NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPLORING THE USE OF HUMAN RELIABILITY AND ACCIDENT INVESTIGATION METHODS TO INFLUENCE DESIGN REQUIREMENTS FOR NAVAL SYSTEMS

by

Cindy R. Whitehead

September 2020

Thesis Advisor: Lawrence G. Shattuck
Co-Advisor: Douglas L. Van Bossuyt

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
EXPLORING THE USE OF HUMAN RELIABILITY AND ACCIDENT INVESTIGATION METHODS TO INFLUENCE DESIGN REQUIREMENTS FOR NAVAL SYSTEMS

5. FUNDING NUMBERS

6. AUTHOR(S) Cindy R. Whitehead

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis explores whether established methods from human reliability analysis and accident investigation can be applied early in system development to identify the design vulnerabilities that increase risk of system failure. Human reliability analyses evaluate performance shaping factors to quantify the likelihood of human failure before an accident occurs. Mishap investigations performed after an accident identify both human contributions to the system's failure and recommendations to avoid human failures in the future. This thesis proposes a method to evaluate system resiliency to variations in human performance and estimate the likelihood of human error. This method begins with functional analysis and failure mode analysis for a system concept, and then proposes two questionnaires based on human reliability and accident investigation criteria. This method is intended for the requirements development phase before system requirements are finalized and system design prototypes are completed. A demonstration of this method evaluates the human role using the electronic chart display and information system. Results from the demonstration reveal the two dominant factors that increase human error probability. The thesis concludes with an examination of the method's performance and results in support of validation of the method. Follow-on work is proposed to conduct a human subjects experiment for further validation and verification of the method.

14. SUBJECT TERMS human factors, human error, human reliability, mishap, risk, total system performance, acquisition	**15. NUMBER OF PAGES** 145
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

EXPLORING THE USE OF HUMAN RELIABILITY AND ACCIDENT INVESTIGATION METHODS TO INFLUENCE DESIGN REQUIREMENTS FOR NAVAL SYSTEMS

Cindy R. Whitehead
Civilian, Department of the Navy
BSE, Case Western Reserve University, 1996
MHS, Johns Hopkins University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2020

Approved by: Lawrence G. Shattuck
Advisor

Douglas L. Van Bossuyt
Co-Advisor

Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores whether established methods from human reliability analysis and accident investigation can be applied early in system development to identify the design vulnerabilities that increase risk of system failure. Human reliability analyses evaluate performance shaping factors to quantify the likelihood of human failure before an accident occurs. Mishap investigations performed after an accident identify both human contributions to the system's failure and recommendations to avoid human failures in the future. This thesis proposes a method to evaluate system resiliency to variations in human performance and estimate the likelihood of human error. This method begins with functional analysis and failure mode analysis for a system concept, and then proposes two questionnaires based on human reliability and accident investigation criteria. This method is intended for the requirements development phase before system requirements are finalized and system design prototypes are completed. A demonstration of this method evaluates the human role using the electronic chart display and information system. Results from the demonstration reveal the two dominant factors that increase human error probability. The thesis concludes with an examination of the method's performance and results in support of validation of the method. Follow-on work is proposed to conduct a human subjects experiment for further validation and verification of the method.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AIS	automatic identification system
ASEP	Accident Sequence Evaluation Program
ATHEANA	A Technique for Human Event Analysis
CDD	capability development document
CONOPS	concept of operations
CREAM	Cognitive Reliability Error Analysis Model
CRUSH	Concept Review Using SPAR-H/HFACS
DOD	Department of Defense
ECDIS	Electronic Chart Display and Information System
ECDIS-N	Electronic Chart Display and Information System-Navy
GPS	global positioning system
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HFACS	Human Factors Analysis and Classification System
HMI	human-machine interface
HRA	human reliability analysis
IMO	International Maritime Organization
JCIDS	Joint Capabilities Integration and Development System
MILI	Method of Investigation for Labor Inspectors
MSC	Maritime Safety Committee
MSC	Military Sealift Command
NAVSEA	Naval Sea Systems Command
NHEP	nominal human error probability
NIMA	National Imagery and Mapping Agency
PNT	position, navigation, and timing
PSF	performance shaping factor
R&ME	reliability and maintainability engineering
SHELL	Software, Hardware, Environment, Liveware-Liveware
SHERPA	System Human Error Reduction and Prediction Approach
SOLAS	International Convention for the Safety of Life at Sea

SPAR-H	Standardized Plant Analysis Risk-Human
STAMP	Systems-Theoretic Accident Modeling and Process
THERP	Technique for Human Error-Rate Prediction
TMRR	Technology Maturation and Risk Reduction
USCG	United States Coast Guard

EXECUTIVE SUMMARY

Accident investigations result in specific and actionable recommendations to address human factors. The review of Navy collisions in 2017 found a number of engineering and procedural contributors including design of helm controls and failure to continuously apply operational risk management (Davidson 2017). This thesis proposes that design vulnerabilities similar to those found during mishap investigations can be identified before accidents occur.

The research question for this thesis explores whether established methods from human reliability analysis and accident investigation can be applied early in system development to identify the design vulnerabilities that increase risk of system failure. These methods focus on the human-machine interactions that are critical to total system performance. This method is intended to be applied before system requirements are finalized and system design prototypes are completed. The method begins with functional analysis and failure mode analysis for a system concept, then proposes two questionnaires based on human reliability and accident investigation criteria.

The proposed method, concept review using Standardized Plant Analysis Risk–Human (SPAR-H)/Human Factors Analysis and Classification System (HFACS) (CRUSH), is an eight-step process that leads a multi-disciplinary team through a series of analyses to determine the operator actions and decisions to be evaluated. The SPAR-H and HFACS methods each provide a different point of view to the system designer. The HFACS results indicate the impact on system performance in the event of human error. The SPAR-H results quantify the likelihood of a human error. Both consequence and likelihood are needed to describe risk. The CRUSH process concludes with a review of results by the multi-disciplinary team of analysts and the formation of recommendations based on the insights gained from examining system resiliency and the likelihood of human error.

The CRUSH Step 5 questionnaire presents HFACS concepts summarizing each major HFACS category: unsafe acts, preconditions, supervisory actions, and organizational

influences. The CRUSH Step 6 questionnaire presents SPAR-H factors for evaluation in the context of HFACS categories, subcategories, and nanocodes. The result of CRUSH Step 6 is not only the human error probability for a specific operator action or decision, but the multipliers for each of the eight factors that contribute to the human error probability. The recommendations formed in CRUSH Step 8 highlight the areas where the human error probability can be reduced through system design decisions.

A demonstration of the CRUSH process uses the Electronic Chart Display and Information System (ECDIS) as the system of interest. The ECDIS is currently used by commercial mariners and the U.S. Navy to assist with safe navigation. The demonstration accomplishes all eight steps of the process to verify that the method was usable and to validate that the method provided results that were similar to findings from investigation reports from maritime accidents involving navigation. The findings of the demonstration are that ECDIS system performance is affected by the single ECDIS operator with additional influence from organizational pressures, and that human-machine interface and operator experience are the two dominant factors that increase human error probability. Follow-on work is proposed to conduct a human subjects experiment for further validation and verification of the model.

References

Davidson, P. S. 2017. *Comprehensive Review of Recent Surface Force Incidents.* Norfolk, VA: U.S. Fleet Forces Command, Department of the Navy.

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Lawrence Shattuck and Dr. Douglas Van Bossuyt, for their continual guidance and feedback during the research and writing of this thesis. Their comprehensive and objective critiques have improved both this thesis and my academic thought. My sincerest thanks go to George Lober for his coaching and thoughtful suggestions to tell the story in a compelling way.

This research would not have been possible, or as enjoyable, without Lawrence Fahey, Dr. Alexander Halliday, and William Muthig, who served as technical advisors to this thesis. I am grateful for their insights into the field of maritime navigation, and appreciate their curiosity and enthusiasm in applying their experiences to this research.

I would like to thank my NAVSEA colleagues for their support and encouragement throughout the course of my studies. Special thanks go to my supervisors from NAVSEA 05H, Ms. Karen Burrows and Ms. Shelly Yost, who are my role models and biggest cheerleaders. Thank you for your mentorship and confidence in my abilities.

Finally, I express my deepest gratitude to my friends and family for their emotional support as I worked to complete this academic achievement. In particular, I would like to recognize my parents, who motivated me to set high goals and do my best; and my husband, Tim, whose patience, unwavering support, and love allow me to grow boundlessly. To my children, Cooper, Tucker, and Piper, who inspire me every day, I love you and hope you never stop learning.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The focus of this thesis is on incorporating aspects of the human reliability analysis and mishap analysis into a methodology applied early in system development. Human reliability analysis and accident investigation methods both focus on the human-machine interactions that are critical to total system performance. This thesis proposes a method to evaluate system resiliency to variations in human performance and estimate the likelihood of human error. The proposed method is intended to be applied during the requirements development phase before system requirements are finalized and system design prototypes are completed. The proposed method is demonstrated on a naval system to uncover design vulnerabilities that increase risk of system failure. The demonstration serves as a proof of concept to (1) verify whether the new method adds additional insight to the design process by identifying previously unknown risks; and, (2) validate whether the new methodology offers useful input to the design effort. Of the four types of thesis research methods described by Giachetti (2016), this thesis is an analysis thesis.

A. RESEARCH QUESTION

Can established methods for identifying and quantifying contributors to human error be applied to the development of new Navy systems for improving the human reliability of operators and maintainers?

B. MOTIVATION

The United States Navy invests a lot of time and resources on technological advancements, yet accidents continue to occur that threaten the lives of sailors and the mission of the Navy. The Joint Capabilities Integration and Development System (JCIDS) defines a process for writing and testing system requirements and identifying risks to the program (Chairman of the Joint Chiefs of Staff 2018). However, the JCIDS process neither incorporates human fallibility into requirements or testing, nor assesses risk to the system resulting from human failure. The motivation for this thesis is to improve the needs analysis and requirements definitions for a system by informing program offices of the potential sources of human error. The goal of this thesis is to improve the expected system outputs

by addressing human performance issues identified from previous mishaps involving comparable systems and operators. Causal factors discovered during accident investigation are different from planned scenarios reflected in requirements definition during system design. For instance, operational tests do not often employ a representative user - the one who is fatigued and under environmental stress, who may or may not receive training on the system, and has to troubleshoot a system malfunction. Program offices may underestimate the importance of developing accurate and complete procedures at the time of system delivery. Program offices may not take into account that operators may be newly trained and inexperienced when they first operate the system, that operators may simultaneously be responsible for multiple systems, or that operators may be subject to personal stressors that affect their focus.

C. ORGANIZATION OF THE THESIS

This thesis is organized in five chapters. Chapter I consists of the motivation and background of this research. Chapter II provides a discussion of early system engineering requirements, human reliability analysis methods, and accident investigation methods. This chapter also includes a description of the system of interest as well as background information on the Navy command that uses the system. Chapter III is a detailed description of the proposed process for incorporating human reliability evaluation into concept review for a new system. This chapter includes a discussion of the questionnaire used to identify system vulnerabilities to human error and a discussion of the questionnaire used to calculate probability of human error. A demonstration of the proposed method on an electronic navigation chart display is the topic of Chapter IV. This chapter also presents the results of the process and a discussion of the results. Chapter V consists of the conclusions, recommendations, and future work that continues exploration of this process.

D. BACKGROUND

This proposed method should be applied during the requirements development phase of system design (Figure 1). The desired level of system reliability is established during the preceding concept development phase. System performance is dependent upon hardware, software, and human performance. Findings from the proposed method may also

result in additional detail added to the concept of operations (CONOPS) before the CONOPS is finalized. Technical specifications written during the requirements development phase are used as input to architecture development. Once a system enters system development, there are fewer opportunities for changes. Changes that occur after product release are estimated to be 30 times more expensive than changes made during the requirements development stage of the product life-cycle (Lenahan 2009).

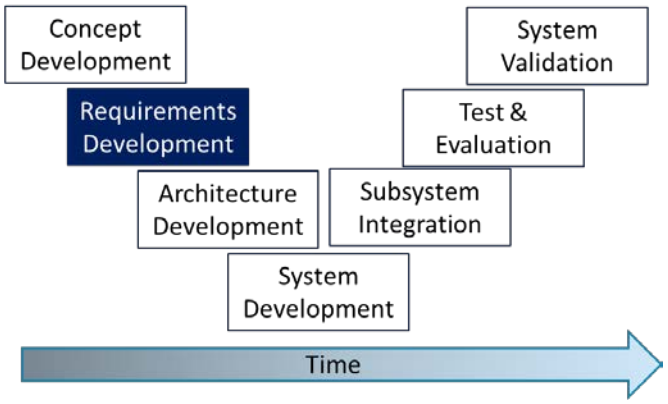

Figure 1. Timeline of insertion into systems engineering process

Acquisition programs work to reduce risk during the Technology Maturation and Risk Reduction (TMRR) phase of Department of Defense (DOD) acquisition (Department of Defense [DOD] 2015). The conceptual system design phase defines what the system must accomplish occurs during TMRR. Prototype designs created during TMRR are evaluated to reduce technical risk, validate designs, and refine requirements (DOD 2015). Training plans and human systems integration are not required to be finalized by the end of TMRR (DOD 2011). Milestone B, at the end of TMRR, is the official start of a program of record (AcqNotes 2018). The Joint Requirements Oversight Council reviews system requirements and system performance goals, described in the capability development document (CDD), in support of the Milestone B review (DOD 2015). Contracts awarded for the Engineering and Manufacturing Development phase, the phase following TMRR, are based on CDD requirements. Changes to requirements following Milestone B may

result in contract revisions. Programs are motivated to identify and mitigate risk early in the acquisition process to over cost and schedule overruns.

Acquisition activities during TMRR focus on reducing technical, production, and cost risk. During TMRR, budget analysts compare cost estimates provided by contractors against program estimates to look for unnecessary or unproductive costs that may result in future cost overages and schedule delays. To meet Milestone B exit criteria, the program must meet a production readiness level that indicates manufacturing processes, materials, and tooling are ready for production (Office of the Secretary of Defense Manufacturing Technology Program 2015). In the absence of physical prototypes, modeling and simulation is used during this phase to provide an early look at how the system may meet each technical specification in order to reduce technical risk. Because physical prototypes for operational testing do not yet exist during TMRR phase, testing with operators in operational environments is not conducted until after individual requirements are tested and system prototypes have been produced. At this late stage, it is often too late to make changes to technical requirements and to the design. The Canadian Space Agency found that insufficient testing and modeling of spacecraft and their environments contributed to 40% of spacecraft mission failures (Majewicz et al. 2020).

The Naval Sea Systems Command (NAVSEA) Reliability and Maintainability Engineering (R&ME) Manual defines operational mission failure exclusively as hardware failures that prevent successful completion of mission-essential functions (Naval Sea Systems Command [NAVSEA] 2017). The R&ME manual mentions human factors engineering and human systems integration as system interfaces but does not describe any methods to evaluate their contributions towards the reliability requirement to demonstrate a mission reliability to a specified confidence level. The manual does not include any of the validated human reliability analysis methods that could be used to estimate the probability of human failure. The NAVSEA R&ME manual also recommends that failure mode analysis and corrective actions be included in safety programs. Failure mode analysis is used to examine how a system can fail. Accident investigations are similarly methodical in determining causes and contributors to failure, but the methods are applied after a catastrophic failure has already occurred. Human Factors Analysis and Classification

System (HFACS) is a validated method that investigates the human contribution to DOD mishaps (Shappell and Wiegmann 2000) but the investigative criteria are not used towards early design requirements for a Navy system.

In the past, defense systems did not automatically incorporate scientists' innovations and analyses into their development. Wagner, Mylander, and Sanders (1999) suggest that prior to World War II, the military did not recognize the importance of scientists' contributions and did not invite scientists to participate in military operations. However, tactical military operations during World War II benefitted from the anti-submarine warfare analysis and radar technology that the scientists developed after World War I. Looking for similar benefits from the field of human systems integration, the research question examines how human performance measures developed by human factors and safety professionals can be applied upfront in system development to improve total system performance.

