially received – perhaps due to the controller being programmed to not provide a command in the event of conflicting process feedback. But why was conflicting feedback received? A third iteration may reveal that the second sensor (which delivered incorrect and conflicting feedback) suffered from an internal malfunction or was exposed to a powerful electromagnetic field that altered its signal during transmission. Possible requirements yielded by this analysis may include reduction of data cable exposure to electromagnetic fields or an alarm/notification in the event of conflicting sensor feedback.

The next two subsections provide excerpts of the output of this Step 2 analysis. The complete generated scenarios are contained the Appendix.

7.5.1 Sample DPS Scenarios

Listed below are Scenarios for UCA-DPS-1 through UPS-DPS-4, which involve interaction between the DPS (controller) and the propulsion systems (controlled processes). The control action considered is "provide propulsion command to MPCMS."

UCA-DPS-1: DPS does not provide propulsion command when cutter deviates by more than X meters from desired position while in "hold position" mode or when cutter deviates from desired heading by more than X degrees in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-1.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading and the DPS does not provide a propulsion command to the MPCMS because the DPS has a flawed process model. This could be caused by:

A. Incorrect or missing sensor information (e.g., from DGPS, Doppler speed log, gyrocompass, meteorological sensor, CG ECDIS, or pitch/roll/yaw sensors) is received at DPS.
B. Inappropriate DGPS reference station is selected by crew technician, resulting in degraded ability to precisely position the cutter.
C. DPS believes required propulsion machinery configuration and sensor availability for DP mode is not satisfied due to unavailable feedback from main diesel engines (MDEs), controllable pitch propeller (CPP), thruster generator, or thrusters, causing DPS to exit DP mode

Possible Requirements for Scenario DPS-1.1:

1. Visual and audible alarm shall annunciate on bridge when DGPS, gyrocompass, Doppler speed log, meteorological sensor, or pitch/roll/yaw sensor input is not received within X seconds of last input.
2. DPS shall identify when sensor messages are incomplete or corrupted and notify user when such messages are received.

3. DPS shall filter out any incomplete or corrupt data strings when making maneuvering calculations.
4. The Commanding Officer's permission shall be obtained prior to using DPS in the absence of active DGPS input (i.e., if DGPS switches to operate in "dead reckoning" mode due to insufficiently precise position determination).
5. DPS shall receive consistent status feedback from MDEs, thruster generator, and thrusters; visual and audible alarm shall annunciate on bridge and in ECC when signal is not received within X seconds of last signal from each propulsor.

Scenario DPS-1.2: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but this command is either not relayed by the MPCMS or not acted on by one or more propulsion systems. This could be caused by:

A. Both MPCMS and/or both computers are offline (e.g., due to failures in both computers, combined failure of normal electrical power and UPS, or malware attack)
B. Improper reformatting of command by MPCMS for delivery via TANOnet (e.g., caused by software bug, malware, or incompatible interface between software versions)
C. Component failure in RTU or propulsor/actuator, or intermittent/broken electrical connection in control loop.

Possible Requirements for Scenario DPS-1.2:

1. Visual and audible alarm shall annunciate on bridge when MPCMS or DDS computer goes offline or when a UPS or DC power supply is not properly functioning.
2. Access procedures and active scanning shall be implemented to protect MPCMS computers from malware; this shall include credential verification and internal logging of all maintenance personnel accessing computers/network.
3. DPS shall be capable of detecting unauthorized system access and shall not operate after such access until an authorized technician completes a thorough and satisfactory malware scan and system diagnostic check.
4. Visual and audible alarm shall annunciate in ECC if poor or intermittent connectivity is detected to/from RTU card or actuator.
5. Maintenance procedure shall be implemented for technicians to check and adjust (as necessary) RTU connections every X weeks.

UCA-DPS-2: DPS provides propulsion command when either insufficient or excessive thrust is produced to maintain station within X meters of desired position while in "hold position" mode or to maintain heading within X degrees of desired heading while in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-2.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but the command is either not sufficient to regain the desired position/heading or it results in overshoot of the desired position/heading. This could be caused by:

A. DPS inappropriately processes sensor feedback leading to undesired command due to sensor message format that is not fully compatible with DPS.
B. The Conning Officer desires unnecessarily precise DPS control of position/heading and selects improper DPS gain settings, resulting in system overreaction to environmental factors and frequent overshoot of cutter response.
C. Limitations (e.g., max rpm, max pitch) are imposed on propulsors by technician (e.g., propulsor placed in local control mode for troubleshooting/maintenance) without notification to bridge personnel.
D. A portion of the thruster allocation logic is incorrect due to bug in software update.
E. Propulsor response is limited due to component failure, clogged fuel filters, etc.

Possible Requirements for Scenario DPS-2.1:

1. Thorough integration review and testing shall be accomplished prior to fielding upgrades to any sensors that transmit to DPS.
2. Current gain settings shall be prominently shown on DPS display.
3. The Commanding Officer's permission shall be required to adjust DPS gain settings.
4. No propulsor shall be in local control while propulsion control resides with DPS.
5. DPS shall be automatically notified when propulsor is unable to respond as ordered.
6. Any DPS software update must be thoroughly tested in all modes at the LBSF prior to introduction to the fleet.
7. DPS shall provide the operator with feedback if programmed thruster allocation logic or MDE load sharing algorithms are preventing execution of commanded maneuver.
8. DPS shall update the thruster allocation logic and MPCMS shall be instructed to modify MDE load sharing if a thruster or MDE/CPP, respectively, exhibits inadequate response to provided command.
9. Visual and audible alarm shall annunciate on bridge and in ECC if any propulsor's response becomes inadequate to the point that DPS and MPCMS cannot effectively and safely modify thruster allocation logic or MDE load sharing.

UCA-DPS-3: DPS provides propulsion command more than X seconds after maneuver is required while in "hold position" mode or in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-3.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but the command provides the ordered thrust more than X seconds after maneuver is required. The delay in propulsor action to change the cutter's position/heading results in the DPS sending additional (redundant) commands to the MPCMS. When the commands are ultimately carried out by the propulsors, the result is overshoot of desired maneuver to maintain position and/or heading. This could be caused by:

A. An abnormally high level of traffic is traveling over CG DDS (e.g., due to high amount / frequency of traffic generated by sensors and DPS or spurious signals), thus resulting in temporary storage of DPS commands in CG DDS memory buffer and latency of DPS command receipt at MPCMS.
B. MPCMS does not re-format and transmit DPS command to the appropriate RTU(s) within X seconds of command receipt.

Possible Requirements for Scenario DPS-3.1:

1. DPS shall affix a “time stamp” to each outgoing command.
2. MPCMS shall read each incoming command's time stamp and compare the time of command issue to time received to determine latency in CG DDS.
3. Visual and audible alarm shall annunciate on bridge when CG DDS reaches X% of capacity or when command latency from DPS to MPCMS exceeds X seconds.
4. *Alternatively to 1-3, above:* DPS shall communicate directly with the MPCMS and not use the CG DDS (used by numerous other sensors).
5. MPCMS shall affix a time stamp to each outgoing command.
6. MPCMS shall compare the time stamp of each outgoing command (sent to RTU) to the corresponding incoming DPS command to determine MPCMS computer latency.
7. Visual and audible alarm shall annunciate on bridge and in ECC when MPCMS computer latency exceeds X seconds.