An investigation of the collisions between Navy ships and commercial vessels in 2017, which together resulted in the deaths of 17 sailors, revealed that human performance factors contributed to the incidents (Davidson 2017). These factors include loss of situational awareness, ineffective training programs, poor fatigue management, and poor self-assessment. Contributing to the USS *McCain* (DDG-56) collision was a bridge team that was inexperienced with the digital throttles on the helm and lee-helm consoles. As a result of the investigation, design changes were made to the steering controls of Navy ships. If the design and testing of the original digital throttles anticipated operation by inexperienced and fatigue crew, it is possible that the original digital throttle design would not have been selected. Since the investigation confirms that crew fatigue and training deficiencies exist, ship design managers must take these deficiencies into account when forming design requirements to preserve total system performance.

The commercial ship industry is also interested in incorporating technology to assist navigation on integrated ship bridges. Modern ships have hundreds of sensors and controllers which produce more information than a human operator can understand and act upon within the amount of time available. Navigators and watchstanders monitor traffic, geographical landmarks, and weather conditions to keep the ship on the desired route. They

receive information from a variety of sources including electronic charts, paper charts, automatic identification system (AIS), and lookouts. Fukuoka (2019) notes that a human's ability to transmit information while also comprehending the information and making a decision is limited, compared with a human's sensory capacity. The International Convention for the Safety of Life at Sea (SOLAS) Chapter V/19 requires the Electronic Chart Display and Information System (ECDIS) for newly built passenger ships of at least 500 gross tonnage, and newly built commercial ships of at least 3,000 gross tonnage. The ECDIS compiles geographical and depth information previously found on paper charts, route planning, and continuous tracking of a ship's own position into a single display (International Maritime Organization [IMO] 2006). The ECDIS can also be used to display radar and radar-tracked target information, among other information, as additional data layers. Automation assists by analyzing all the sensor data and presenting clear information to the operator with increased reliability, compared to a human's capacity for processing the potentially thousands of data points. This thesis uses ECDIS in a demonstration to identify the human factors that determine whether automated data presentation will guarantee safe navigation. Results from the demonstration will expose whether the system design is susceptible to human variance and also identify contributing factors to human error. The results from the demonstration will be used to form recommendations to improve human integration in the system design. The demonstration of this method will verify that the combination of human reliability analysis and mishap investigation methods can be used to evaluate the design for human roles within a system concept. The demonstration will also validate that the method results can be used to form specific recommendations to improve human integration and reduce technical risk in the system.

II. LITERATURE REVIEW

This chapter describes early system design activities and the need for reliable and recoverable systems. The literature review focuses on the importance of human integration with a system and introduces validated methods for human reliability analysis and accident investigation. The research underscores the cost impact of early error correction and justifies the selection of the specific human reliability and mishap investigation methods used in this thesis. The chapter concludes with a system description for the ECDIS, as well as a description of the Military Sealift Command mission and policies that dictate ECDIS's use.

A. SYSTEMS DESIGN

Humans, as an integral part of a system, are often the cause of system failure. An Institute of Nuclear Power Operations study found that 52% of root causes for mishaps resulting in extensive damage were due to human performance and that 33% of these significant mishaps were also subject to design deficiencies (Reason 1990). In addition to design deficiencies, Reason found that human-centered root causes, and combinations of root causes, included deficient procedures and documentation (43%) and training (18%).

The International Council on Systems Engineering defines a system as an "arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not" (International Council on Systems Engineering n.d.). System elements are typically comprised of hardware, software, and a human (Figure 2). Product design focuses on functional interactions between the hardware and software product and the human user (Langford 2012). Users interact directly with the system and impact the whole system. Internal stakeholders are entities that affect the system directly. External stakeholders are affected by a system. Langford (2012) offers that when people interact with systems, they become part of a system of systems. It is his view that interactions between a person and the system do not mean the person is integrated with the system. In practice, the system of systems includes the operators and the maintainers of the system and beyond to the organizational structure within which the operators and maintainers exist.

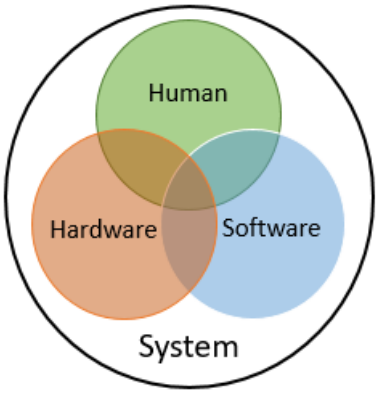

Figure 2. System composition

Integration must be considered during planning phases of system design. Langford (2012) lists requirements definition, problem solution, and stakeholder needs as key determinants of integration. He asserts that integration activities must be planned upfront to guide scheduling and development tasks. Additionally, he states that because people are integrated into a system, social and political environments can negatively affect an otherwise satisfactory technical design. Failure to consider routes of human failure in the system design and operation are failures to integrate the human with the system.

Engineered systems have a functional purpose and are created to meet an operational need (Blanchard and Fabricky 2011). Langford (2012, 251) states that if a problem is "ill-defined, erroneously defined, or undefined, the solution has no meaning." Reliability, a major component of system usefulness, is an operational need. System reliability is a combination of hardware reliability, software reliability, and human reliability (Giuntini 2000). For system hardware, the reliability function is a curve resembling a bathtub, with high failure rates at the beginning and end of their life cycle. Human performance is proposed to also have similar curve of reliability with three distinct phases: learning error rate phase, stabilized error rate phase, and fatigue error rate phase (Giuntini 2000). During the learning error rate phase, the probability of error decreases over time as the operator becomes more experienced with using the system. This reliability function is dependent on the complexity and size of the task. When the operator has learned the system, the likelihood of error is stabilized to a fairly constant value. As the operator fatigues, the error rate increases exponentially over time. Therefore, it

is not realistic to represent the human reliability rate as 100% for the full life cycle of the system. The literature review continues to search sources of variability that exist between operators and determine how a system can estimate human reliability given system-specific design attributes.

A dynamic model of situated cognition considers how humans are influenced by both technology and other humans (Shattuck and Miller 2006). System designers prioritize which data is presented to the operator. If the data is technically inaccurate or incomplete, an operator may make the wrong decision or take the wrong action. Additionally, perception and comprehension of information can vary between operators or even vary for each event, while the underlying characteristics that affect how people form perceptions stay the same (Groth 2009). System designers should be aware that these differences between operators exist and consider whether human variance can affect total system performance.

Experiments for robust design help to establish system performance targets (Ulrich and Eppinger 2016). Ulrich and Eppinger (2016) define robust design as a product development activity that improves performance while minimizing the effects of uncontrolled variations during operation. Variations can occur in human performance or operating conditions. Human reliability assessments consider variable human performance factors such as stress, training, experience, and fatigue (Gertman et al. 2005). In the detailed design phase, set points for human performance and environmental factors can be incorporated into design requirements and operating procedures to represent less than ideal operating conditions (Ulrich and Eppinger 2016). During testing, system designers can study the effect of variations on system performance by isolating and introducing control factors (Ulrich and Eppinger 2016).

System design can incorporate engineering concepts such as human-computer interfaces and redundant systems to protect against human error (Reason 1990). Buede and Miller (2016), in contrast, state that an overlap is a redundancy in functionality and that functional overlaps only cause problems. System designers will have to weigh the risks of system failure with the cost and added complexity of having a backup system. In addition to incorporating mitigations such as redundant functions into the product design, procedures that

incorporate emergency operating procedures can assist operators with recovering systems after a hardware or software failure (Papakonstantinou et al. 2016).

Incorporating recovery actions by operators and maintainers to diagnose early signs of a hardware or software failure condition can improve hardware and software reliability. Redundancy, for instance, can limit system failure by providing both visual and audible warnings to an operator to prompt action in the event of system malfunction. Written checklists can reinforce procedures otherwise subject to an operator's memory. Accident Sequence Evaluation Program (ASEP), a human reliability analysis (HRA) method, allows for recovery factors to decrease human error probability in optimum conditions (Swain 1987). The presence of multiple recovery conditions could result in a negligible human error probability of 0.00001.

In addition to pressure to deliver a product that meets all technical specifications, defense and aerospace industries have constant pressure to complete systems on time and within cost. Tan, Otto, and Wood (2017) compared the cost of correcting defects during an operational phase with the cost of correcting errors found during development. They cited a National Aeronautics and Space Administration cost study that reported a 50-fold difference in cost of space system defects found during operations compared to the defects found during early concept phases. They also cite a National Institute of Standards and Technology cost study that reported a 10-fold cost increase to fix software bugs found during operation over software errors found during coding and testing. Tan, Otto, and Wood (2017) provide additional examples of reworked projects due to engineering design decisions but do not mention the 70–80% of accidents that are attributed to human error during aviation accidents (Shappell and Wiegmann 2000). It is likely that any system errors attributed to humans also have a significant cost impact. System designers could benefit from additional tools to identify design defects early in the system development process. Early identification and correction of system flaws would avoid costly fixes after system deployment. Cost, production, and engineering risk analyses are already incorporated in the early phases of the acquisition process. Risks to system performance due to human performance should also be included for a more complete risk evaluation.

B. HUMAN RELIABILITY ANALYSIS METHODS

Systems are comprised of human and machines. Even highly automated systems require human interaction to initiate system operation, to input decisions, or to maintain the system. Human reliability analyses can alert system designers to potential modes of human failure that impact the intended operation of the system. Human error probability is the likelihood of human error quantified by a human reliability analysis.

Human reliability analyses build upon task analyses to provide qualitative and quantitative assessments of human error during human interaction with a system. Quantitative assessments use detailed data from system design and task procedures to return a probability of error. Qualitative assessments use more general information to identify areas of improvement relating to human error. Many human reliability quantification methods exist (Figure 3). The earliest method, Technique for Human Error-Rate Prediction (THERP) was developed in 1983 for the U.S. Nuclear Regulatory Commission (Swain and Guttman 1983). Analysts match their human failure events to scenarios in THERP tables that reference stress and experience to determine human error probability. Human Error Assessment and Reduction Technique (HEART) also requires analysts to match their tasks to one of six generic task types before applying adjustments from 30 different error-producing conditions (Kirwan 1996). A Technique for Human Event Analysis (ATHEANA) is among the most thorough of HRA methods, but it uses subject matter experts to form the nominal human error probabilities when other HRA methods cannot be applied (Boring and Gertman 2016).

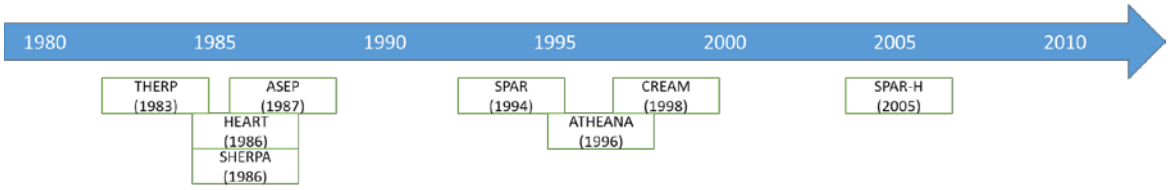

Figure 3. Timeline of selected HRA methods

Some HRA methods, such as Cognitive Reliability Error Analysis Model (CREAM), can be used for both human error prediction and accident investigation. This method categorizes failures by their error modes and causes of action (Hollnagel 1998). The method

must be applied twice, once for basic analysis and once for complex analysis, to map errors to control modes that are either strategic, tactical, opportunistic, or scrambled. The range of human error probabilities depends on the control mode. CREAM has been applied to studying causal factors for marine accidents resulting from human failures of a ship's bridge, such as the Officer of the Watch (Yoshimura, Takemoto, and Mitomo 2015). Wu et al. (2017) also studied CREAM as an accident investigative method but focused on determining uncertainty within the method's common performance conditions.

The U.S. Nuclear Regulatory Commission developed the Standardized Plant Analysis Risk-Human (SPAR-H) in the mid-1990s as a simplified approach for HRA. The SPAR-H analyst evaluates eight performance shaping factors (PSFs) for each human action and decision required by the system of interest: available time, procedures, ergonomics/human-machine interface (HMI), training and experience, complexity, stress, fitness for duty, and work processes. Three of the eight PSFs, complexity, ergonomics/human-machine interface, and procedures, align with system technical specifications. Operational tempo and product design influence the PSF of available time because system design can affect how operators make decisions. The other PSFs address organizational factors and factors specific to an individual's experience, training and stress level. Multiple studies use SPAR-H PSFs to evaluate specific aspects of system design including industrial maintenance (Franciosi 2019) and design of corrective actions (L'Her, Van Bossuyt, and O'Halloran 2017).

Researchers have created hybrid HRA methods to capitalize on the strengths of each model while compensating for the weaknesses of the other model. De Felice, Petrillo, and Zomparelli (2016) combined CREAM and System Human Error Reduction and Prediction Approach (SHERPA) into a single hybrid model that keeps the basic framework from CREAM and uses SHERPA's methods to consider the variety of operator actions. Rangra et al. (2017) created a new method specifically for the railway industry that evaluates the conditional relationship between human, technical, and organizational factors.

The desired HRA method for this thesis process should be able to be applied predictively ahead of any accident; repeatedly to allow for evaluation of alternative designs and conditions; and easily by analysts with limited HRA experience. Results from the analysis should provide enough detail to help the designers understand which factors most greatly

drive human error probability despite limited system information available during the early stages of system development. Both THERP and HEART methods require analysts to understand the HRA methods well enough to apply the nuclear-industry-originated task tables to the generic non-nuclear system under evaluation (Boring and Blackman 2016). Further, the limited number of THERP PSFs do not provide sufficient feedback to the system design team. A simplified version of THERP and geared toward for teams without HRA expertise, ASEP is criticized for being over-simplified by trading details for conservative results (Boring and Gertman 2016). Boring and Blackman judge results from CREAM to be excessively uniform due to the use of three human failure events despite the number of decisions input into the method and therefore, CREAM is rejected as a candidate method for this thesis in favor of a method that better illustrates contributions from each performance factor. De Felice, Petrillo, and Zomparelli (2016) found a limitation of SHERPA to be application to complex decision-making tasks; therefore, this method is rejected in favor of a method that considers both operator actions and decisions. An in-house analysis method is preferred; therefore ATHEANA is not considered to be a suitable candidate method due to its reliance on multiple HRA experts to form a consensus opinion. The selected HRA method, SPAR-H, is a blend of both qualitative and quantitative analysis that considers eight performance shaping factors. It allows for one-pass, repeatable evaluation of tasks by a team of non-experts. The SPAR-H method allows analysts to quickly modify inputs in response to system design or operating condition changes. This will allow the analysts to observe any resulting changes to the human error probabilities for decisions and actions.

SPAR-H calculates human error probability (HEP) by multiplying eight factors by a nominal human error probability (NHEP). Nominal HEP is widely accepted as one per one thousand occurrences (Gertman et al. 2005). However, there are multiple factors that influence whether humans fail or succeed. SPAR-H considers each of these factors one at a time using performance shaping factors. Each of eight PSFs is evaluated to determine a multiplication factor to the nominal human error probability for action, 1E-3 or the nominal human error probability for diagnosis, 1E-2. The eight SPAR-H PSFs are available time, stress and stressors, experience and training, complexity, ergonomics (including the human-

machine interface), procedures, fitness for duty, and work processes. Larger multipliers result in a greater likelihood of event occurrence.

- Available time assesses the amount of time an operator has to diagnose, decide, and execute an appropriate action. The time spent to diagnose and decide reduces time available to take action and vice versa. SPAR-H multipliers for available time range from 0.01 to 10 (Gertman et al. 2005). If there is inadequate time to diagnose, decide, or act, the human error probability is 1.0. If there is additional time to recover from errors, a multiplier less than 1 is allowed.

- High and extreme levels of stress can have a negative impact on human performance. Stress includes mental stress such as apprehension or nervousness, excessive workload, and physical stress due to excessive heat, noise, or ventilation. SPAR-H multipliers for stress range from 1 to 5 (Gertman et al. 2005).

- Complexity considers the difficulty of a task. Complex tasks require a greater skill to successfully complete. Difficult tasks have a larger chance of human error. Difficulty can be associated with great mental effort such as memory or mental calculations or physical efforts that require a complicated pattern of movement. SPAR-H multipliers for complexity range from 1 to 5 (Gertman et al. 2005).

- The experience and training PSF considers the years of experience of the individual or crew and whether the operator or crew has been trained on recovery from equipment failure. SPAR-H multipliers for this PSF range between 0.5 and 10 (Gertman et al. 2005).

- Formal operating procedures may be ambiguous, wrong, inadequate, or nonexistent. Material evaluated in support of this PSF include technical manuals, procedures, emergency operating procedures, and standing orders.

SPAR-H multipliers for procedures range from 1 to 50 (Gertman et al. 2005).

- The ergonomics PSF evaluates the displays and controls as well as the equipment and interface layout. When system controls and displays are not co-located in one designated place, it is difficult for an operator to simultaneously monitor and respond to all indicators. In some cases, required indicators are missing or misleading. Operators that ignore equipment that is consistently unreliable, even if the equipment is working correctly, cause the overall system to negatively perform. SPAR-H multipliers for ergonomics range from 0.5 to 50 (Gertman et al. 2005).

- Fitness for duty considers whether or not the individual is physically or mentally able to perform the current task. Fatigue, sickness, legal or illegal drug use, and overconfidence are unrelated to training and experience but all negatively affect operator performance. If the operator is unable to perform due to these conditions or has a negative cognitive status, the human error probability for the event is 1.0. Otherwise, SPAR-H multipliers for fitness for duty are scored 1 or 5 (Gertman et al. 2005).

- Work processes include organizational culture, communication, and management and supervisory policies that may affect performance. Individuals may not understand work requirements if planning and communication are poor. Conflicts between groups such as between engineering and operations or between operators and management, indecisiveness, an uncoordinated approach to safety, or lack of adherence to enforcement actions and notices are examples of work process problems. SPAR-H multipliers for work processes range from 0.8 to 5 (Gertman et al. 2005).

C. MISHAP INVESTIGATION METHODS

Mishaps are unplanned events that occur as a result of human actions and decisions (Reason 1990). Mishaps have negative impacts on cost, schedule, safety, and mission completion. Mishaps can also result in loss of confidence in a system or organization.

There are three types of Navy mishap investigations (Office of the Chief of Naval Operations [OCNO] 2011). Safety investigations are conducted for the purpose of preventing future mishaps. Judge advocate general manual investigations are administrative investigations. Criminal and security investigations are conducted by Naval Criminal Investigative Service. The Navy and Marine Corps Mishap and Safety Investigation, Reporting, and Recordkeeping Manual specifies the information that is collected during a safety investigation and reported by the safety investigation board (OCNO 2005). Safety investigation boards are comprised by three to five members that include subject matter experts on the system, equipment, or procedures.

The safety investigation board leader documents the following information regarding the mishap in the safety investigation report: environmental state, human factors, and material condition (OCNO 2005). Details of the mishap environment include wind, sea state, temperature, visibility, noise, and presence of lightning. Unsafe acts, supervisory violations, preconditions, and procedures are captured in the human factors section of the report. The investigators also inquire about the operator's training and experience level, level of fatigue at the time of the accident, and any evidence of drug use. Material conditions, such as wear and tear, defects, safety guard failures, and unauthorized alterations, are documented by investigators.

Both accident investigation methods and human reliability methods recognize contributions to mishaps beyond a single operator action. Leveson (2004) developed Systems-Theoretic Accident Modeling and Process (STAMP) which focuses on system safety controls as leading cause of accidents, rather than component failures. Basnyat et al. (2006) propose using mishap investigation to improve safety systems. The Software, Hardware, Environment, Liveware-Liveware (SHELL) (International Civil Aviation Organization 2012) model evaluates the interactions between physical systems, computer software, operating

procedures, pilots, air traffic controllers, maintenance personnel, and their environment, as contributors to an accident. Labor inspectors use Method of Investigation for Labor Inspectors (MILI) (Katsakiori et al. 2010) to evaluate the impact of workplace and organization factors on accident causation. DOD HFACS uses nanocodes in the domains of unsafe acts, preconditions, unsafe supervision, and organizational influences to track contributing causes of aviation mishaps (Shappell and Wiegmann 2001). The DOD HFACS classification categories are the same four categories as those in Reason's model of error causation (Reason 1990).

Multiple studies have adapted HFACS by rephrasing and adding nanocodes to be applicable to a specific industry and analysts who are more familiar with their own industry than with human reliability analysis. Modified HFACS methods have been developed, including HFACS-Maintenance Error (Schmidt, Schmorrow, and Figlock 2000), HFACS-Maritime (Xi et al. 2017), HFACS-Maritime Accidents (Chen and Chou 2012), and HFACS-Bayesian Network (Zhou, Zhang, and Baasansuren 2018). Modification of HFACS has been shown to increase inter-rater agreement over use of the original HFACS nanocodes (Schmidt, Schmorrow, and Figlock 2000; Bilbro 2013).

Studies have used HFACS to discern significance between contributing factors to human error. For instance, Taranto (2013) used HFACS to determine that ground control station design had more of an impact on human error than aircraft design. The study also found that organizational climate was the only diagnostic category that was statistically significant. The Preconditions category was rated by Chen and Chou (2012) to be the most vulnerable part of the system because hardware defects influence human actions and decisions.

Of the accident investigation methods surveyed, SHELL and HFACS are favored because STAMP and MILI each have a narrower focus; STAMP considers primarily safety controls and MILI primarily considers broad workplace factors. The SHELL method is rejected for this thesis because the tool is more conceptual than HFACS. The organization of HFACS is preferred because the description of subcategories and nanocodes both assist the analysts with applying the investigative criteria and also with understanding the results which map back to the subcategories and nanocodes.

The first category in DOD HFACS 7.0 is Unsafe Acts. Unsafe acts are the operator actions that directly lead to a mishap. Operator actions considered in this category are deliberate violations of rules and unintentional errors due to performance or mental lapse. There are 13 Unsafe Acts nanocodes in three subcategories. Accidental movements by an operator that turn equipment on or off and movements that are performed too quickly or slowly are examples of skill-based errors. Examples of judgement-based errors are failures to acknowledge a warning, failures to correctly prioritize tasks, and application of incorrect logic to choose an action. Performing workarounds to published procedures are willful violations. Individuals, crews, and teams can commit violations.

The second DOD HFACS 7.0 category is Preconditions. Preconditions include factors attributed to the operator, environment, or equipment that influence an operator's action or judgement to cause a failure. The majority of HFACS codes are preconditions. There are 61 total nanocodes in seven subcategories. Physical elements such as weather, whiteout, or dust storms impair vision. Extraneous noises and extreme temperatures distract operators from accomplishing tasks. Individuals may have cognitive, behavioral, or physical and mental limitations that can cause an unsafe condition. Mental awareness factors, including inattentiveness, fixation, confusion, overload, and boredom, affect operator perception and performance. An operator's state of mind is important to successful task completion. Life stresses, overconfidence, complacency, motivation, and burnout all affect state of mind. Physical problems affecting human performance include effects of drugs or alcohol, fatigue or dizziness, hyperventilation, light adaptation, strength, dexterity, and coordination. Sensory inputs that misrepresent balance, movement, space, time, or visual and auditory cues can lead to unsafe situations. The HFACS Preconditions category also considers team interactions. Individual failures in leadership, task delegation, assertiveness, and effective communications also contribute to human error. Step 5 uses six of the precondition subcategories. The Technological Environment subcategories propose human failures that result from system design. Technical preconditions include design of seating, instrumentation, warnings, controls, switches, automation, workspace, personal equipment, and communication equipment. This subcategory is reserved for use in Step 6.

The next category is Unsafe Supervision. The supervisory chain of command influences how operators perform. The Unsafe Supervision category considers supervision, operations planning, and supervisor violations that lead to operator error. There are three subcategories decomposed into 17 total Unsafe Supervision individual factors. Supervisors provide guidance, training, and oversight. Failure to provide good role-modeling and critical feedback, failure to selected proficient individuals, and failure to respond to critical information do not help the operator to succeed. Supervisors must adequately assess risk before their teams perform the work. They must enforce existing rules and never direct individuals to violate rules and procedures.

The last DOD HFACS category is Organizational Influences. Commanding officers establish the tempo and priorities for their organizations. The Organizational Influences category considers how senior leaders address overall operations, procedures, and oversight. Four Organizational Influences subcategories are decomposed into 18 total nanocodes. Senior leaders control resource levels and staffing selection, including the establishment of infrastructure, intelligence, command and control, and funding in the overall system environment.

D. ELECTRONIC CHART DISPLAY AND INFORMATION SYSTEM

Accident investigations following ship collisions and groundings find that human error is a cause of 80–85% of maritime accidents (Baker and Seah 2004). Baker and Seah (2004) report that 72% of the human factor errors were due to situation assessment and awareness. Filipkowski (2013, 256) reports that the most common cause of groundings are "bad management and lack of cooperation on the bridge" (18%) and "lack of or improperly preparing voyage planning" (17%). Modern seafarers also face an increasing operational pace and longer working hours, resulting in insufficient rest hours (Yilmaz, Basar and Yüksekyildiz 2018). These findings indicate that although an installed system provides compiled navigational and voyage information, human error using the system can still result in accidents at sea.

The system selected for demonstration, ECDIS, is used by the Navy and by commercial ships worldwide. The ECDIS is an electronic navigation system that integrates

data such as ship's course and speed, the ship's depth and radar data, and electronic navigation charts (IMO 2006). Manufacturers of the ECDIS include Furuno, Marine Technologies, Navico, Northrop Grumman Sperry Marine, and Raytheon (United States Coast Guard [USCG] 2020). Ships may use any United States Coast Guard (USCG)-certified ECDIS system. According to the Military Sealift Command Force Navigator, a ship's navigation officer uses ECDIS for voyage planning, route monitoring, and monitoring traffic on AIS (email to the author, July 17, 2020). Prior to electronic charting, mariners used paper charts to track the ship's position against water depth, navigational hazards and navigational aids. A separate National Oceanic and Atmospheric Administration database supplies information electronically on tides and currents (Lawrence Fahey, personal communication, June 14, 2020). Future iterations of ECDIS will allow for integration of tidal information within ECDIS (Alexander Halliday, personal communication, July 1, 2020). The system has 40 layers of geographic information that users can choose to individually show or hide on the computer screen (IMO 2004). Visual and audible alerts warn the operator when the ship crosses preset navigational boundaries or enters dangerous conditions (IMO 2006). However, it is the ship's radar system and not ECDIS which issues alerts when the ship is in close proximity to other ship traffic (Lawrence Fahey, personal communication, July 1, 2020).

The International Maritime Organization (IMO) Maritime Safety Committee (MSC) requirement, MSC.232(86), mandates that all ships ranging from 500 gross ton passenger ships to cargo ships in excess of 10,000 gross tons use ECDIS. Implementation began in 2010 with newly constructed ships and ended in 2018 on existing ships (Figure 4).

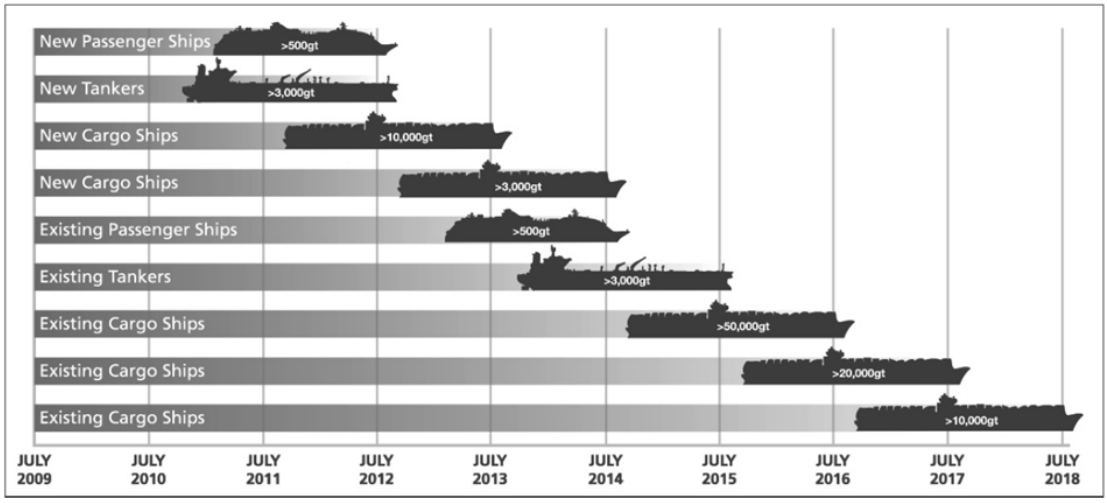

Figure 4. ECDIS implementation schedule on commercial ships.
Source: Kos, Brcic, and Pusic (2013).

The global positioning system (GPS) was first developed in 1963 for position, navigation, and timing (PNT) and became fully operational in 1995 (Grenier 2019). Celestial navigation, once relied upon by sea voyagers, is no longer taught at the U.S. Naval Academy (Grenier 2019). In 2006, the IMO MSC introduced Resolution MSC.232(82) which revised the performance standards for ECDIS. The revised performance standards address the capability to update electronic charts, preservation of the data integrity of electronic navigation charts, operational and functional ECDIS requirements, and requirements for integration and interfaces with other ship equipment. Ships are still required to keep paper logs and paper charts as a means of redundancy. The *Guidance for Good Practice*, published by IMO in 2017, consolidates guidance from seven IMO circulars into one consolidated document to assist navigators with ECDIS implementation and safe operation. The seven topics within MSC.1/Circ.1503/Rev.1 (2017a) are SOLAS chart carriage requirements, maintenance of ECDIS software, known ECDIS operating anomalies, differences between raster chart display system and ECDIS, ECDIS training, transitioning from paper charts to ECDIS navigation, and guidance on training on ECDIS simulators.

The installation of ECDIS on ships does not mean a ship will be free of all navigation failures. Ships equipped with ECDIS still have grounding accidents. The United

Kingdom Marine Accident Investigation Branch found instances in their investigations where ship's officers had not been trained to use ECDIS, the navigation officer and other bridge personnel did not have sufficient ECDIS experience, and a voyage plan that was prepared by an inexperienced and unsupervised junior officer was reviewed neither by the captain before departure nor the navigation officer at the beginning of the watch (Fukuoka 2019). Bye and Aalberg (2018) studied 931 maritime accidents that occurred in Norwegian waters between 2010 and 2016. They found that navigation accidents comprised 69.2% of cargo vessels accidents, 44.3% of passenger vessel accidents, and 66.5% of fishing vessel accidents. Generally speaking, not all collisions and groundings are due to navigational error. Some accidents result from improper steering. Bye and Aalberg also found that variables that increase risk of navigation accident are unrelated to ECDIS operation: type of vessel, low visibility, darkness, vessel length, vessel age, gross tonnage, days of operation, speed in last hour, number of course alteration, number of recent port calls, and the number of vessels in the immediate area. Bauk and Radlinger (2013) suggest that electronic navigation systems mitigate navigator fatigue and stress, which results in fewer maritime accidents. Others such as Fahey and Muthig (Lawrence Fahey and William Muthig, interview, July 8, 2020), theorize that ECDIS is a safety improvement because it provides warnings based on a continuous PNT data and adds operational capability by providing the navigator with accurate, real-time information. Schweighardt (2001) found in his thesis that eight of the Navy's 17 collisions and groundings from 1998–2001 could have been prevented by using Electronic Chart Display and Information System-Navy (ECDIS-N). He also calculated that installation of ECDIS across the fleet would have saved 96% of the repair cost for the accidents.