UCA-DPS-4: DPS stops providing propulsion commands too soon before sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within X degrees of desired heading while in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-4.1: The cutter’s steering and propulsion are operating under DPS control and in DP mode and “hold heading” and “hold position” commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides propulsion commands to the MPCMS, but the commands stop before sufficient commands are received and acted upon to keep the cutter within X meters of the desired position or within X degrees of the desired heading. This could be caused by:

A. DPS receives conflicting position feedback between CG ECDIS and the DGPS signal that is fed directly to DPS.
B. DPS receives incorrect feedback regarding cutter position, heading, or speed from DGPS, gyrocompass, or Doppler speed log, respectively.
C. MPCMS receives incorrect feedback from thrusters or MDE and CPP indicating that more thrust is being provided than what is actually being provided.

Possible Requirements for Scenario DPS-4.1:

1. In the event of conflicting positional information at DPS between CG ECDIS input and direct DGPS signal, the direct DGPS signal shall be used for determining appropriate commands to MPCMS.
2. Gyrocompass error shall be determined daily and DPS process model shall be updated with current gyrocompass error any time it changes.
3. DPS shall periodically compare gyrocompass and fluxgate compass inputs to determine if they are diverging, and notify the operator if the divergence is more than the sum of known magnetic deviation, magnetic variation, and gyrocompass error.
4. ISCS shall have ability to compare, via modeling, propulsor feedback at MPCMS, command issued by DPS, external forces (e.g., wind, current), and actual movement of ship to determine when propulsor feedback is inaccurate; visual and audible alarm shall annunciate on bridge and in ECC when propulsor feedback to MPCMS differs by more than X% from model-generated output.

7.5.2 Sample Conning Officer Scenarios

Listed below are Scenarios for UCA-Conn-3 and UCS-Conn-4, which involve interaction between the Conning Officer (controller) and the propulsion systems (controlled processes). The control action considered is “provide hold position or hold heading command to DPS.”

UCA-Conn-3: Conning Officer provides "hold position" or "hold heading" command to DPS when chosen position or heading is unsafe. [H1, H2, H4]

Scenario Conn-3.1: The cutter is operating under DPS control and is receiving input from the Conning Officer via joystick controller while in DP mode while approaching a work site. The Conning Officer attempts to get the cutter to the desired heading and/or position via joystick controls, and then provides a “hold heading” and/or “hold position” command. However, the Conning Officer’s mental model is inaccurate and the chosen heading and/or position is/are unsafe due to proximity to shoals, proximity to vessel traffic, or proximity to a fixed object. This could be caused by:

A. Environmental conditions (e.g., wind, current, sea state) cause the Conning Officer to take a different approach than what was briefed prior to the evolution, resulting in him/her not conducting a through risk analysis.
B. The Conning Officer is unfamiliar with the area of operations, and he/she is not provided with sufficient oversight and coaching during the evolution.
C. The appropriate chart is not loaded into ECDIS.
D. The Conning Officer feels rushed to complete the evolution due to pressing operational tasking.
E. Sensors and bridge systems (e.g., DGPS, CG ECDIS, radar) do not provide adequate warning of unsafe position/heading
F. “Hold heading” command is transmitted to and acted upon by MPCMS but “hold position” is delayed in receipt due to latency in delivery to MPCMS by CG DDS (e.g., due to high amount / frequency of traffic on CG DDS generated by sensors and DPS or spurious signals).

Possible Requirements for Scenario Conn-3.1:

1. Operational risk assessments shall be conducted when environmental conditions differ significantly from what is expected or was previously briefed.
2. In areas of high vessel traffic or reduced visibility, an additional Deck Watch Officer shall be placed on watch to monitor and communicate with vessel traffic, allowing the Conning Officer to concentrate on maneuvering the cutter.
3. Use of the appropriate chart in CG ECDIS shall be verified prior to any evolution.
4. The Commanding Officer's permission shall be obtained prior to using DPS in the absence of active DGPS input (i.e., if DGPS switches to operate in "dead reckoning" mode due to insufficiently precise position determination).
5. The Commanding Officer's standing orders shall state that no underway evolution should be rushed, and that the Conning Officer shall contact the Commanding Officer if uncomfortable with an operational situation.
6. Visual and audible alarm shall annunciate on bridge when CG DDS reaches X% of capacity or when command latency from DPS to MPCMS exceeds X seconds.

UCA-Conn-4: Buoy deck team begins servicing buoy before the Conning Officer provides "hold position" and/or "hold heading" command. [H3]

Scenario Conn-4.1: The cutter is operating under DPS control and is receiving input from the Conning Officer via joystick controller while in DP mode while approaching a work site. The Conning Officer

attempts to get the cutter to the desired heading and/or position via joystick controls. The Buoy Deck Supervisor has a flawed mental model and believes the cutter is in “hold heading/hold position” mode, and orders the buoy servicing evolution to begin. This could be caused by:

A. The Conning Officer believes that prevailing weather, current, seas, and vessel traffic conditions are extremely mild and do not require use of DPS.
B. Malfunction of DPS results in the Conning Officer deciding to control maneuvers with joystick while DPS has control (i.e., “hold heading” and “hold position” modes not available).
C. Prevailing weather, current, and/or sea conditions are such that DPS is unable to adequately maintain cutter's position and/or heading in "hold position/hold heading" mode.
D. Inadequate communications are maintained between the Conning Officer and the Buoy Deck Supervisor

Possible Requirements for Scenario Conn-4.1:

1. The Commanding Officer's permission shall be obtained to conduct buoy servicing operations in Bridge mode or in DP mode without “hold heading” or “hold position” commanded, and this evolution shall be specifically briefed following established operational risk management procedures.
2. The Buoy Deck Supervisor shall not allow the buoy deck team to initiate buoy servicing evolution until order is received from the Conning Officer or Commanding Officer.
3. The Commanding Officer shall be notified if environmental conditions deteriorate to a point where “hold heading” and/or “hold position” commands are ineffective.
4. At least two effective operating modes of two-way communications shall exist between the Conning Officer and the Buoy Deck Supervisor at all times throughout a buoy servicing evolution.

7.6 STPA Recommendations

Upon initial completion of UCA identification, 40 independent UCAs were identified (26 associated with the DPS controller, 14 with the Conning Officer). These were then examined for similarity and several were subsequently combined to eliminate redundant analysis, where possible. For example, UCAs (and their subsequent draft scenarios) involving the Conning Officer providing a “hold position” command were very similar to scenarios where the Conning Officer provides a “hold heading” command. Such UCAs were consolidated to improve the usefulness and readability of the analysis. After this consolidation, 17 UCAs emerged (ten associated with the DPS controller, seven with the Conning Officer).

As shown in the preceding sections of this chapter, numerous causal factors were distinguished for each scenario presented, and system requirements were subsequently articulated to guard against the examined control actions becoming unsafe. A total of 92 distinct requirements emerged from the Step 2 analysis. These requirements comprise the recommendations of the STPA, and are fully detailed in the Appendix.

Chapter 8 – Conclusion

"Sunset and evening star
And one clear call for me!
And may there be no moaning of the bar,
When I put out to sea"

- Alfred, Lord Tennyson (from the poem *Crossing the Bar*)

A partial MPCMS system recapitalization commenced on the WLBs in 2015, representing a major change to the WLB ISCS. Feedback received in March 2017 from a current cutter commanding officer is that the upgraded MPCMS is "awesome" and is working with "no issues." While this is certainly heartening to hear, there will unquestionably be future system upgrades needed to improve supportability (e.g., obsolescence protection) and interoperability (e.g., to ward off negative effects of asynchronous development as other ISCS subsystems also evolve). Additionally, the TANOnet and RTUs were not modified as part of the recent WLB MPCMS upgrade. As the WLB ISCS evolves, maintaining cognizance of additional requirements such as those derived from the recommendations generated by the CAST and STPA performed in this thesis may help guide requirements generation for future upgrades.