1. Military Sealift Command

The Military Sealift Command (MSC) supports the Navy and DOD by providing logistics support, transporting military equipment, cargo, and supplies combat forces worldwide, as well as humanitarian relief (Military Sealift Command [MSC] n.d.a). For the purpose of this thesis, the acronym MSC is used to refer to the Military Sealift Command, while the International Maritime Organization Maritime Safety Committee will be referred to as IMO MSC. All government-owned, government-operated MSC ships have

ECDIS installed in accordance with SOLAS V/19. U.S. Fleet Forces Command directs MSC Navy-unique matters, and the Assistant Secretary of the Navy for Research, Development and Acquisition directs MSC procurement policy and provides oversight (MSC n.d.a). However, according to Dr. Alexander Halliday, the MSC Force Navigator, MSC is exempt from some Navy requirements, specifically those pertaining to combatant ships (Alexander Halliday, personal communication, July 1, 2020). In further discussion with Dr. Halliday and Mr. William Muthig, MSC Training Division Chief, MSC meets both Navy requirements and the IMO certificate of voluntary compliance. In contrast to Navy ships, the MSC workforce is comprised of 80% federal civil service mariners (CIVMARs) (MSC n.d.a). It follows that the MSC follows civilian commercial ship standards, including those for manning levels and personnel organization.

The commanding officer of an MSC ship is the master and his executive officer is the chief mate (MSC n.d.b). Both are required to be licensed (USCG 2018). The second officer is the navigation officer (MSC n.d.b). It is the sole responsibility of the second officer to prepare a navigation plan (MSC n.d.b). According to Dr. Halliday, in discussion with the author on July 8, 2020, the navigation officer prepares the voyage plan and the master reviews and signs the voyage plan. Both the second and third officers serve as watch officers (MSC n.d.b). Dr. Halliday states that a typical watch team consists of a watch officer, helmsman, and lookout. The watch officer is responsible for monitoring the voyage (MSC n.d.b).

2. U.S. Navy

The Navy's electronic charting system, ECDIS-N, has Navy-specific requirements in addition to those in Maritime Safety Committee revised performance standards for ECDIS. Program Executive Office Integrated Warfare Systems 6.0 controls the software requirements document for ECDIS-N (Scott Downs, personal communication, May 14, 2020). Northrop Grumman's Sperry Marine Interfaces developed the ECDIS-N to work with a ship's navigation system and sensors including PNT distribution systems, GPS receivers, gyrocompass, speed sensors, and fathometers, and radio detection and ranging (Fein 2005). The Navy certified ECDIS-N for use on all surface ships and Los Angeles-

class submarines in 2005, with full-fleet implementation in 2009 (Fein 2005). Fein continues that electronic charts on 29 compact discs replace approximately 5,000 paper charts. According to Lawrence Fahey in a discussion on July 1, 2020, ships install chart updates received via compact disc or data link.

Differences exist between ECDIS-N and ECDIS. The Navy's ECDIS-N includes software requirements that do not apply to ECDIS and receives chart information from the National Imagery and Mapping Agency (NIMA) instead of the Government Hydrographic Office (Lawrence Fahey, personal communication, May 14, 2020). The Navy's ECDIS-N uses the NIMA database format and automatic updating instead of the International Hydrographic Organization database format and updates, and also uses Navy-specific position systems and sources (OCNO 2001). Differences also exist between the navigational requirements that the Navy follows and the requirements followed by commercial ships. The general requirements for safe navigation apply to military vessels. However, Navy military ships are exempt from following certain aspects of SOLAS convention such as those pertaining to carrying a second power supply for the navigation system as claimed by Dr. Halliday in a July 1, 2020, interview with the author. Also, the Navy is generally not required to comply with IMO resolutions but follows DOD mandates to use international standards wherever possible. (OCNO 2001).

The thesis process proposed in Chapter III considers a motivation during TMRR is to reduce risk despite the lack of detailed system specifications following the concept development phase. The literature review surveyed a number of human reliability methods and accident investigation methods to select candidate methods that could be used by a team of analysts with little knowledge and experience of human reliability and accident investigation. The SPAR-H human reliability method and the DOD HFACS accident investigation method both have potential to accept the available concept information as input and then return potential areas of risk of system failure as results of the analysis. The selected system of interest for the demonstration has relevance to the Navy, but because of the classification requirements for ECDIS-N, this thesis will focus on the usage of ECDIS within the MSC, which follows commercial requirements for ECDIS.

III. RESEARCH METHOD

Both human reliability analysis and mishap analysis involve systems-of-systems thinking to understand the individual, environment, and organizational factors that contribute to human errors in action and decision-making. Human reliability analysis considers the likelihood of events that have not yet occurred. Mishap investigations uncover contributing factors to an accident that has already occurred. Using these methods in combination reveals whether the system design is resilient to human failure or whether the design itself causes a human to make the wrong decision or take the wrong action. This chapter describes a method to combine the attributes of human reliability analysis and mishap investigation into a process that begins with the concept of a new system.

A. OVERALL DESIGN EFFORT

Humans, as part of the system, are important for system success. System success is the accomplishment of the intended system function. Within the system boundaries, humans interact with system hardware and software to control and monitor functions, to recover from system malfunctions, and to maintain and support the system architecture among other activites. Given that humans are able to adapt to the capabilities and limitations of technology, the role of humans within systems is even more powerful (Norman 2005, 16). Norman proposes that system failures could be the result of a misunderstanding of humans and activities, and that a greater understanding of the activity could benefit total system performance. The proposed method in this thesis is intended to be used during the requirements development phase following the definition of desired system activities during the concept development phase. At this stage of development results from the proposed method can be used to improve the definition of human activities within the system if warranted.

Systems rely on humans to diagnose, decide and act. The operator recognizes the system state and the operational environment, decides on an appropriate action, and executes the action. Boyd described this cycle as an observe-orient-decide-act loop (Angerman 2004). In this loop, the human takes in sensory input and considers the new

input in the context of the present environment and previously obtained knowledge before forming a decision and taking action. The operator's role ranges from controlling the machine to making complex decisions on actions in atypical or emergency situations (Havlikova and Sediva 2012). Successful accomplishment of human activities is dependent upon an operator's personal factors including training, experience, and present physical condition, among other factors. The SPAR-H methodology applies these performance factors to calculations of both decision-based and action-based errors.

Hermann (2014) offers that the system boundary between the technical infrastructure, of which the human is a part, and organizational processes is blurred. He advocates for a socio-technical system design to improve system success. Beyond the system boundaries, humans affect a system through supervisory practices, organizational policies, and operational pace (Figure 5). Both SPAR-H and HFACS evaluate supervisory and organizational influences on system performance.

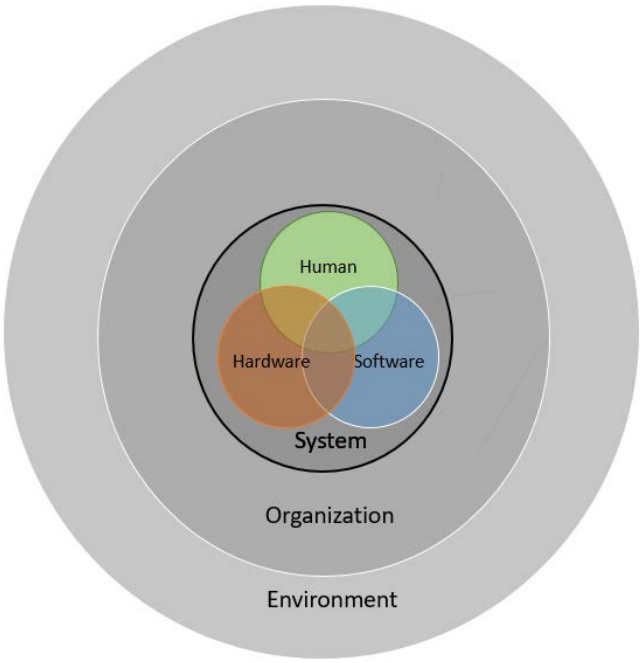

Figure 5. External interfaces to system

System hardware and software operate within defined tolerances. There is a similar range of individual human performance and organizational processes that affect system performance. The questionnaires developed for the proposed process present performance factors that may affect how successfully an operator contributes to system performance. The proposed method will evaluate how well the design is anticipated to perform given a range of individual, supervisory, and organizational conditions.

Sequential steps in the proposed process help an assessment team to scope the analysis to the system functions that require human action and decision then identify the combination of human, hardware, and software events that are needed to complete the function. As the process continues, the analysis will reveal which functions are the most vulnerable to a variable human performance, and the likelihood that the human will make an error while performing a system function. The results in total can be used to form specific recommendations that address human interactions with the system that increase technical risk.

B. CONCEPT REVIEW USING SPAR-H/HFACS PROCESS

As an approach to review the system concept for the purpose of providing inputs and feedback to system requirements, this thesis creates the Concept Review Using SPAR-H/HFACS (CRUSH) process (Figure 6). The overall CRUSH process is based on IEEE-1082-2017 (2017) which describes how HRA can be included in a probabilistic risk assessment. A brief description of each step of CRUSH follows with detailed information in subsequent subsections.

Figure 6. CRUSH process steps

In Step 1 of CRUSH, the program identifies a human reliability requirements team to perform the evaluation. Requirements are developed by a multi-disciplinary team that is invested in the operations and maintenance of the system. This team develops requirements that include system functionality, the user population, the system environment, and concept of operations. The requirements development team resourced by the program is typically comprised of a diverse group of engineers, operators, managers, and logisticians. A subset of the program requirements team will be used for the human reliability requirements team to focus specifically on human interactions with the physical system. The addition of at least one human factors specialist gives the human reliability requirements team a perspective on how humans make decisions and perform given various inputs and under varying environments. Once formed, each member of the human reliability requirements team becomes familiar with basic human reliability concepts such as human failure events, causes and types of human error, and nominal human error potential.

In Step 2, the human reliability requirements team studies the goals of the proposed system operation. This is a top-down approach as the team looks from the overall system capability to individual system functions. During this second step, the team defines the system boundaries, which subsystems are critical, essential, or non-essential, and threshold

levels for success in the case of degraded operations. The team notes system functions that require human interactions including processes to initiate, operate, maintain, and retire the system. The team should also note any policies and constraints that affect system operation. At the end of Step 2, the human reliability requirements team reaches a consensus on the threshold of acceptable system performance. This guides the sensitivity of the analysis. Human failure events can result in various levels of system performance ranging from normal operation to system degradation or system loss.

Step 3 has the human reliability requirements team note the system functions that require human interactions and initial estimates of time available for each human interaction for decision-making and to take successful action. Sources of information include the draft CONOPS, draft CDD, and preliminary acquisition strategy. For each system function with a human interaction, the team can decompose system functions into human functions using a functional analysis. This analysis is a functional analysis and not a task analysis because the system is still being conceptualized. Even with highly automated systems, humans receive input from indicators and alarms. Humans may also initiate or execute actions for operation or recovery. An action diagram (Figure 7) is one type of model that depicts functions in a chronological order. Each block in the action diagram represents a human interaction with the system needed to complete the system function. Recovery actions to restore functions can also be included in an action diagram. The functions represented in the action diagram will be referred to as “work blocks” for the purpose of this thesis. The work blocks in the action diagram are presented in chronological order to show the order functions are access to complete a task from start to finish. In reality, the tasks depicted by each work block are used multiple times as needed by the operating personnel.

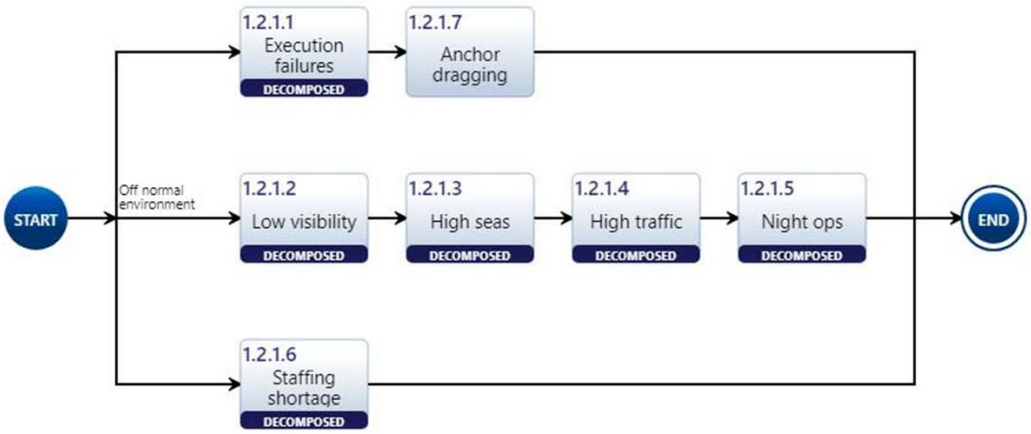

Figure 7. Sample action diagram for bridge navigation operations

In Step 4, each human function in an action diagram can be further decomposed into combinations of basic events comprised of hardware, software and human events. These may be depicted in fault trees to show various ways that the combinations of events are needed to succeed or fail. The fault tree is a logic diagram that depicts the combination of basic events that could cause the top event failure to occur. The top event of each fault tree is a failure of each work block in each action diagram. For instance, a fault tree depicting “Failure to recognize that an alarm or indicator requires attention” shows failure pathways encompassing shortcomings of the system design and personal factors that affect whether an individual’s attention is drawn to the indicator or alarm (Figure 8). Human events can be combined with hardware and software failure. Among other design reasons, the machine components responsible for the visual or audible presentation may not be adequate given the operational environment. The sample fault tree shows that, in addition to an operator’s personal factors, if the alarm was previously disabled or an operator is attending another piece of equipment in a different area, then the alarm can go unnoticed. For other top events, if successful completion of a prerequisite step is required, the fault tree logic includes a basic event for the completion of the prerequisite step.

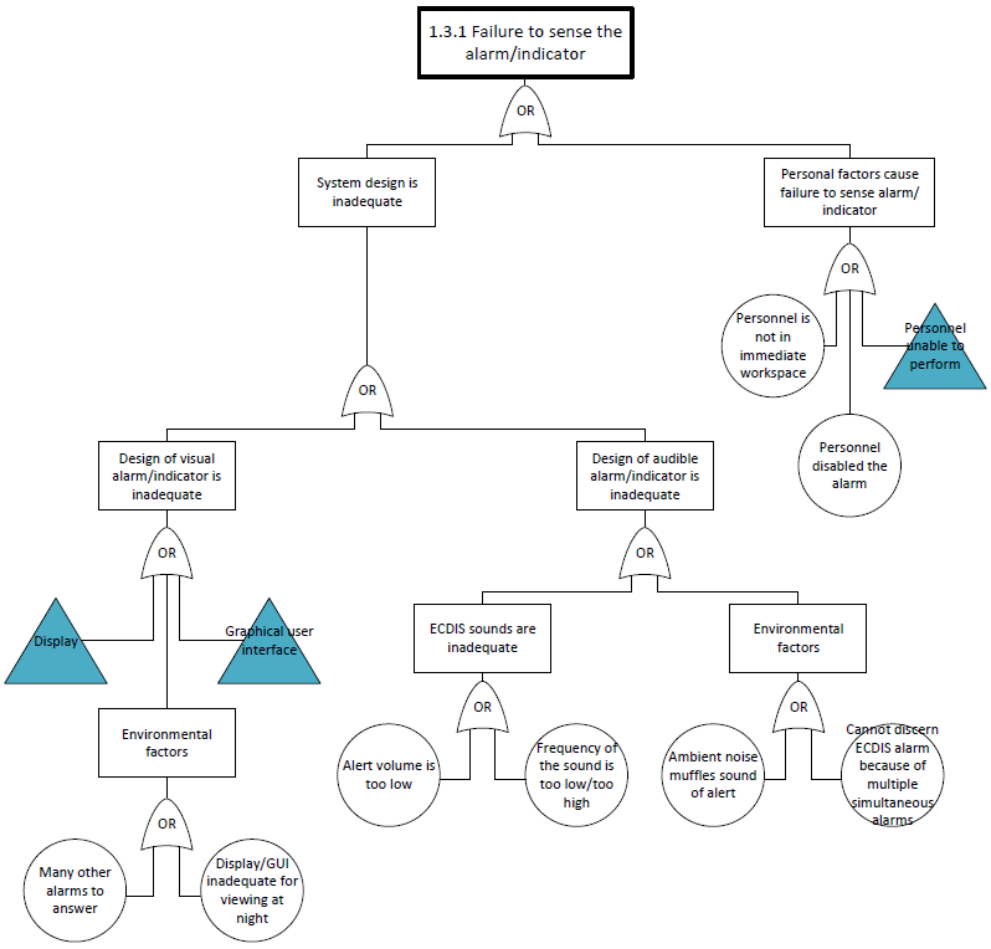

Figure 8. Sample fault tree for failure to sense the alarm/indicator

Recovery events by humans are also subject to human failure. Analysts may include planned recovery events by humans in the functional analysis, action diagram, or in the fault tree in combination with a hardware or software error. Recovery events are treated the same as other human failure events in CRUSH. The likelihood of human error for a recovery event indicates the probability that the recovery event is not successful.