More immediately, the 175' *Keeper* class WLMs share an ISCS architecture that is highly similar to that of the WLB ISCS that was examined in detail in this thesis. The primary differences between the two ISCSs are the WLM's use of azimuthing Z-drive propulsors (vice a linear shaft and rudder arrangement) and its configuration with a bow thruster only (vice both bow and stern thrusters). The WLM MPCMS OEM is the same as the manufacturer of the original WLB MPCMS, and the two MPCMSs use common components. The DPS, DGPS, CG ECDIS, CG DDS, and radar systems between the two cutter classes are identical. Some (yet undetermined) degree of recapitalization of the WLM MPCMS is on the near term horizon, and the USCG will do well to maintain a systems approach to safety in generating requirements.

Given this discussion, we now revisit the research questions that were posed in Chapter 1:

- Are STAMP methodologies appropriate for use to generate actionable recommendations and requirements for future control system upgrades onboard U.S. Coast Guard buoy tenders?

- Are STAMP methodologies appropriate for use to provide greater insights that may lead to safer controls in the greater hierarchical control structure for U.S. Coast Guard buoy tenders?

Based on the analysis completed in the preceding chapters, the answer to both questions is clearly "yes." Using a systems approach, potential requirements were identified for future control system upgrades (Chapter 7). Additionally, recommendations for improvements to organizational controls were identified (Chapter 5).

An area of future work identified by this thesis include further application of STAMP principles to USCG systems acquisition programs. When new cutters, aircraft, or IT systems are proposed, it may prove effective to incorporate system safety considerations beginning with the ORD and ending with life cycle support for delivered assets. The treatment of system safety in the USCG Major Systems Acquisition Manual and associated USCG and Department of Homeland Security policy documents and process guides may be examined for effectiveness.

Consideration of using STAMP methodologies in accident analyses may pay dividends in preventing future similar accidents. Chapter 6 exhibited the large amount of additional actionable information that may be garnered by conducting a CAST in additional to an RFCA, vice performing an RCFA in isolation.

Additionally, future work may be performed in the form of a STAMP-based analysis of USCG safety policies as well as tactics, techniques, and procedures. This would include a review of the USCG Safety and Environmental Health Manual and other official publications that provide specific guidance on subjects such as mishap reporting and operational risk management.

A final area that bridges both acquisition and safety policy is that of cybersecurity. As systems have become more complicated and complex in order to meet increasing requirements borne of evolving threats, computer controllers have proliferated in use throughout USCG surface, aircraft, and command, control, and communication systems. While some of the scenarios associated with UCAs described in Chapter 7 the Appendix touch on cybersecurity, this evolving front provides a developing frontier for further application of STAMP principles.

Bibliography

[1] American Association of Port Authorities, “America’s Ports Today,” 2008. [Online]. Available: http://aapa.files.cms-plus.com/PDFs/Americas_Ports_Today.pdf. [Accessed: 25-Jan-2017].

[2] W. Wheeler, “History of the Administration of Lighthouses in America,” 2016. [Online]. Available: http://uslhs.org/history-administration-lighthouses-america. [Accessed: 25-Jan-2017].

[3] T. Strobridge, “Chronology of Aids to Navigation and the United States Lighthouse Service 1716 - 1939,” 2016. [Online]. Available: https://www.uscg.mil/history/articles/h_uslhschron.asp. [Accessed: 25-Jan-2017].

[4] Volpe National Transportation Systems Center, “Overview of the U.S. Coast Guard Short Range Aids to Navigation Mission,” Cambridge, MA, 1993.

[5] J. Tozzi and H. Millan, *An Analysis of the Positioning Accuracy of Horizontal Sextant Angles,* Springfield, VA: U.S. Department of Commerce National Technical Information Service, 1974.

[6] N. Leveson, *Safeware*. Boston: Addison-Wesley, 1995.

[7] H. Heinrich, *Industrial Accident Prevention - A Scientific Approach*, Second Edition. New York: McGraw-Hill, 1942.

[8] J. Thomas, “Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis,” Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2013.

[9] G. Navarro, “Tesla Sued After Model X Crashes Into Living Room But Tesla Points To Possible Driver Error,” *Tech Times*, 2017. [Online]. Available: http://www.techtimes.com/articles/190932/20170101/tesla-sudden-acceleration-tesla-sued-after-model-x-crashes-into-living-room-but-tesla-points-to-possible-driver-error.htm. [Accessed: 25-Jan-2017].

[10] F. Bird and R. Loftus, *Loss Control Management*. Loganville, GA: Institute Press, 1976.

[11] J. Reason, *The Human Contribution: Unsafe Acts, Accidents, and Heroic Recoveries*. Burlington, VT: Ashgate, 2008.

[12] J. Reason, *Human Error*. Cambridge, UK: Cambridge University Press, 1990.

[13] P. Lewycky, “Notes Toward an Understanding of Accident Causes,” *Hazard Prevention*, vol. 7, no. March/April 1987, pp. 6–8, 1987.

[14] W. Vesely, *Fault Tree Handbook with Aerospace Applications*. Washington, DC: NASA, 2002.

[15] M. Rausand and A. Høyland, *System Reliability Theory*, 2nd Edition. Hoboken, NJ, 2004.

[16] W. Johnson, *MORT Safety Assurance Systems*. New York: Marcel Dekker, Inc., 1980.

[17] E. Rechtin, “What is Systems Engineering?” 2000. [Online]. Available: http://www.incose.org/AboutSE/WhatIsSE. [Accessed: 02-May-2017].

[18] J. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: McGraw-Hill, 2000.

[19] W. Ashby, “Principles of the Self-Organizing System,” in *Principles of Self-Organization*, G. Zopf and H. Von Foerster, Ed. New York: Pergamon, 1962, pp. 255–278.

[20] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: The MIT Press, 2011.

[21] J. Lederer, “How Far Have We Come? A Look Back at the Leading Edge of System Safety 18 Years Ago,” *Hazard Prevention*, May/June, pp. 8–10, 1986.

[22] G. Weinberg, *An Introduction to General Systems Thinking*. Hoboken, NJ: John Wiley and Sons, Inc., 1975.

[23] J. Leplat, “Occupational Accident Research and Systems Approach,” in *New Technology and Human Error*, J. Leplat, J. Rasmussen, and K. Duncan, Ed. New York: John Wiley and Sons, Inc., 1987, pp. 181–191.

[24] U.S. Coast Guard, “Seagoing Buoy Tender Replacement (WLB) Operational Requirements Document (ORD),” Washington, DC, 2000.

[25] U.S. Coast Guard, *U.S. Coast Guard Technical Publication 3505A: Machinery Plant Control and Monitoring Sysem Operating Manual - 225’ “A” Class WLB*. Baltimore: U.S. Coast Guard, 1998.

[26] U.S. Coast Guard, *U.S. Coast Guard Technical Publication 4925A: Dynamic Positioning System (Model NMS6000) - 225’ WLB (A) and (B) Class Cutters*. Baltimore, 2016.

[27] U.S. Coast Guard, *U.S. Coast Guard Technical Publication 3501: WLB 225’ Seagoing Buoy Tender Ship’s Information Book*. Baltimore: U.S. Coast Guard, 2000.

[28] U.S. Coast Guard, *U.S. Coast Guard Data Distribution System Technical Manual*, Version 1. Portsmouth, VA: U.S. Coast Guard 2010.

[29] M. Gimple, “Investigation of Allision of USCGC Willow (WLB 202) with Pier 2, Naval Station Newport, on 14 August 2009,” New London, CT, 2009.

[30] U.S. Coast Guard, “Seagoing Buoy Tender 225’ WLB Integrated Logistics Support Plan (ILSP),” Washington, DC, 2008.

[31] U.S. Coast Guard, *U.S. Coast Guard Surface Forces Logistics Center Process Guide CGTO PG-85-00-560-S: Engineering Investigation Process Guide*. Baltimore, 2012.

[32] ABS Consulting, “WLM/WLB MPCMS Casualties Root Cause Analysis,” Baltimore, 2013.

[33] H. Castro, *MPCMS Failures Root Cause Failure Analysis*, PowerPoint presentation, U.S. Coast Guard Command, Control, and Communications Center, Portsmouth, VA, 2013.

[34] U.S. Coast Guard, *U.S. Coast Guard Regulations (Commandant Instruction M5000.3B)*. Washington, DC, 1992.

[35] N. Leveson, “An STPA Primer,” *Version 1,* 2013 (updated 2015). [Online]. Available: http://sunnyday.mit.edu/STPA-Primer-v0.pdf.

[36] J. Thomas, N. Leveson, N. Ishimama, M. Katahira, N. Hoshino, and K. Kakimoto, “A Process for STPA - STAMP Accident Model of HITOMI and Expansion to Future Safety Culture,” in *MIT Partnership for a Systems Approach to Safety (PSAS) - 2017 STAMP Workshop*, 2017.

Appendix – Complete List of Generated UCA Scenarios

A.1 DPS Action: Provide Propulsion Command to MPCMS

Dynamic Positioning System (DPS)				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide Propulsion Command to MPCMS	UCA-DPS-1: DPS does not provide propulsion command when cutter deviates by more than X meters from desired position while in "hold position" mode or when cutter deviates from desired heading by more than X degrees in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-2: DPS provides propulsion command when either insufficient thrust is produced to maintain station within X meters of desired position while in "hold position" mode or to maintain heading within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-3: DPS provides propulsion command more than X seconds after maneuver is required while in "hold position" mode or in "hold heading" mode [H1, H2, H3, H4]	UCA-DPS-4: DPS stops providing propulsion commands too soon before sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]
				UCA-DPS-5: DPS provides propulsion commands for too long after sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within Y degrees of desired heading while in "hold heading" mode [H1, H2, H3, H4]

UCA-DPS-1: DPS does not provide propulsion command when cutter deviates by more than X meters from desired position while in "hold position" mode or when cutter deviates from desired heading by more than X degrees in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-1.1: The cutter's steering and propulsion is operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the

ordered heading and the DPS does not provide a propulsion command to the MPCMS because the DPS has a flawed process model. This could be caused by:

D. Incorrect or missing sensor information (e.g., from DGPS, Doppler speed log, gyrocompass, meteorological sensor, CG ECDIS, or pitch/roll/yaw sensors) is received at DPS.
E. Inappropriate DGPS reference station is selected by crew technician, resulting in degraded ability to precisely position the cutter.
F. DPS believes required propulsion machinery configuration and sensor availability for DP mode is not satisfied due to unavailable feedback from main diesel engines (MDEs), controllable pitch propeller (CPP), thruster generator, or thrusters, causing DPS to exit DP mode

Possible Requirements for Scenario DPS-1.1:

6. Visual and audible alarm shall annunciate on bridge when DGPS, gyrocompass, Doppler speed log, meteorological sensor, or pitch/roll/yaw sensor input is not received within X seconds of last input.
7. DPS shall identify when sensor messages are incomplete or corrupted and notify user when such messages are received.
8. DPS shall filter out any incomplete or corrupt data strings when making maneuvering calculations.
9. The Commanding Officer's permission shall be obtained prior to using DPS in the absence of active DGPS input (i.e., if DGPS switches to operate in "dead reckoning" mode due to insufficiently precise position determination).
10. DPS shall receive consistent status feedback from MDEs, thruster generator, and thrusters; visual and audible alarm shall annunciate on bridge and in ECC when signal is not received within X seconds of last signal from each propulsor.

Scenario DPS-1.2: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but this command is either not relayed by the MPCMS or not acted on by one or more propulsion systems. This could be caused by:

D. Both MPCMS and/or both computers are offline (e.g., due to failures in both computers, combined failure of normal electrical power and UPS, or malware attack)
E. Improper reformatting of command by MPCMS for delivery via TANOnet (e.g., caused by software bug, malware, or incompatible interface between software versions)
F. Component failure in RTU or propulsor/actuator, or intermittent/broken electrical connection in control loop.

Possible Requirements for Scenario DPS-1.2:

6. Visual and audible alarm shall annunciate on bridge when MPCMS or DDS computer goes offline or when a UPS or DC power supply is not properly functioning.

7. Access procedures and active scanning shall be implemented to protect MPCMS computers from malware; this shall include credential verification and internal logging of all maintenance personnel accessing computers/network.
8. DPS shall be capable of detecting unauthorized system access and shall not operate after such access until an authorized technician completes a thorough and satisfactory malware scan and system diagnostic check.
9. Visual and audible alarm shall annunciate in ECC if poor or intermittent connectivity is detected to/from RTU card or actuator.
10. Maintenance procedure shall be implemented for technicians to check and adjust (as necessary) RTU connections every X weeks.

UCA-DPS-2: DPS provides propulsion command when either insufficient or excessive thrust is produced to maintain station within X meters of desired position while in "hold position" mode or to maintain heading within X degrees of desired heading while in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-2.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but the command is either not sufficient to regain the desired position/heading or it results in overshoot of the desired position/heading. This could be caused by:

F. DPS inappropriately processes sensor feedback leading to undesired command due to sensor message format that is not fully compatible with DPS.
G. The Conning Officer desires unnecessarily precise DPS control of position/heading and selects improper DPS gain settings, resulting in system overreaction to environmental factors and frequent overshoot of cutter response.
H. Limitations (e.g., max rpm, max pitch) is imposed on propulsors by technician (e.g., propulsor placed in local control mode for troubleshooting/maintenance) without notification to bridge personnel.
I. A portion of the thruster allocation logic is incorrect due to bug in software update.
J. Propulsor response is limited due to component failure, clogged fuel filters, etc.

Possible Requirements for Scenario DPS-2.1:

10. Thorough integration review and testing shall be accomplished prior to fielding upgrades to any sensors that transmit to DPS.
11. Current gain settings shall be prominently shown on DPS display.
12. The Commanding Officer's permission shall be required to adjust DPS gain settings.
13. No propulsor shall be in local control while propulsion control resides with DPS.
14. DPS shall be automatically notified when propulsor is unable to respond as ordered.
15. Any DPS software update must be thoroughly tested in all modes at the LBSF prior to introduction to the fleet.
16. DPS shall provide the operator with feedback if programmed thruster allocation logic or MDE load sharing algorithms are preventing execution of commanded maneuver.

17. DPS shall update the thruster allocation logic and MPCMS shall be instructed to modify MDE load sharing if a thruster or MDE/CPP, respectively, exhibits inadequate response to provided command.
18. Visual and audible alarm shall annunciate on bridge and in ECC if any propulsor's response becomes inadequate to the point that DPS and MPCMS cannot effectively and safely modify thruster allocation logic or MDE load sharing.

UCA-DPS-3: DPS provides propulsion command more than X seconds after maneuver is required while in "hold position" mode or in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-3.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides a propulsion command to the MPCMS, but the command provides the ordered thrust more than X seconds after maneuver is required. The delay in propulsor action to change the cutter's position/heading results in the DPS sending additional (redundant) commands to the MPCMS. When the commands are ultimately carried out by the propulsors, the result is overshoot of desired maneuver to maintain position and/or heading. This could be caused by:

C. An abnormally high level of traffic is traveling over CG DDS (e.g., due to high amount / frequency of traffic generated by sensors and DPS or spurious signals), thus resulting in temporary storage of DPS commands in CG DDS memory buffer and latency of DPS command receipt at MPCMS.
D. MPCMS does not re-format and transmit DPS command to the appropriate RTU(s) within X seconds of command receipt.