In Step 5, the team completes a questionnaire that is based on the HFACS categories of unsafe acts, preconditions, supervision, and organizational influences. The purpose of this step is to determine the impact on system performance if specific conditions exist. The result of this evaluation is a list of HFACS subcategories that would each render a system nonoperational. Section C details the development and rationale of this questionnaire.

In Step 6, the team focus is on evaluation of the impact of the system design on human reliability. The purpose of this step is to determine the probability that a human commits an error for a particular event and the factors that increase this likelihood. This is a bottom-up approach as the team looks to reverse-engineer the system design to remove sources of error. SPAR-H performance shaping factors and PSF multipliers are used to calculate human error potential. This thesis proposes a questionnaire in Step 6 that uses HFACS nanocodes to select the level of each PSF. PSF evaluation focuses on attributes that result in a PSF level greater than 1. Certain conditions cause a 50-fold increase in error probability while other conditions do not increase the standard human error potential. The result of this step is a calculated probability of human error and a specific reason for selection of each PSF multiplier. Section C details the development and rationale for this questionnaire.

In Step 7, the results from Steps 5 and 6 are reviewed to confirm that the results are correct and realistic. The program may not have anticipated all the human roles that influence whether the system function can be completed. It may also be unexpected to have a number of work blocks where the calculated HEP is 1.0. The team can review the individual PSF multipliers for any HEPs that did not meet expectations and re-evaluate the HEPs to provide extra fidelity in the assessment of the individual PSFs.

In the final step, Step 8, the team presents the results of the CRUSH process to program leaders. Decision makers can consider whether the calculated human error probability is acceptable for total system performance. The analysis also can identify relative probabilities between two actions if alternate designs are presented. Program leaders may use the results to add functional requirements, technical specifications, or advocate for changes to training, staffing, or policy guidelines. Leaders may also choose to accept the identified risks without any changes to program efforts. Because this new method is a model, different inputs can be proposed to determine impact to the overall probability of occurrence. Decision makers can examine the inputs to the analysis to determine which actions and designs have major contributors to the probability.

C. DETAILED DESCRIPTION OF CRUSH STEPS 5 AND 6

Steps 5 and 6 of CRUSH use a combination of HFACS and SPAR-H attributes to evaluate the proposed system concept. This section discusses each question posed by the Step 5 and Step 6 questionnaire, and how each question is related to the HFACS and SPAR-H assessment criteria.

1. CRUSH Step 5

In Step 5, the impact of external influences on system performance is explored further. This step is repeated for each work block identified in Step 4. Physical environment and organization culture as well as individual attributes like training, experience, motivation, and physiological problems are put forward individually as challenges to the system to determine if the work block can still be accomplished.

Step 5 uses predominantly HFACS subcategories as the basis for the questionnaire. Shappell and Wiegmann (2000) organized HFACS into four categories that match the four tiers of Reason's Swiss Cheese Model: Unsafe Acts, Preconditions to Unsafe Acts, Unsafe Supervision, and Organizational Influences. Each category is further divided into subcategories and nanocodes, which are individual factors within the subcategories. Shappell and Wiegmann's (2000) original HFACS has 147 total nanocodes. King et al. (2015) reduced the number of nanocodes in DOD HFACS 7.0 to 109 nanocodes for the purpose of improving inter-rater agreement (King et al. 2015). This thesis uses the subcategories in DOD HFACS 7.0.

The questionnaire references the HFACS subcategories instead of the more detailed HFACS nanocodes because inter-rater agreement is greater at the category level compared to the nanocodes level (O'Connor 2008; Griggs 2012). Agreement at the category level ranged from 53% to 99% (Ergai 2013). Agreement at the nanocode level ranged from 24% to 43% (Ergai 2013). Studies propose that poor agreement is due to over-specificity of nanocodes descriptions, amount of HFACS training, and human factors experience of the raters (O'Connor 2008). Restricting the use of HFACS in this thesis to 17 subcategories instead of using all 109 nanocodes reduces the complexity of the method and improves the

reliability of the method itself. Figure 9 introduces the categories, subcategories, and nanocodes used in the CRUSH Step 5 questionnaire.

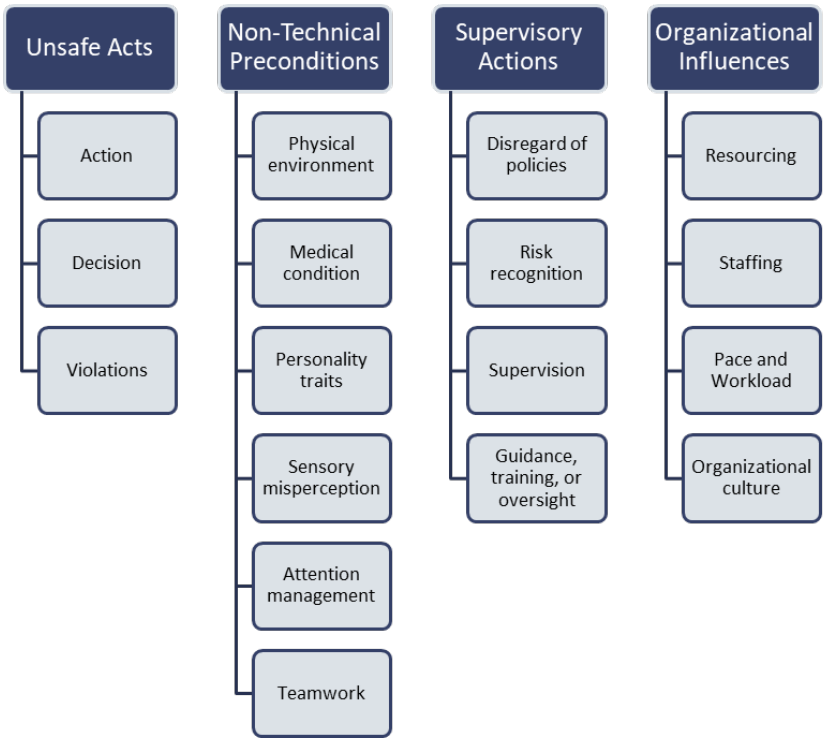

Figure 9. CRUSH Step 5 focus areas based on HFACS

The Step 5 questionnaire consists of four binary questions with additional descriptive statements for each question (Figure 10). The evaluator should add a specific example of failure for each sub-statement as applies. The Step 5 questionnaire is provided in the Appendix.

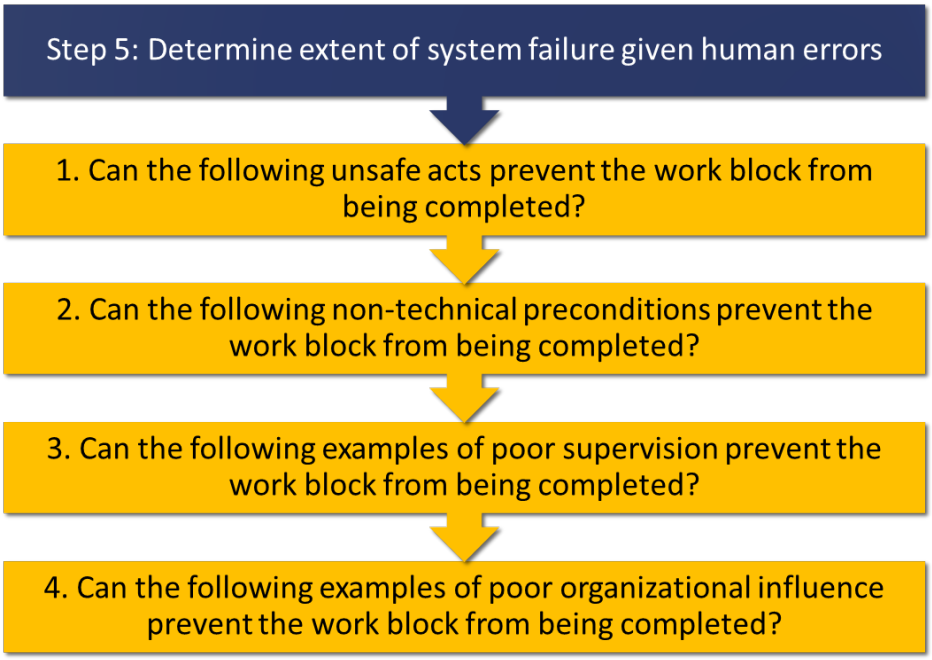

Figure 10. Individual questions in the CRUSH Step 5 questionnaire

Question 1 focuses on unsafe acts and asks whether a judgement error, action error, or violation would cause the work block to be uncompleted. There are three statements in this section that correspond to HFACS nanocodes for the subcategories: performance-based errors (AE100), judgment and decision-making errors (AE200), and violations (AV000). Question 1 is anchored by the phrase "Can the work block be completed" to remind the evaluator that only the statements that result in a work block failure are counted. This does not imply that the entire system will fail if each condition is satisfied. The conditions supporting question 1 are:

- Wrong decision or no decision
- Wrong action or no action
- Violation of known procedure.

Agreement with at least one of the three conditions results in a Yes for Question 1. The team notes any specific actions, decisions, or violations to document the assumptions used in the evaluation. The result from this evaluation shows the work blocks that withstand

the worst-case scenarios for each of the 17 HFACS subcategories; and the HFACS subcategory that prevent other work blocks from being completed.

Question 2 focuses on preconditions and asks whether non-technical preconditions would cause the work block to fail. There are six statements in this section that correspond to HFACS nanocodes for precondition subcategories: physical environment (PE100), physical problem (PC300), state of mind (PC200), sensory misperception (PC500), mental awareness (PC100), and teamwork (PP100). Question 2 is anchored by the phrase "Can the work block be completed" to remind the evaluator that only the statements that result in a work block failure are counted. This does not imply that the entire system will fail if each condition is satisfied. The statements supporting question 2 are:

- Physical environment negatively affects operator action or decision
- Individual's medical or physiological condition
- Individual's personality traits, psychosocial problems, psychological disorders, or inappropriate motivation
- Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation
- Individual's attention management or awareness negatively affects the perception or performance of individuals
- Interactions among individuals, crews, and teams.

Agreement with at least one of the six conditions results in a Yes for Question 2. To document the assumptions used, the team notes the specific physical environment, individual trait, condition, or team interaction that exemplifies each statement. The result of this step is a list of individual conditions and physical environments that prevent completion of each work block.

Question 3 focuses on supervisor influences and asks whether these would cause the work block to fail. There are four statements in this section that correspond to HFACS

nanocodes for the supervisor subcategories: supervisory violations (SV000), planned inappropriate operations (SP000), and inadequate supervision (SI000). An extra statement that addresses guidance, training and oversight is added both to include a specific example of improper supervision and also to later inform Step 6 of the availability of training. Question 3 is anchored by the phrase "Can the work block be completed" to remind the evaluator that only the statements that result in a work block failure are counted. This does not imply that the entire system will fail if each condition is satisfied. The statements supporting question 3 are:

- Supervisor willful disregard of instructions or policies
- Supervisor failure to recognize and control risk
- Inappropriate or improper supervision
- Supervisor failure to provide guidance, training, or oversight.

Agreement with at least one of the four conditions results in a Yes for Question 3. To document the assumptions used, the team notes the specific supervisor action that exemplifies each statement. The result of this step is a list of work blocks that are resistant to all supervisory failures; and work blocks that cannot be completed due to supervisory failures.

Question 4 focuses on organizational influence and asks whether organizational policies and resourcing would cause the system to fail. There are four statements in this section that correspond to HFACS nanocodes for organizational influence subcategories: resource problems (OR000), personnel selection and staffing (OS000), policy and process issues (OP000), and climate or cultural influences (OC000). Question 4 is anchored by the phrase "Can the work block be completed" to remind the evaluator that only the statements that result in a work block failure are counted. This does not imply that the entire system will fail if each condition is satisfied. The statements supporting question 4 are:

- Deficient or inadequate resources
- Personnel selection and staffing

- Policy and process issues, including pace and workload, training, and guidance
- Organizational culture influences on individual actions.

Agreement with at least one of the four statements results in a Yes for Question 4. As objective quality evidence, the team notes the specific organizational influence that exemplifies each statement. The result of this step is a list of work blocks that are resistant to all organizational failures; and work blocks that cannot be completed due to organizational failures.

The final step is to tally all the statements that would individually incapacitate each work block. The application of HFACS 7.0 after an accident is to detect and identify causal factors. During the concept review process, the same causal factors can be used proactively as a risk detection and mitigation strategy during system development. By matching each of the causal factors to system performance one at a time, none of the causal factors is excluded from consideration. The outcome of Step 5 informs system designers of all the conditions that would compromise the human functions that are required for system performance.

2. CRUSH Step 6

In CRUSH Step 6, the major contributors to failure analyzed for this step are those that are under the control of the system designers and program office. The result from Step 6 is a probability of human error for each work block. This step is repeated for each human function required by the system, as identified in Step 3 and analyzed in Step 5. The analysis for each event uses the eight SPAR-H PSFs and a nominal HEP to calculate the likelihood of failure for the human interaction. This questionnaire prioritizes PSFs with the largest impact on HEP, then other factors that affect HEP to a lesser degree. The analysis includes both a qualitative assessment and some limited quantitative assessment of relative risk. HFACS subcategories associated with system design form the base of the qualitative assessment for system induction of human failure.

Step 6 uses the SPAR-H methodology because the evaluation of each performance shaping factor is qualitative in nature, selecting the PSF multiplier level that best describes the work block. The method does not require system maturity and can be applied to early designs. It does not rely on reference models. It does not require specialized training to apply the method.

The eight SPAR-H PSFs encompass system design (ergonomics, complexity), logistics support (procedures, training), and operational environment. The PSFs consider both individual contributions to failure (training, stress, fitness for duty, experience) and organizational culture (training, work processes). The PSFs represent both internal factors, such as human attributes, skills, and abilities that are unique to individuals, and external factors that are associated with the task, such as the environment and equipment.

CRUSH recognizes that some PSFs have the greater potential to increase the HEP than other PSFs. Available time and fitness for duty have the potential for guaranteed failure. It is possible for available time, procedures, ergonomics, complexity, work processes, and experience/training to reduce HEP (Figure 11).