Possible Requirements for Scenario DPS-3.1:

8. DPS shall affix a "time stamp" to each outgoing command.
9. MPCMS shall read each incoming command's time stamp and compare the time of command issue to time received to determine latency in CG DDS.
10. Visual and audible alarm shall annunciate on bridge when CG DDS reaches X% of capacity or when command latency from DPS to MPCMS exceeds X seconds.
11. MPCMS shall affix a time stamp to each outgoing command.
12. MPCMS shall compare the time stamp of each outgoing command (sent to RTU) to the corresponding incoming DPS command to determine MPCMS computer latency.
13. Visual and audible alarm shall annunciate on bridge and in ECC when MPCMS computer latency exceeds X seconds.

UCA-DPS-4: DPS stops providing propulsion commands too soon before sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within X degrees of desired heading while in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-4.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered

heading. DPS provides propulsion commands to the MPCMS, but the commands stop before sufficient commands are received and acted upon to keep the cutter within X meters of the desired position or within X degrees of the desired heading. This could be caused by:

D. DPS receives conflicting position feedback between CG ECDIS and the DGPS signal that is fed directly to DPS.
E. DPS receives incorrect feedback regarding cutter position, heading, or speed from DGPS, gyrocompass, or Doppler speed log, respectively.
F. MPCMS receives incorrect feedback from thrusters or MDE and CPP indicating that more thrust is being provided than what is actually being provided.

Possible Requirements for Scenario DPS-4.1:

5. In the event of conflicting positional information at DPS between CG ECDIS input and direct DGPS signal, the direct DGPS signal shall be used for determining appropriate commands to MPCMS.
6. Gyrocompass error shall be determined daily and DPS process model shall be updated with current gyrocompass error any time it changes.
7. DPS shall periodically compare gyrocompass and fluxgate compass inputs to determine if they are diverging, and notify the operator if the divergence is more than the sum of known magnetic deviation, magnetic variation, and gyrocompass error.
8. ISCS shall have ability to compare, via modeling, propulsor feedback at MPCMS, command issued by DPS, external forces (e.g., wind, current), and actual movement of ship to determine when propulsor feedback is inaccurate; visual and audible alarm shall annunciate on bridge and in ECC when propulsor feedback to MPCMS differs by more than X% from model-generated output.

UCA-DPS-5: DPS provides propulsion commands for too long after sufficient propulsion response is provided to keep cutter within X meters of desired position while in "hold position" mode or within Y degrees of desired heading while in "hold heading" mode. [H1, H2, H3, H4]

Scenario DPS-5.1: The cutter's steering and propulsion are operating under DPS control and in DP mode and "hold heading" and "hold position" commands have been issued. The buoy deck team begins working a buoy (retrieving or setting a buoy) using the buoy crane and cross-deck winches on deck. The cutter deviates more than X meters from the ordered position or more than Y degrees from the ordered heading. DPS provides propulsion commands to the MPCMS, but the commands continue to be issued after the desired maneuver is complete, resulting in overshoot. This could be caused by:

A. Latency exists in DGPS feedback receipt at DPS (e.g., due to high amount / frequency of traffic on CG DDS generated by sensors and DPS or spurious signals).
B. Incorrect or missing sensor information (e.g., from DGPS, Doppler speed log, gyrocompass, meteorological sensor, CG ECDIS, or pitch/roll/yaw sensors) is received at DPS.

Possible Requirements for Scenario DPS-5.1:

1. Visual and audible alarm shall annunciate on bridge when DGPS, gyrocompass, Doppler speed log, meteorological sensor, or pitch/roll/yaw sensor input is not received within X seconds of last input.

2. DPS shall identify when sensor messages are incomplete or corrupted and notify user when such messages are received.
3. DPS shall filter out any incomplete or corrupt data strings when making maneuvering calculations.
4. The Commanding Officer's permission shall be obtained prior to using DPS in the absence of active DGPS input (i.e., if DGPS switches to operate in "dead reckoning" mode due to insufficiently precise position determination).

A.2 DPS Action: Provide Rudder Command to Steering System

Dynamic Positioning System (DPS)				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide Rudder Command to Steering System	UCA-DPS-6: DPS does not provide rudder command when cutter deviates more than X meters to the left or right of desired trackline or when cutter is within Y meters of calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-7: DPS provides rudder command when excessive or insufficient rudder force causes cutter to deviate more than X meters to the left or right of desired trackline or to overshoot/undershoot turn to join next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-8: DPS provides rudder command more than X seconds before or after reaching the calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]	UCA-DPS-9: DPS stops providing rudder command too soon before sufficient maneuvering response is achieved to safely maintain ordered track or before sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]
				UCA-DPS-10: DPS provides rudder command for too long after sufficient maneuvering response is achieved for cutter to safely maintain ordered track or after sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]

UCA-DPS-6: DPS does not provide rudder command when cutter deviates more than X meters to the left or right of desired trackline or is when cutter is within Y meters of calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode. [H1, H2, H4]

Scenario DPS-6.1: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter deviates more than X meters to either the right or the left of the ordered trackline. DPS does not provide a rudder command to bring cutter back to within set tolerance for deviation from ordered trackline. This could be caused by:

A. DPS believes required steering configuration and sensor availability for Autopilot mode is not satisfied due to unavailable signals from main engines, propeller pitch positioner, or steering system.
B. Gyrocompass error is not updated in DPS process model.
C. Both gyrocompass and fluxgate compass do not provide signal to DPS due to internal failure or loss of primary power source and UPS.
D. Steering accidentally is placed in local control by technician.
E. Steering system malfunctions due to component failure

Possible Requirements for Scenario DPS-6.1:

1. DPS shall receive consistent status feedback from MPCMS ensuring that MPCMS is receiving consistent status feedback from main engines, propeller pitch positioner, and steering system.
2. Gyrocompass error shall be determined daily and DPS process model shall be updated with current gyrocompass error any time it changes.
3. Visual and audible alarm shall annunciate on bridge and visual prompt shall be provided for the Conning Officer to transfer propulsion and steering control to bridge control at MSCC if compass signal is not received by DPS within X seconds of last signal.
4. Visual and audible alarm shall annunciate on bridge and in ECC if steering system is in local control while operating in DPS mode
5. Visual and audible alarm shall annunciate on bridge and in ECC if steering system fails to deliver and maintain the ordered rudder angle

Scenario DPS-6.2: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter reaches the point on the ordered trackline when a rudder command must be initiated to navigate the cutter to the next leg of the ordered track (position for commencing turn is computed based on speed input to CG ECDIS). DPS does not provide a rudder command to initiate the turn. This could be caused by:

A. DPS believes required steering configuration and sensor availability for Autopilot mode is not satisfied due to unavailable signals from main engines, propeller pitch positioner, or steering system.
B. Gyrocompass error is not updated in DPS process model.
C. Both gyrocompass and fluxgate compass do not provide signal to DPS due to internal failure or loss of primary power source and UPS.
D. Steering accidentally is placed in local control by technician.
E. Steering system malfunctions due to component failure

Possible Requirements for Scenario DPS-6.2:

1. Visual and audible alarm shall annunciate on bridge if cutter goes more than X meters beyond turn initiation point (as calculated by CG ECDIS) with no rudder command issued by DPS.
2. DPS shall receive consistent status feedback from MPCMS ensuring that MPCMS is receiving consistent status feedback from main engines, propeller pitch positioner, and steering system.
3. Gyrocompass error shall be determined daily and DPS process model shall be updated with current gyrocompass error any time it changes.
4. Visual and audible alarm shall annunciate on bridge and visual prompt shall be provided for the Conning Officer to transfer propulsion and steering control to bridge control at MSCC if compass signal is not received by DPS within X seconds of last signal.
5. Visual and audible alarm shall annunciate on bridge and in ECC if steering system is in local control while operating in DPS mode
6. Visual and audible alarm shall annunciate on bridge and in ECC if steering system fails to deliver and maintain the ordered rudder angle

UCA-DPS-7: DPS provides rudder command when excessive or insufficient rudder force causes cutter to deviate more than X meters to the left or right of desired trackline or to overshoot/undershoot turn to join next trackline (planned course change) while in "high speed track follow" mode. [H1, H2, H4]

Scenario DPS-7.1: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter deviates more than X meters to either the right or the left of the ordered trackline. DPS provides a rudder command to bring cutter back to within set tolerance for deviation from ordered trackline, but the rudder angle provided is too much or too little, resulting in cutter not staying within set tolerance for deviation from ordered trackline. This could be caused by:

A. Rudder angle is incorrectly indicated by rudder angle indicator, providing incorrect feedback to DPS.
B. Steering system is unable to execute ordered maneuver due to environmental conditions.
C. The steering actuator malfunctions due to internal failure or loss of electrical power.

Possible Requirements for Scenario DPS-7.1:

1. Rudder angle indication shall be independently determined by more than one method and using more than one sensor.
2. Visual and audible alarm shall annunciate on bridge and in ECC if rudder angle indications read by different methods / sensors differ by more than X degrees.
3. Visual and audible alarm shall annunciate on bridge and operator shall be prompted to place propulsion and steering controls under Bridge mode if steering system cannot follow ordered trackline due to environmental conditions.
4. Visual and audible alarm shall annunciate in ECC when steering actuator is unable to provide commanded output.

Scenario DPS-7.2: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter reaches the point on the ordered trackline when a rudder command must be initiated to navigate the cutter to the next leg of the

ordered track (position for commencing turn is computed based on speed input to CG ECDIS). DPS provides a rudder command to initiate the turn, but the rudder angle provided is too much or too little, resulting in the cutter not staying within set tolerance for deviation from ordered trackline. This could be caused by:

A. Same causes as listed for Scenario DPS-7.1.

Possible Requirements for Scenario DPS-7.2:

1. Same requirements as listed for Scenario DPS-7.1.

UCA-DPS-8: DPS provides rudder command more than X seconds before or after reaching the calculated position on trackline where turn is required to navigate to next trackline (planned course change) while in "high speed track follow" mode. [H1, H2, H4]

Scenario DPS-8.1: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. A rudder command is issued more than X seconds before or more than X seconds after the cutter reaches the point on the ordered trackline when a rudder command must be initiated to navigate the cutter to the next leg of the ordered track (position for commencing turn is computed based on speed input to CG ECDIS). This results in an incorrectly timed turn, which further results in the cutter ending up unacceptably far to the right or left of the new ordered trackline when the cutter steadies up on its next course following completion of the turn. This could be caused by:

A. DPS has flawed process model regarding ship handling characteristics (i.e., advance and transfer) due to bugs or inconsistencies in DPS software update.
B. DPS has flawed process model regarding ship handling characteristics or changes to ship's maneuvering characteristics (e.g., changes to steering actuators, rudders or other underwater appendages).
C. Neither gyrocompass nor fluxgate compass provide signal to CG ECDIS.
D. CG ECDIS provides incorrect turning point to DPS based on incorrect advance and transfer calculation due to incorrect or missing signal from Doppler speed log.

Possible Requirements for Scenario DPS-8.1:

1. Any DPS software updates shall be tested and validated in the LBSF prior to fielding in the fleet.
2. Any changes to the ship's handling maneuvering characteristics shall be modeled and tested in the LBSF to determine potential need to update DPS software.
3. Visual and audible alarm shall annunciate on bridge when neither gyrocompass nor fluxgate compass signal is available at CG ECDIS.
4. Doppler speed log must be calibrated every X days.
5. Visual and audible alarm shall annunciate on bridge when Doppler speed log malfunction or loss of signal to CG ECDIS is detected.
6. The Commanding Officer's permission must be obtained to operate in Autopilot mode when error in Doppler speed log output is known or believed to exist.

UCA-DPS-9: DPS stops providing rudder command too soon before sufficient maneuvering response is achieved to safely maintain ordered track or before sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode. [H1, H2, H4]

Scenario DPS-9.1: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter deviates more than X meters to either the right or the left of the ordered trackline. DPS provides a rudder command, but the command stops before the cutter maneuvers to a position within the specified tolerance left or right of the ordered trackline. This could be caused by:

A. DGPS malfunction or DGPS signal degradation during transmission to DPS leads DPS to believe that cutter is on desired trackline when it is not.
B. CG ECDIS malfunction leads DPS to believe that cutter is on desired trackline when it is not.

Possible Requirements for Scenario DPS-9.1:

1. CG ECDIS must have ability to detect indications of erroneous position sensor input
2. Visual and audible alarm shall annunciate on bridge when ECDIS detects suspect position input

Scenario DPS-9.2: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter reaches the point on the ordered trackline when a rudder command must be initiated to navigate the cutter to the next leg of the ordered track (position for commencing turn is computed based on speed input to CG ECDIS). DPS provides a rudder command to initiate the turn, but the rudder command stops before the cutter maneuvers to next trackline on the track ordered by CG ECDIS. This could be caused by:

A. DGPS malfunction or DGPS signal degradation during transmission to DPS leads DPS to believe that cutter is maneuvering appropriately to the next ordered trackline when it is not.
B. CG ECDIS malfunction leads DPS to believe that cutter is maneuvering appropriately to the next ordered trackline when it is not.

Possible Requirements for Scenario DPS-9.2:

1. Same requirements as listed for Scenario DPS-9.1.

UCA-DPS-10: DPS provides rudder command for too long after sufficient maneuvering response is achieved for cutter to safely maintain ordered track or after sufficient maneuvering response is achieved for cutter to navigate to next trackline (planned course change) while in "high speed track follow" mode [H1, H2, H4]

Scenario DPS-10.1: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter deviates more than X meters to either the right or the left of the ordered trackline. DPS provides a rudder command, but the command continues for longer than is necessary for cutter to regain a position on the ordered trackline, resulting in overshoot by more than X meters. This could be caused by:

A. Same causes as listed for Scenario DPS-9.1.

Possible Requirements for Scenario DPS-10.1:

1. Same requirements as listed for Scenario DPS-9.1.

Scenario DPS-10.2: The cutter's steering and propulsion are operating under DPS control and in Autopilot mode and "high speed track follow" command has been issued. The cutter is transiting in the vicinity of other vessel traffic and/or within a marked navigation channel. The cutter reaches the point on the ordered trackline when a rudder command must be initiated to navigate the cutter to the next leg of the ordered track (position for commencing turn is computed based on speed input to CG ECDIS). DPS provides a rudder command to initiate the turn, but the rudder command continues for X seconds too long, resulting in overshoot of the turn and the cutter not steadying up on the track ordered by CG ECDIS. This could be caused by:

A. Same causes as listed for Scenario DPS-9.2

Possible Requirements for Scenario DPS-10.2:

2. Same requirements as listed for Scenario DPS-9.2.

A.3 Conning Officer Action: Transfer Propulsion and Steering Control from Bridge to DPS

Conning Officer				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Transfer Propulsion and Steering Control from Bridge to DPS	UCA-Conn-1: Conning Officer does not shift propulsion control from Bridge to DPS while Commanding Officer and / or bridge team believe cutter propulsion was placed under DPS control [H1, H2, H3, H4]	UCA-Conn-2: Conning Officer shifts propulsion control from Bridge to DPS while Commanding Officer and / or bridge team believe cutter propulsion is still under Bridge control at MSCC [H1, H2, H4]		