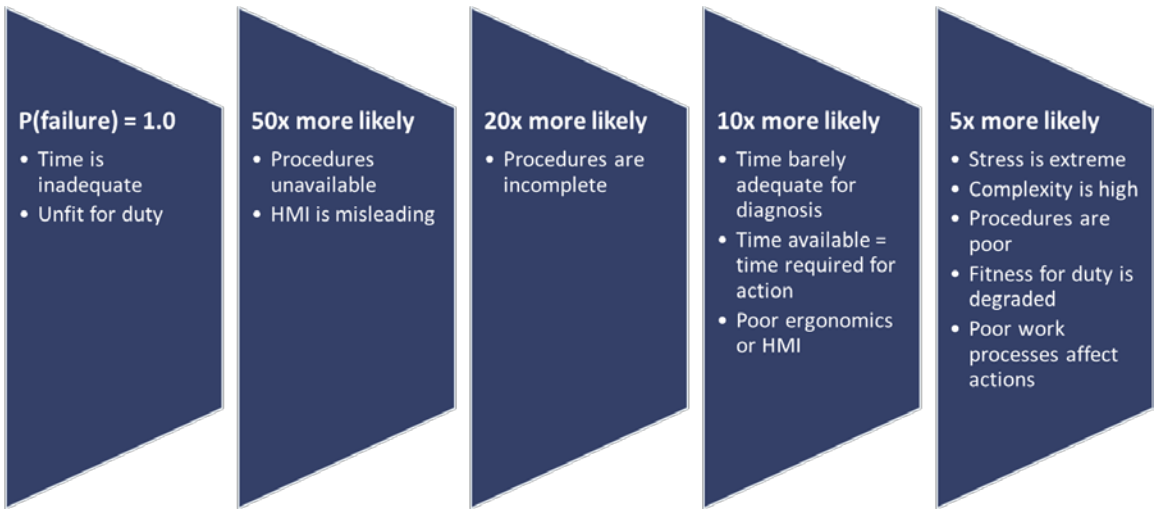

Figure 11. Performance shaping factor multipliers that increase human error probability

The Step 6 questionnaire leads the analyst to consider each PSF category one at a time (Figure 12) because only one multiplier is selected for each PSF. The PSFs are presented in the order with the greatest increase to the HEP. Statements for each PSF category correspond to applicable HFACS subcategories as a binary approach to elicit system information. HFACS subcategories conditions are presented to the analyst in an order that reveals that the greatest multiplier for the PSF which results in a worst-case scenario HEP. If the event does not have the attributes that match a greater than 1 or lesser than one multiplier, then a multiplier of 1 is assigned for the PSF.

1. Is the human mainly making decisions or taking action?		Nominal HEP of 0.01 for decisions or 0.001 for action
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		If Yes, then automatic P(failure) = 1.0, otherwise next question
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	If No, then F = 5 and move to next category, otherwise F = 1 and move to next category
3. Will there be insufficient time to diagnose and act?		If Yes, then automatic P(failure) = 1.0
	Will there be more than 50x time needed to act?	If Yes, then T = 0.01 and move to next category, otherwise next question
	Will there be between 5x-50x time needed to act?	if Yes, then T = 0.1 and move to next category, otherwise next question
	Will there be only enough time to diagnose or act?	If Yes, then T = 10 and move to next category, otherwise next question
	Will the system always be fully staffed?	If No, then T = 10 and move to next category, otherwise T = 1 and move to next category
4. Will procedures exist?		If No, then P = 50 and move to next category, otherwise next question
	Will procedures be complete?	If No, then P = 20 and move to next category, otherwise P = 1 and move to next category
	Will procedures be symptom or diagnosis oriented?	If Yes then P = 0.5 and move to next category, otherwise P = 1 and move to next category
5. Will human machine interface be misleading?		If Yes, then H = 50 and move to next category, otherwise next question
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	If No, then H = 10 and move to next category, otherwise next question
	Will the system function be designed to support the human in any adverse physical environment?	If No, then H = 10 and move to next category, otherwise next question
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?	If No, then H = 10 and move to next category, otherwise H = 1 then move to next category
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?	If Yes then H = 0.5 and move to next category, otherwise H = 1 then move to next category
6. Will the work block satisfy at least 3 of the 5 following conditions?		If Yes, then C = 1 and move to next category, otherwise next question
	a. Tasks are prioritized for the human	
	b. Diagnostic information is presented by the system	
	c. Controls and switches are clear and easily accessible	
	d. Instrumentation and warning systems are designed with the human in mind.	
	e. The system will always be fully staffed	
	Will at least 2 of the above conditions apply?	If Yes, then C = 2 and move to next category, otherwise C = 5 and move to next category
7. Will all operators be trained on and retain knowledge on this work block?		If No, then E = 10 for decisions or E = 3 for actions and move to next category, otherwise next question
	Will only operators with previous experience operate this system?	If No, then E = 10 for decisions or E = 3 for actions and move to next category, otherwise E = 1 and move to next category
8. Could any system operator ever experience extreme stress?		If Yes, then S = 5 and move to next category, otherwise next question
	Could any system operator ever experience high stress?	If Yes, then S = 2 and move to next category, otherwise S = 1 and move to next category
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		If Yes, then O = 2 for decisions or O = 5 for actions and move to next step, otherwise next question
	Will every supervisor perform and communicate continuous risk assessments?	If No, then O = 2 for decisions or O = 5 for actions and move to next step, otherwise next question
	Will organizational culture always be exceptionally good?	If Yes, then O = 0.8 for decisions or O = 0.5 for actions, otherwise O = 1 then end.

Figure 12. CRUSH Step 6 questionnaire

The questionnaire first prompts the analyst to answer the question, “Is the human mainly making decisions or taking action?” Before any failures are applied, the analyst

must decide whether the basic event resembles a diagnosis or an action. Depending on the analysis fidelity selected by the human reliability requirements team, it is possible that the event has both diagnosis and action components. The team is free to use judgment to select between the diagnosis and action HEPs. SPAR-H assigns diagnosis activities a NHEP of 0.01 and action activities a nominal HEP of 0.001. Any subsequent decisions on PSF levels are applied to the NHEP.

The next question focuses on fitness for duty. If an operator is unfit for duty, the probability of human failure is 1.0. The multi-disciplinary human reliability requirements team will document the threshold for human fitness required for acceptable function. Because human failure is guaranteed if an individual is unfit, fitness for duty is the first PSF assessed in Step 6. While the system design does not cause a human to be unfit for duty, system policies and guidelines to assess fitness for duty can exclude unfit humans from operating the system. The assessment of fitness for duty prompts a binary response to a planned aspect of the system, "Will there be protocols or controls to prevent physically or mentally unfit individuals from working?" If operators who are not physically or mentally fit are allowed to work, then the assigned HEP is 1.0 and the analysis for this basic event ends. If physically or mental unfit individuals are screened before working, a second question asks whether degraded physical mental performance is allowed: "Will there be protocols or controls to exclude individuals from working if injured, fatigued, or medicated?" The word choice in this question draws from HFACS nanocodes for the subcategories: physical problems (PC300), mental awareness (PC200), and state of mind (PC100). If the analyst answers No, then degraded performance is possible and the Fitness for Duty PSF multiplier, F, is set to 5. If the analyst answers Yes, then F is set to 1. If there is insufficient information to answer these questions, SPAR-H assigns F a nominal multiplier of 1. A conservative approach to assigning multipliers results in the identification of more system failures than if all nominal multipliers are assigned. Once criteria is met for a multiplier, the analyst moves to the next PSF for assessment.

The next question focuses on the PSF of Available Time. If there is insufficient time to diagnose or act, the probability of human failure for the work block is 1.0. Because this PSF has the possibility of guaranteed human failure, it is the second PSF assessed. The

system affects an individual's available time by presenting information given reaction time and cognition time. The assessment of available time requests a binary response to an assessment of each work block, "Will there be sufficient time to make a diagnosis and act?" If there is not enough time to make a diagnosis and act, then the assigned HEP is 1.0 and the analysis for this work block ends. Subsequent questions ask about the amount of time available to make decisions and take action. The order of questions starts with extreme conditions of extraneous time for which SPAR-H has provided relative time limits. If system design includes more than 50 times the time needed for action or at least twice the time needed for diagnosis, then the Available Time multiplier, T, is set to 0.01, which reduces the HEP. If there is not, the questionnaire asks if between 5–50 times the time needed will be provided. If this is true, then T is set to 0.1. If neither of these extreme conditions apply, the questionnaire prompts the analyst to consider if only the time needed is allotted for the diagnosis or action. If this is true, then T is set to 10. The final question for evaluating available time asks if staffing resources are guaranteed. If the system is not always fully staffed, then T is 10 because individuals are required to do multiple jobs within the allotted time. If the system will always be fully staffed and there is enough time to make a diagnosis and take action, then T is 1. Given the early development phase, much of this information may not be defined. Therefore, the multi-disciplinary human reliability requirements team must use their operational experience to judge whether the system concept provides enough time to successfully complete the function given the operational context of mission requirement and anticipated staffing levels.

The third section focuses on Procedures. If procedures do not exist, individuals do not have written guidance on how to operate the system and must rely on training or memory to complete the steps correctly. The Procedures PSF is the third PSF assessed because SPAR-H assigns one of the highest multipliers to the absence of procedures. The assessment of this PSF first asks, "Will procedures exist?" If there will not be procedures for the event, then the assigned multiplier for Procedures, P, is 50 and the analyst moves to the next PSF for analysis. If procedures exist, they may be incomplete. The next evaluation question, "Will procedures be complete?" addresses this possibility. If procedures are

incomplete, then P is 20. If procedures exist and are complete, the Procedures multiplier, P, is 1.

Ergonomics/HMI is the next PSF assessed in the questionnaire because the multiplier could be as high as 50. The questionnaire first asks, “Will HMI be misleading?” If HMI is misleading, the SPAR-H multiplier is for this PSF, H, is 50. While the question is binary, the answer is not be obvious and requires input from the multi-disciplinary human reliability requirements team. Yet, if a misleading HMI can be ruled out, the analyst can proceed to evaluate other system characteristics. A negative response to any of the following three questions results in a multiplier of 10 for the Ergonomics/HMI PSF:

- Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?
- Will the system function be designed to support the human in any adverse physical environment?
- Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?

These additional questions correspond to HFACS nanocodes for technical precondition subcategories: technological environment (PE200), physical environment (PE100), and sensory misperception (PC500) over which the system designer has the ability to affect the human interface. Otherwise, the Ergonomics/HMI multiplier, H, defaults to 1.

System factors that affect complexity are wide-ranging. For the Complexity PSF, C, multipliers range from 1 to 5. The assessment approach asks the analyst to consider a number of positive system attributes:

- Tasks are prioritized for the human.
- Diagnostic information is presented by the system.
- Controls and switches are clear and easily accessible.

- Instrumentation and warning systems are designed with the human in mind.

- The system will always be fully staffed.

If the team judges that one or none of the system attributes apply, the highest possible multiplier is assigned. If two attributes apply then C is 2. If at least three attributes are present in the system design, then the default multiplier, 1, is applied. These attributes correspond to HFACS technical precondition subcategories: technological environment (PE200), physical environment (PE100), and sensory misperception (PC500). Gertman et al. (2005) note that poor ergonomics and inadequate staffing each can increase complexity. Diagnostic information results in a reduced Complexity multiplier in SPAR-H.

Lack of experience and training can increase the HEP by a factor of 10. Two questions are presented to the analyst to determine the Experience/Training PSF multiplier, E. First, the questionnaire asks, “Will all operators be trained on and retain knowledge on this system?” If operators are not trained or if trained operators do not retain knowledge, then E is set to 10 for decision-based tasks or 3 for action-based tasks. The evaluation level in SPAR-H is “low (Gertman et al. 2005).” If operators are trained but do not have experience, the analyst answers an additional question, “Will only operators with previous experience operate this system?” If some operators do not have previous experience working on the system, then E is 10 or 3, depending on the type of task. If all operators will be experienced and trained, then E is set to 1 since experience and training do not increase the failure probability.

Stress, as a performance shaping factor, has three levels: extreme, high, and nominal. Because stress is largely an individual attribute, the word choice for this PSF asks, “Could any system operator ever experience extreme stress?” and “Could any system operator ever experience high stress?” Positive responses result in assignment of multipliers of 5 and 2, respectively, for the Stress PSF multiplier, S. Otherwise, the multiplier for nominal stress, 1, applies. Responses can be based on team judgement of the presence of non-technical HFACS preconditions: physical environment (PE100), physical

problem (PC300), state of mind (PC200), sensory misperception (PC500), mental awareness (PC100), and teamwork (PP100).

Work processes reflect organizational influences that affect system resources, work pace, and culture climate. The questionnaire first asks, "Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?" The word choice for this question considers the HFACS subcategory nanocodes: resource problems (OR000), personnel selection and staffing (OS000), policy and process issues (OP000), and climate or cultural influences (OC000). A positive response results in a Work Process PSF, W, assignment of 5 for action-based tasks or 2 for decision-based tasks; both correspond to the SPAR-H level, "poor (Gertman et al. 2005)." A negative response leads to a second question to determine the effect of supervisory actions on work processes. The question asks, "Will every supervisor perform and communicate continuous risk assessments?" This question considers the HFACS subcategory codes: planned inappropriate operations (SP000) and inadequate supervision (SI000). A negative answer results in an assignment of 5 or 2 for W, depending on the type of task. A multiplier of 1 is otherwise assigned for positive responses. However, if the analyst is able to positively answer, "Will organizational culture always be exceptionally good?" a multiplier of 0.8 can be assigned for W. The score for organization is likely the same score for all work blocks of human functions as the organization will apply to the entire system.

The final part of the Step 6 questionnaire is to calculate the HEP for the human failure event using the nominal probability selected in the first part of Step 6 and the multipliers selected for each PSF: Fitness for Duty (F), Available Time (T), Procedures (P), Ergonomics/HMI (H), Experience/Training (E), Complexity (C), Stress (S), Work Processes (W).

$$\boldsymbol{HEP = NHEP \times F \times T \times P \times H \times E \times C \times S \times W} \quad (1)$$

Following the SPAR-H method for calculating human reliability, if three or more PSFs are greater than 1, then the HEP is calculated using the equation:

$$\boldsymbol{HEP = \frac{NHEP \times F \times T \times P \times H \times E \times C \times S \times W}{NHEP \times ((F \times T \times P \times H \times E \times C \times S \times W) - 1) + 1}} \quad (2)$$

There should be an HEP calculated for each human event identified in CRUSH Step 4. Each HEP should be between 8E-6 and 1.0. The assessment team will compile the results from each work block and review them in Step 7 to form recommendations to the program office.

The CRUSH method can be used on a system concept during the requirements development phase. The method steps form the basis of a functional analysis focusing on system functions that are dependent on human interaction. These system functions are further characterized by the combinations of hardware, software, and human actions required to complete the function. Questionnaires that are based on the evaluation factors of SPAR-H and HFACS use the proposed system design and available technical specifications as input for the evaluation. Examining the results from all the work blocks, the assessment can address those blocks that have high likelihood of human error and whose completion is sensitive to variation in human roles. The questionnaires contain sufficient detail to identify system requirements that would improve the reliability of the system function. The method can also be used to compare design concepts or prototypes to anticipate human contributors to system failure.

IV. APPLICATION OF CRUSH TO ECDIS

The CRUSH method was demonstrated on an existing system as part of verification and validation of the proposed method. The verification and validation of CRUSH follow the Validation Square developed by Pedersen et al. (2000). The Validation Square examines the "internal consistency" of the logic used within the method, as well as the usefulness of the method that demonstrates its "external relevance." The ECDIS, a currently fielded system, was selected to demonstrate the CRUSH method in support of the method's verification and validation. Though there are many ECDIS systems on the market, the assessment used policy documents and operational guidance as source documents to represent requirements for the system concept, instead of evaluating one manufacturer's version of the system. This chapter describes the application of the CRUSH steps in a case study of how the ECDIS is used to support MSC navigation.

A. FAMILIARIZATION WITH SYSTEM CONCEPT: CRUSH STEPS 1 THROUGH 4

The initial CRUSH steps establish the team that will assess the system, collect information about the system concept, identify human interfaces with the system, and identify individual tasks that comprise each operator function, and model combinations of conditions and actions that result in task failure. For this case study, the CRUSH steps examined the ECDIS system functions and their use within the operating policies and procedures of the MSC organization.