UCA-Conn-1: Conning Officer does not shift propulsion control from Bridge to DPS while the Commanding Officer and/or bridge team believe cutter propulsion was placed under DPS control [H1, H2, H3, H4]

Scenario Conn-1.1: The cutter's steering and propulsion are operating under Bridge control (input directly from the Conning Officer). The cutter is approaching a navigation aid to perform a buoy servicing operation. The mental model of the Commanding Officer and the bridge team is that the Conning Officer will shift propulsion and steering control to DPS and reach desired heading using joystick, followed by providing a "hold heading" and/or "hold position" command. At that point, cutter position and heading should be precisely controlled and the buoy deck team may begin buoy servicing

operations. However, control is not shifted to DPS mode, although the Commanding Officer and/or bridge team believe the cutter propulsion was placed under DPS control. This could be caused by:

A. The Conning Officer shifts control to DPS, but the minimum required propulsion machinery is not online for Joystick/DP mode (i.e., at least one MDE clutched in, pitch in remote control, steering pump online, MPCMS in maneuvering mode (MDE(s) at 720 rpm), thruster generator online, bow and stern thruster running, signal available at DPS from gyrocompass and DGPS).
B. The Conning Officer receives incorrect feedback regarding MPCMS configuration, leading him/her to attempt to shift propulsion control to DPS before necessary configuration (i.e., maneuvering mode) is obtained.
C. A fault or malfunction exists within the MSCC or DPS, preventing DPS from taking control.
D. The Conning Officer is task saturated or otherwise distracted, and forgets to switch control to DPS.
E. The Conning Officer issues command to have a member of the bridge team switch control to DPS, but bridge team members are task saturated or otherwise distracted.

Possible Requirements for Scenario Conn-1.1:

1. Visual and audible alarm shall annunciate on bridge if DPS control mode is selected without propulsors configured as required or if signal is not available at DPS from gyrocompass and/or DGPS.
2. MPCMS configuration shall be prominently on bridge in a manner that is prominent during both daytime and night operations.
3. Visual and audible alarm shall annunciate on bridge when transfer of control does not occur within X seconds of attempt to transfer control.
4. The Commanding Officer's standing orders shall encourage bridge team members to speak up if they see a safety issue due to distractions, task saturation, mode confusion, or any other reason.
5. The Commanding Officer's standing orders shall require the Conning Officer to state his/her intent in standardized phraseology when about to shift propulsion control mode and after switch has been accomplished.
6. The Commanding Officer's standing orders shall require verbal repeat-backs from bridge team when the Conning Officer announces intent to shift propulsion control mode and after switch has been accomplished.
7. Clear indication of controller mode (i.e., Bridge, Autopilot, Joystick/DP) shall be visible to the entire bridge team from their normal watch stations.

UCA-Conn-2: Conning Officer shifts propulsion control from Bridge to DPS while The Commanding Officer and/or bridge team believe cutter propulsion is still under Bridge control at MSCC [H1, H2, H4]

Scenario Conn-2.1: The cutter's steering and propulsion are operating under Bridge control (input directly from the Conning Officer). The cutter is approaching a navigation aid to perform a buoy servicing operation. The Conning Officer shifts propulsion and steering control to DPS, but the Commanding Officer and/or bridge team believe the cutter propulsion was placed under DPS control, resulting in bridge team members having wrong mental model of current controls in the event of an incident that requires casualty control procedures (e.g., inappropriate procedures would be taken due to incorrect process model). This could be caused by:

A. The Conning Officer does not verbally inform the rest of the bridge team that he/she is shifting control to DPS.
B. The Conning Officer verbally states that he/she is shifting control to DPS, but bridge team members are task saturated or otherwise distracted and neither hear nor acknowledge the statement.
C. The Conning Officer (or another operator) accidentally shifts control to DPS mode.

Possible Requirements for Scenario Conn-2.1:

1. The Commanding Officer's standing orders shall require verbal repeat-backs from bridge team when the Conning Officer announces intent to shift propulsion control mode and after switch has been accomplished.
2. Clear indication of controller mode (i.e., Bridge, Autopilot, Joystick/DP) shall be visible to the entire bridge team from their normal watch stations.

A.4 Conning Officer Action: Provide Hold Position or Hold Heading Command to DPS

Conning Officer				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide Hold Position or Hold Heading Command to DPS		UCA-Conn-3: Conning Officer provides "hold position" or "hold heading" command to DPS when chosen position or heading is unsafe [H1, H2, H4]	UCA-Conn-4: Buoy deck team begins servicing buoy before Conning Officer provides "hold position" and/or "hold heading" command [H3]	

UCA-Conn-3: Conning Officer provides "hold position" or "hold heading" command to DPS when chosen position or heading is unsafe. [H1, H2, H4]

Scenario Conn-3.1: The cutter is operating under DPS control and is receiving input from the Conning Officer via joystick controller while in DP mode while approaching a work site. The Conning Officer attempts to get the cutter to the desired heading and/or position via joystick controls, and then provides a “hold heading” and/or “hold position” command. However, the Conning Officer’s mental model is inaccurate and the chosen heading and/or position is/are unsafe due to proximity to shoals, proximity to vessel traffic, or proximity to a fixed object. This could be caused by:

G. Environmental conditions (e.g., wind, current, sea state) cause the Conning Officer to take a different approach than what was briefed prior to the evolution, resulting in him/her not conducting a through risk analysis.
H. The Conning Officer is unfamiliar with the area of operations, and he/she is not provided with sufficient oversight and coaching during the evolution.

I. The appropriate chart is not loaded into ECDIS.
J. The Conning Officer feels rushed to complete the evolution due to pressing operational tasking.
K. Sensors and bridge systems (e.g., DGPS, CG ECDIS, radar) do not provide adequate warning of unsafe position/heading
L. “Hold heading” command is transmitted to and acted upon by MPCMS but “hold position” is delayed in receipt due to latency in delivery to MPCMS by CG DDS (e.g., due to high amount / frequency of traffic on CG DDS generated by sensors and DPS or spurious signals).

Possible Requirements for Scenario Conn-3.1:

7. Operational risk assessments shall be conducted when environmental conditions differ significantly from what is expected or was previously briefed.
8. In areas of high vessel traffic or reduced visibility, an additional Deck Watch Officer shall be placed on watch to monitor and communicate with vessel traffic, allowing the Conning Officer to concentrate on maneuvering the cutter.
9. Use of the appropriate chart in CG ECDIS shall be verified prior to any evolution.
10. The Commanding Officer's permission shall be obtained prior to using DPS in the absence of active DGPS input (i.e., if DGPS switches to operate in "dead reckoning" mode due to insufficiently precise position determination).
11. The Commanding Officer's standing orders shall state that no underway evolution should be rushed, and that the Conning Officer shall contact the Commanding Officer if uncomfortable with an operational situation.
12. Visual and audible alarm shall annunciate on bridge when CG DDS reaches X% of capacity or when command latency from DPS to MPCMS exceeds X seconds.