1. CRUSH Step 1: Human Reliability Requirements Team

In lieu of a human reliability requirements team, various subject matter experts served as technical advisors on this thesis to provide operational perspective into current ECDIS use throughout the demonstration. The technical advisors included retired Navy Quartermasters and directors from Military Sealift Command Headquarters. The technical advisors provided perspective on MSC mission tempo, hierarchy of the MSC officers and watchstanders, and operator training and experience.

2. CRUSH Step 2: Familiarization with ECDIS Functions

The second step of CRUSH identified the primary function of the system. The revised performance standards (MSC 2006) state that the ECDIS's primary function is to "contribute to safe navigation." The scope of ECDIS defined in the revised performance standards includes display of electronic charts as well as the capability to display radar, AIS, and other data systems; facilitation of electronic chart updates; capability to plan and monitor routes; and use of alarms or indicators for system malfunction. The ECDIS is expected to perform as reliably as paper charts, which are the previous method of charting and navigation. Even in the revised performance standards, paper charts are required as a backup for ECDIS. A hierarchy view of ECDIS function shows the work blocks representing the ECDIS scope outline in the revised performance standards (Figure 13). This is a system point of view of ECDIS required functions.

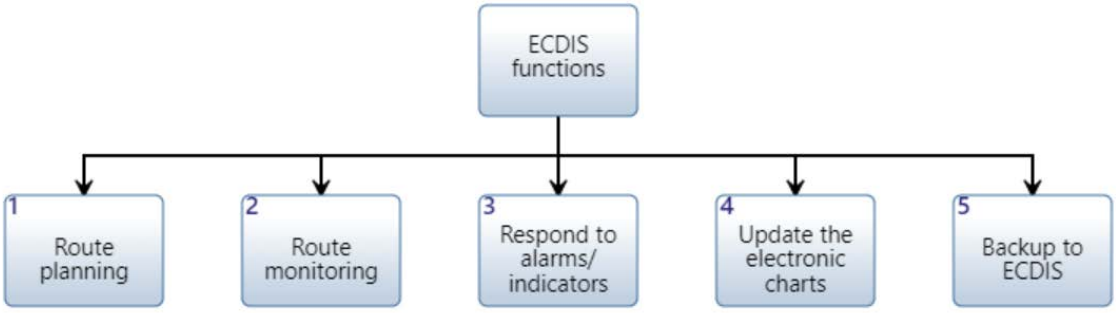

Figure 13. Hierarchy chart for the ECDIS system human functions

Together, these ECDIS functions aid the mariner by integrating data sources and providing charting and radar information with alarms that call dangerous conditions to the mariner's attention. This results in safer navigation.

3. CRUSH Step 3: Human Interfaces

Given the ECDIS functions described in the IMO MSC revised performance standards, CRUSH Step 3 identified the human actions and decisions that are required

by each system function. This necessitated an understanding of each work block as well as each operator role set by the MSC organization. Each work block from Figure 13 is decomposed into specific actions and decisions that must all be completed for the work block to be accomplished successfully (Table 1).

Table 1. Decomposition of work blocks used in ECDIS concept review

Work Block	Human Function
1	**Route planning**
1.1	Plan the route
1.2	Input the route
1.3	Change the route
2	**Route monitoring**
2.1	View the route
2.2	Change the view
2.3	Interpret the data
3	**Respond to alarms/indicators**
3.1	Sense the alarm/indicator
3.2	Understand the alarm/indicator
3.3	Take action
3.4	Reset the alarm/indicator
4	**Update electronic navigation charts**
4.1	Retrieve new charts
4.2	Install new charts
5	**Act as backup to ECDIS**
5.1	Paper charts
5.2	Paper logs
5.3	Redundant navigation system
5.4	Redundant sensors
5.5	Alternate power source

Action diagrams show the steps that comprise the ECDIS functions in Table 1. Route planning requires the navigation officer to plan the voyage route, input the voyage route, and change the route as needed (Figure 14). For route monitoring, the operator views the charts, changes the layers in each view, and changes the viewing scale and the day/night brightness settings, as needed. The operator must interpret the data viewed in

order to take the next navigation action, which could be to communicate the current ship position to the watch office or plot a paper fix (Figure 15).

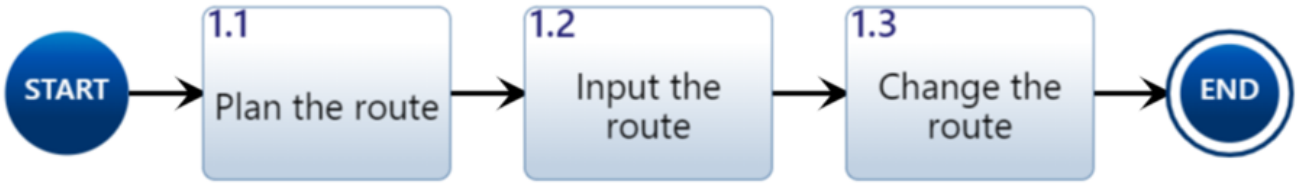

Figure 14. Action diagram for route planning

Figure 15. Action diagram for route monitoring

Alarms can occur during route planning and route monitoring to warn of a dangerous condition or system malfunction. Before an operator can act on an alarm, he must know that the alarm is sounding and what the alarm means (Figure 16). He must also be able to clear the alarm when the alarm condition is resolved.

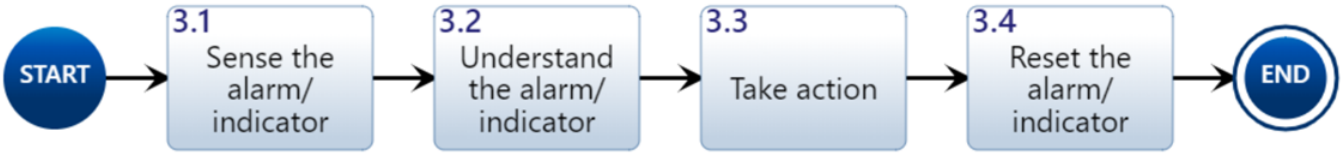

Figure 16. Action diagram for response to alarm

The update of electronic charts requires the ability to retrieve the charts before the charts can be installed (Figure 17).

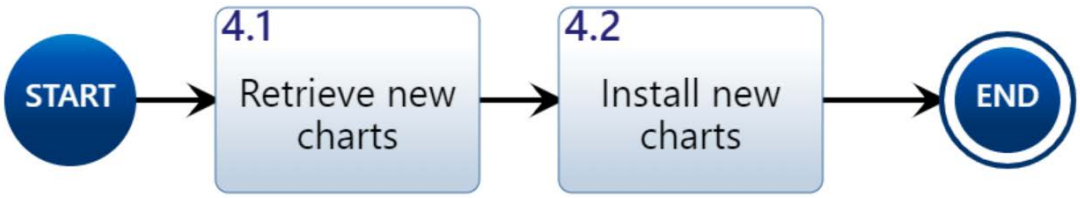

Figure 17. Action diagram for electronic chart update

An action diagram was also created for ECDIS backup, which is highlighted in the scope of the revised performance standards. While backup systems to ECDIS are not controlled by ECDIS designers, having a backup to ECDIS is a performance requirement. The action diagram shows the different roles assumed by operators, supervisors, and organizations for various backup system options (Figure 18). The IMO considers paper charts and paper logs kept by the navigation officer to be the backup for ECDIS. The ship command structure is responsible for maintaining sensor systems on board that can be used to provide PNT information to the watchstander. The ship command structure is also responsible for maintaining electric power to all systems onboard the ship; the IMO revised performance standard includes operational requirements for an alternate power source. In addition, the action diagram for ECDIS backup models a second navigation system in the event the organization chooses to install a redundant ECDIS system as a backup.

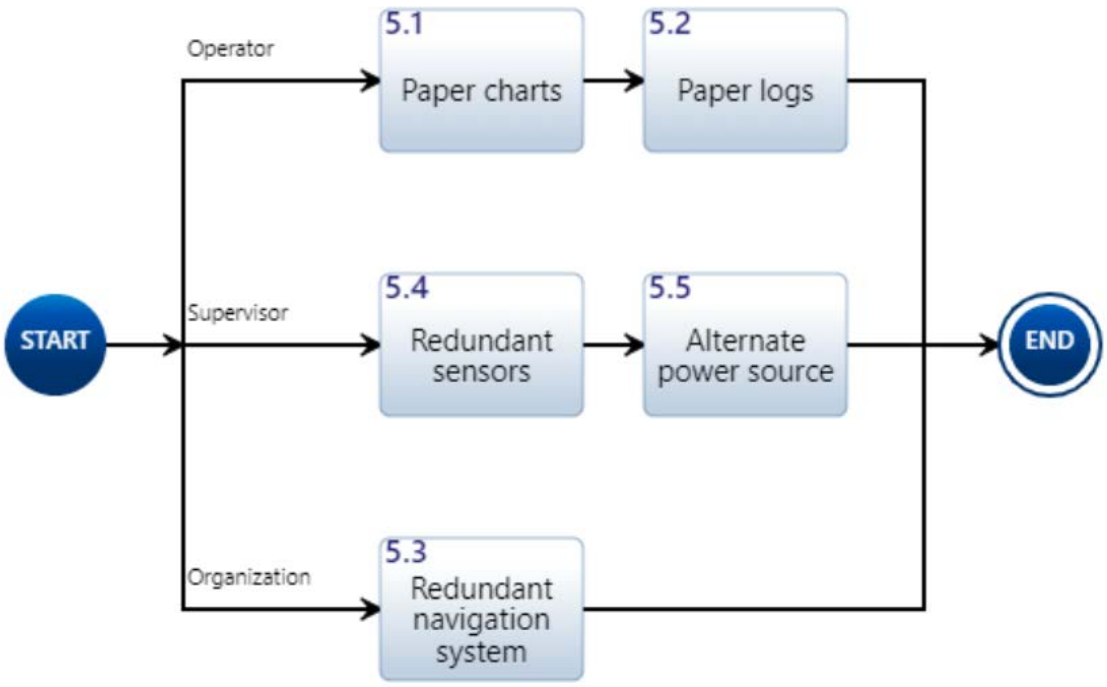

Figure 18. Action diagram for ECDIS backup

The tasks depicted by each work block are used multiple times during ECDIS operation as needed, though each block was only analyzed once in this thesis. The action diagrams from CRUSH Step 3 informed the fault tree logic of CRUSH Step 4 because fault tree success is dependent upon successful completion of all preceding work blocks.

4. CRUSH Step 4: Functions for each human interface

In the next CRUSH step, this thesis inspected the ECDIS concept for combinations of hardware, software, and human failures, as well as environmental and technological conditions that result in failure of each work block. Successful completion of a required prerequisite step was modeled in the fault tree logic. For instance, electronic charts must be successfully retrieved before they are installed.

The fault trees modeled human actions and conditions that, in combination with the system design, prevent ECDIS from achieving the desired result or completing the desired action. The trees focused on human failures and suboptimal knowledge, skills, and abilities. An operator's lack of knowledge and recall of ECDIS operation was

modeled as a failure condition. An ECDIS that is unable to perform to the level needed by the operator, despite operating as designed, was modeled as a failure condition because it reflects a design flaw rather than a hardware or software failure.

The fault trees modeled in this thesis assumed that the ECDIS system hardware and software operate as designed. That is, the hardware and software are 100% reliable and available. However, fault trees for recoverable failures, such as a redundant system to ECDIS or an alert to a recoverable system malfunction, included hardware failures as basic events that are required in the failure pathway for these trees. The Step 4 fault trees also assumed the data that ECDIS passes to the operator is correct. In practice, lookouts use binoculars to scan the environment and are in constant communication with the ECDIS operator. They provide redundancy by confirming information from ECDIS. The performance of the lookouts is outside the scope of this thesis.

The fault trees do not include probabilities, and therefore resulting failure paths formed with the logic will not have any values. The fault trees are still useful because they detail the conditions that could result in failure. Where applicable, the basic events referenced HFACS conditions that are used by the CRUSH Step 5 questionnaire. The probability of human error is determined in CRUSH Step 6.

a. Fault Trees for Failure to Plan Route

Figure 19 shows the fault trees for the navigation officer voyage planning role. Rectangles depict top level failures. Failures to update electronic charts were included in the fault tree logic for route planning. Though the navigation officer can update the electronic navigation charts at any time, MSC requires that charts be updated prior to each voyage (Alexander Halliday, personal communication, July 1, 2020). This ensures that the most recent charts are used. In order to plan the route, the navigation officer must be able to view the charts on the monitor and understand the information. Next, the navigation officer views the updated charts and inputs a route. The route can be changed if needed. Only failures between the ECDIS and the human interface were modeled. For example, if the captain has not determined the destination, the navigation

officer will not be able to plan the route. However, this is not a failure between the ECDIS and the navigation officer.

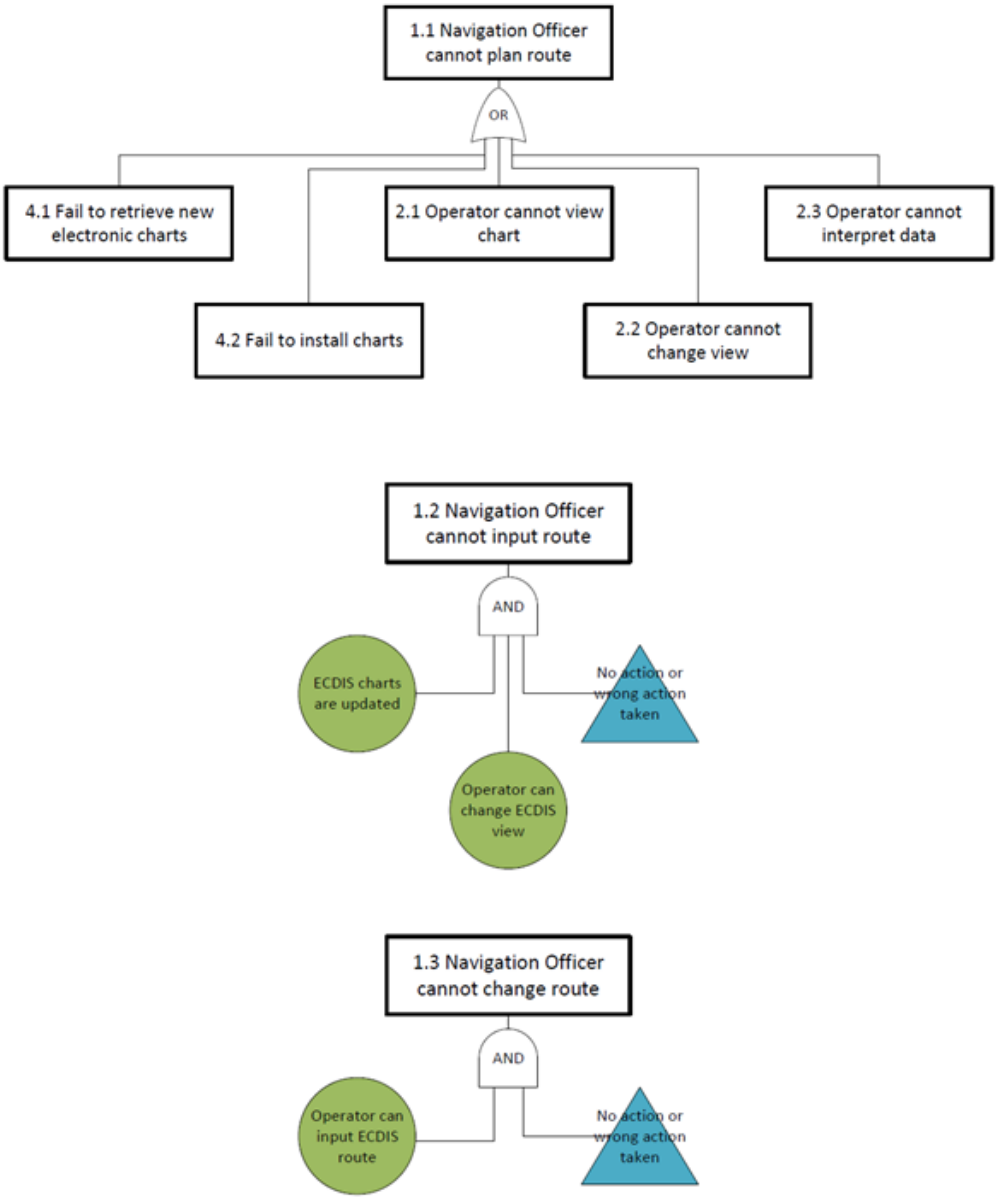

Figure 19. Top-level fault trees for the route planning work blocks

In this thesis, colors are used to quickly identify and differentiate information. Circles denote events at the lowest level of elaboration. Green circles denote basic events

that are successfully completed prerequisite conditions. White circles represent basic events which are failures or contributors to failure specific to the failure tree. Basic events can be further divided into increasing levels of detail, but in the context of this application, decomposition only adds value if the additional details can be useful in shaping the design requirements or improving upon the system concept. Otherwise the amount of details can be overwhelming to a management team. During the concept development phase there is no physical system architecture to evaluate, so the analysis may be limited until the program establishes system performance requirements and physical architecture.