UCA-Conn-4: Buoy deck team begins servicing buoy before the Conning Officer provides "hold position" and/or "hold heading" command. [H3]

Scenario Conn-4.1: The cutter is operating under DPS control and is receiving input from the Conning Officer via joystick controller while in DP mode while approaching a work site. The Conning Officer attempts to get the cutter to the desired heading and/or position via joystick controls. The Buoy Deck Supervisor has a flawed mental model and believes the cutter is in “hold heading/hold position” mode, and orders the buoy servicing evolution to begin. This could be caused by:

E. The Conning Officer believes that prevailing weather, current, seas, and vessel traffic conditions are extremely mild and do not require use of DPS.
F. Malfunction of DPS results in the Conning Officer deciding to control maneuvers with joystick while DPS has control (i.e., “hold heading” and “hold position” modes not available).
G. Prevailing weather, current, and/or sea conditions are such that DPS is unable to adequately maintain cutter's position and/or heading in "hold position/hold heading" mode.
H. Inadequate communications are maintained between the Conning Officer and the Buoy Deck Supervisor

Possible Requirements for Scenario Conn-4.1:

5. The Commanding Officer's permission shall be obtained to conduct buoy servicing operations in Bridge mode or in DP mode without “hold heading” or “hold position” commanded, and this

evolution shall be specifically briefed following established operational risk management procedures.

6. The Buoy Deck Supervisor shall not allow the buoy deck team to initiate buoy servicing evolution until order is received from the Conning Officer or Commanding Officer.
7. The Commanding Officer shall be notified if environmental conditions deteriorate to a point where “hold heading” and/or “hold position” commands are ineffective.
8. At least two effective operating modes of two-way communications shall exist between the Conning Officer and the Buoy Deck Supervisor at all times throughout a buoy servicing evolution.

A.5 Conning Officer Action: Provide High Speed Track Follow Command to DPS

Conning Officer				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Provide High Speed Track Follow Command to DPS		UCA-Conn-5: Conning Officer provides "high speed track follow" command to DPS when unsafe track is entered in CG ECDIS while cutter is controlled by DPS in Autopilot mode [H1, H2, H4]		

UCA-Conn-5: Conning Officer provides "high speed track follow" command to DPS when unsafe track is entered in CG ECDIS while cutter is controlled by DPS in Autopilot mode. [H1, H2, H4]

Scenario Conn-5.1: The cutter is transiting between operating areas. Minimal bridge watch team members are assigned in order to take advantage of bridge automation and allow crew members time to take care of work list tasks or rest. The Conning Officer shifts propulsion and steering control to DPS and selects Autopilot mode. He/she then provides a “high speed track follow” command to DPS. However, the trackline that DPS is commanded to follow is unsafe because, if followed, it will bring the cutter into unacceptable proximity with shoals, fixed objects, or other vessels. This could be caused by:

A. Conning Officer receives alarms when telling DPS to follow unsafe track that is entered in CG ECDIS, but decides that the track must be safe since it was entered into CG ECDIS and thus silences/overrides alarms.
B. No alarm is received warning of unsafe trackline due to internal malfunction of CG ECDIS or DPS.
C. Alarm is received but is mistaken for another alarm that is received at a similar time.
D. Conning Officer is unaware of malfunction of radar or radar signal to CG ECDIS.

Possible Requirements for Scenario Conn-5.1:

1. Visual and audible alarm shall annunciate on bridge if unsafe trackline is selected in CG ECDIS
2. Alarms related to unsafe CG ECDIS tracklines shall be distinctive in tone or pattern from other bridge alarms.
3. Any alarm for unsafe trackline shall be immediately reported to the Navigator for resolution.
4. Any CG ECDIS trackline that generates an alarm in DPS shall not be followed.
5. Unless otherwise approved by the Commanding Officer, only the Navigator shall enter tracklines into CG ECDIS, and each trackline shall be approved by the Commanding Officer prior to use.
6. Visual and audible alarm shall annunciate on bridge if there is a malfunction of radar or radar signal to CG ECDIS.

A.6 Conning Officer Action: Transfer Propulsion and Steering Control from DPS to Bridge

Conning Officer				
Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/Order**	**Stopped too Soon/Applied too Long**
Transfer Propulsion and Steering Control from DPS to Bridge		UCA-Conn-6: Conning Officer transfers propulsion and steering control to Bridge mode while he/she has incorrect mental model of the operating environment [H1, H2, H4]	UCA-Conn-7: Conning Officer transfers propulsion control from DPS to Bridge mode before buoy servicing operation is complete [H3]	

UCA-Conn-6: Conning Officer transfers propulsion and steering control to Bridge mode while he/she has incorrect mental model of the operating environment. [H1, H2, H4]

Scenario Conn-6.1: The cutter finishes a buoy servicing operation and still under DPS control in Joystick/DP mode. The Conning Officer receives orders to transit to the next work site. He/she shifts control from DPS to Bridge to manually maneuver away from the buoy and toward the desired trackline. However, the maneuver is unsafe because the Conning Officer does not have a correct mental model of the situation (proximity to or location of vessel traffic, shoals, or fixed objects). This could be caused by:

A. An otherwise qualified Conning Officer lacks the experience to handle conning duties in an unusual situation (e.g., environmental conditions, density and type of vessel traffic).
B. The Conning Officer receives correct information regarding operating environment but does not properly process it because he is task saturated, otherwise distracted, or feels rushed to get to the next work site.
C. The Conning Officer does not receive correct information regarding the operating environment due to malfunction of sensor (radar, CG ECDIS, weather sensors, Doppler speed log, or gyrocompass and fluxgate compass).

D. The Conning Officer does not receive correct information regarding the operating environment due to latency of sensor input receipt caused by high level of traffic traveling over DDS (e.g., due to high amount / frequency of traffic generated by sensors and DPS or spurious signals).

Possible Requirements for Scenario Conn-6.1:

1. When the environmental / operational situation becomes more confusing, the Operations Officer shall consider the experience level of the scheduled Conning Officer before assigned him/her to the watch.
2. The Commanding Officer's standing orders shall encourage bridge team members to speak up if they see a safety issue due to distractions, task saturation, mode confusion, or any other reason.
3. Visual and audible alarm shall annunciate on bridge when CG DDS reaches X% of capacity.
4. Visual and audible alarm shall annunciate on bridge when DGPS, gyrocompass, Doppler speed log, meteorological sensor, or pitch/roll/yaw sensor input is not received within X seconds of last input.
5. Visual and audible alarms shall annunciate on the bridge in the event of sensor malfunction.
6. No bridge alarm shall be silenced without specific verbal acknowledgement of the alarm by the Conning Officer and the Officer of the Deck.

UCA-Conn-7: Conning Officer transfers propulsion control from DPS to Bridge before buoy servicing operation is complete. [H3]

Scenario Conn-7.1: The buoy deck team is finishing a buoy servicing operation, and another operation is scheduled to follow at a different work site. The Conning Officer has an incorrect mental model that the buoy deck team has completed servicing the buoy, but they are not. The Conning Officer transfers propulsion from DPS to Bridge control while the buoy is still being actively worked (e.g., buoy or chain is secured by buoy crane, cross deck winch, or crew member with a boat hook. This could be caused by:

A. The Conning Officer believes he or she has received appropriate notification from the Buoy Deck Supervisor that the evolution is complete.
B. Inadequate communications are maintained between the Conning Officer and the Buoy Deck Supervisor
C. The Conning Officer feels rushed to complete the evolution due to pressing operational tasking.

Possible Requirements for Scenario Conn-7.1:

1. The Conning Officer shall not transfer control from DPS to Bridge without concurrence from buoy deck supervisor.
2. Standard commands and responses shall be used between the buoy deck and the bridge in order to avoid confusion.
3. At least two effective operating modes of two-way communications shall exist between the Conning Officer and the Buoy Deck Supervisor at all times throughout a buoy servicing evolution.
4. If the Conning Officer believes that he/she must transfer control from DPS to Bridge prior to completion of buoy servicing operation, the Commanding Officer's permission is required before he or she does so.

5. The Commanding Officer's standing orders shall state that no underway evolution should be rushed, and that the Conning Officer shall contact the Commanding Officer if uncomfortable with an operational situation.