Triangles represent transfer gates to sub-trees that are shared by two or more top level events. These sub-trees have similar logic and contributors. For instance, the fault tree model for route planning used similar logic to the fault tree for route monitoring. The navigation officer must manipulate the screen views while viewing and inputting a route in ECDIS similar to ECDIS operators who manipulate the screen views to monitor the ship's position. Transfer gate triangles in this analysis are blue. The top level events that the triangles reference are also blue with titles in all capital letters to better identify that the tree is referenced in multiple places (Figure 20). Figures 21 through 24 show the fault trees that are referenced in Figure 20.

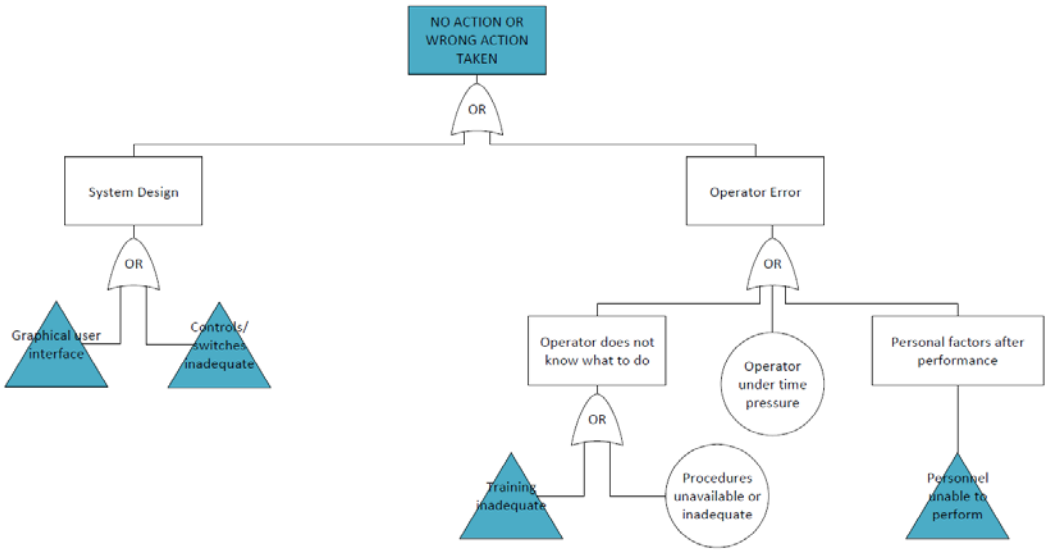

Figure 20. Transfer gate fault tree for "No action or wrong action taken"

Basic events that comprise failures of the graphical user interface (Figure 21) and controls and switches (Figure 22) reflect examples of design criteria from Military Standard 1472, *Design Criteria Human Engineering* (DOD 2019) that should have been incorporated into the ECDIS design. The basic events also reflect HFACS nanocodes: "Instrumentation and Warning System Issues (PE202)," "Visibility Restrictions (Not Weather-related) (PE203)," and "Controls and Switches are Inadequate (PE204)."

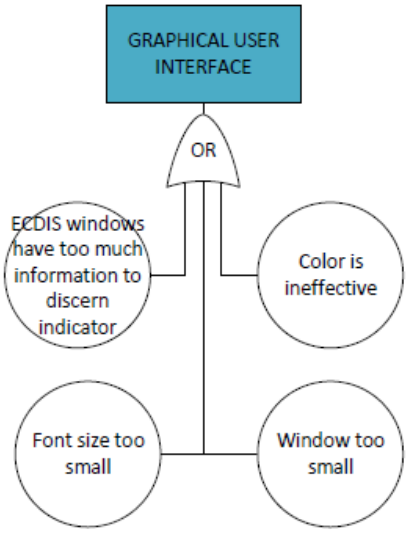

Figure 21. Transfer gate fault tree for "Graphical use interface"

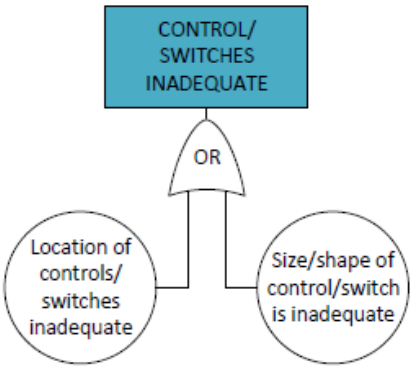

Figure 22. Transfer gate fault tree for "Controls/switches inadequate"

Failure to complete or retain information from training is a sub-tree that is used in multiple fault trees (Figure 23). Lack of training is cited by both SPAR-H and HFACS as contributing to failure. Human Factors Analysis and Classification System nanocodes that reference training are "Technical or Procedural Knowledge Not Retained After Training (PC109)," "Authorized Unqualified Individuals for Task (SV004)," "Authorized Unqualified Individuals for Task (SI003)," and "Organizational (Formal) Training Is Inadequate or Unavailable (OP004)."

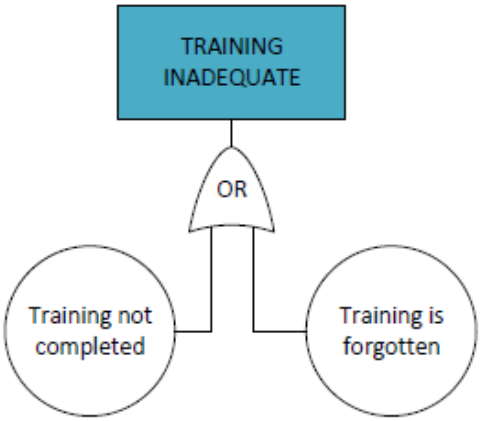

Figure 23. Transfer gate fault tree for "Training inadequate"

Personnel unable to perform is another sub-tree that is used in multiple fault trees (Figure 24). This sub-tree refers to an individual's personal factors that contribute to failure. These factors map to HFACS subcategories for preconditions: "Physical Problem (PC300)," "State of Mind (PC200)," and "Mental Awareness (PC100)."

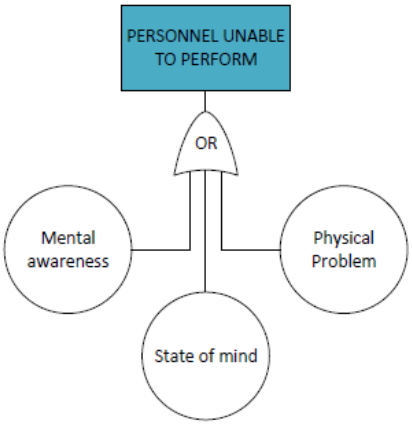

Figure 24. Transfer gate fault tree for "Personnel unable to perform"

b. Fault Trees for Failure to Monitor Route

The route monitoring fault trees considered that the operator cannot view the charts on the ECDIS display, cannot change the view on the charts, and cannot understand the information on the display (Figure 25). The route monitoring fault trees

reference the same combinations of failures from the route planning fault tree, namely failures of the graphical user interface (Figure 21), controls/switches (Figure 22), training (Figure 23), and personnel (Figure 24). In addition, a sub-tree details how design of the ECDIS hardware may not be adequate for the operator (Figure 26).

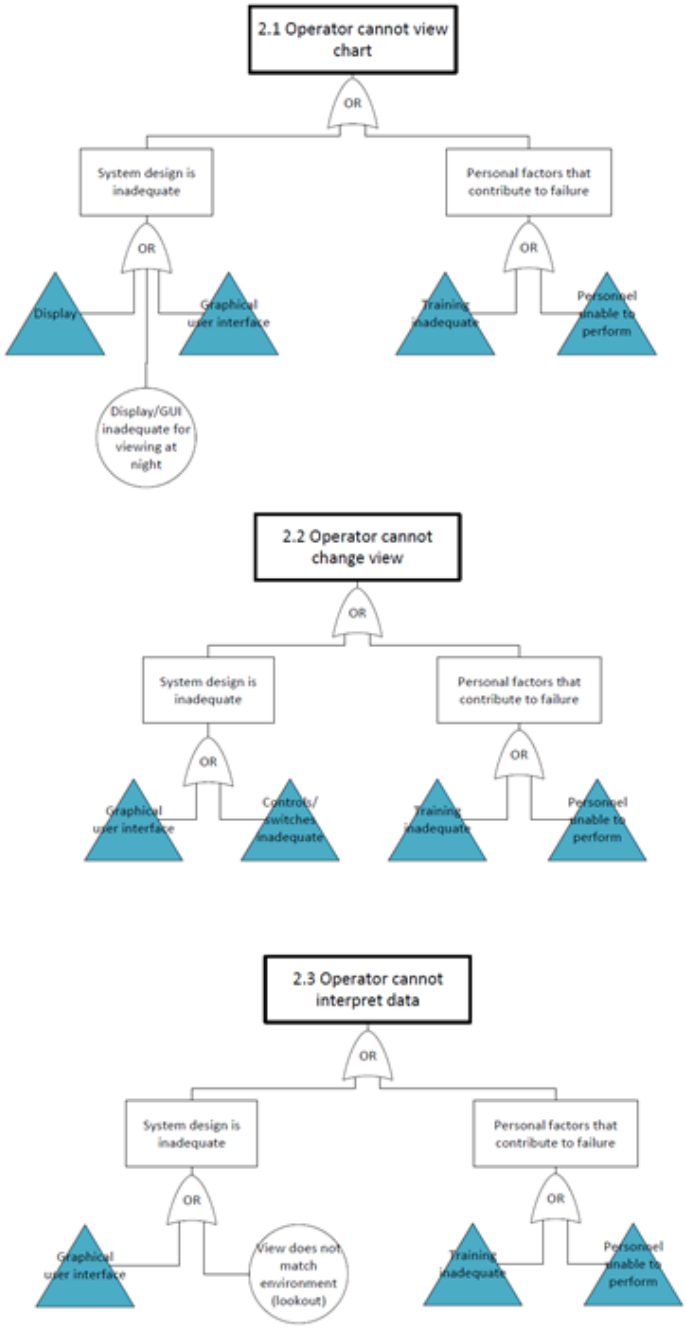

Figure 25. Top-level fault trees for the route monitoring work blocks

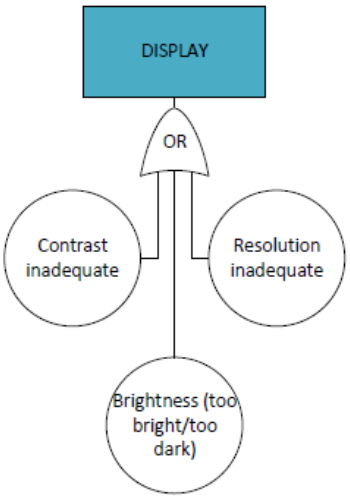

Figure 26. Transfer gate fault tree for failure of ECDIS display hardware design

c. Fault Trees for Failure to Respond to Alarm/Indicator

Figure 27 shows the combinations of events associated with a failure to sense the alarm/indicator. The logic assumed that alarms and indicators can be audible or visual. The logic also assumed that if the operator is in another location, he may not hear the alarm. Failure to understand the alarm requires that the alarm is first sensed (Figure 28). Failure to take action requires that the alarm is first understood (Figure 28). This thesis assumed that the logic required to clear the alarm is the same as the logic to take action in acknowledgement of an alarm. Both require the operator to first sense and understand the alarm before performing a combination of steps to complete an action.

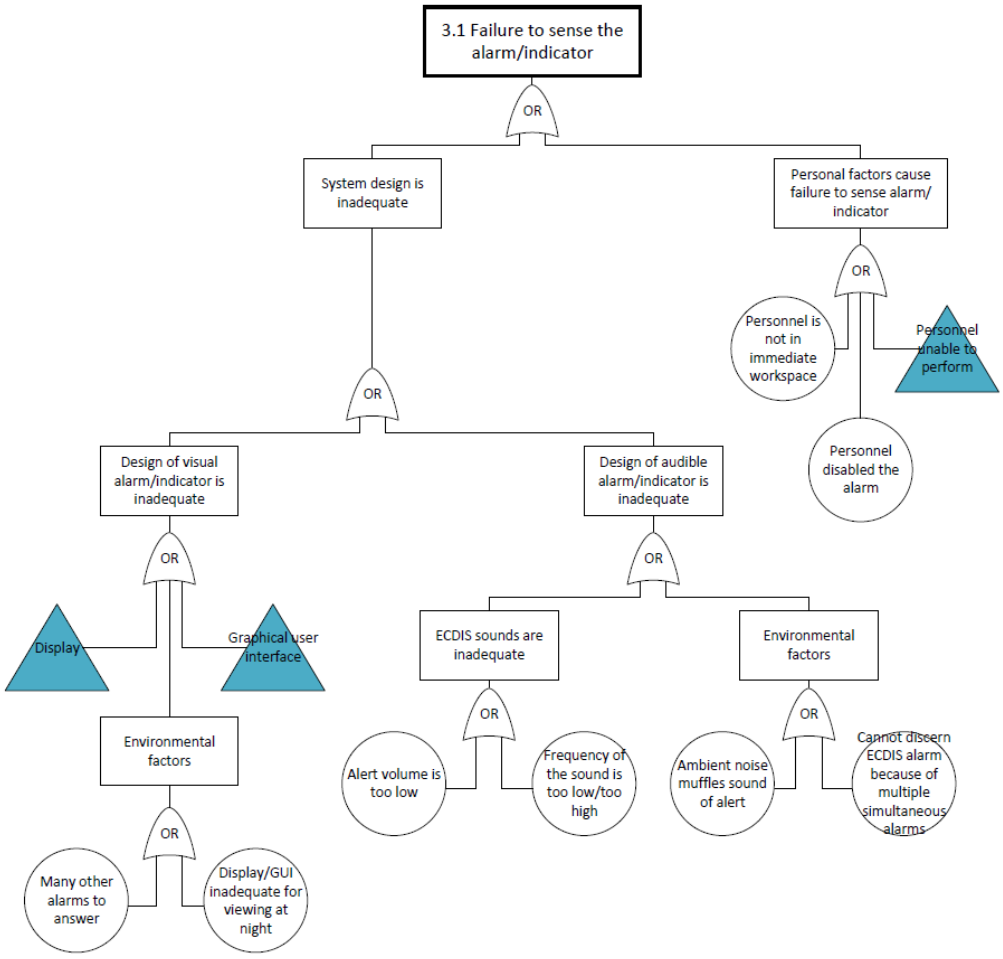

Figure 27. Top-level fault tree for the “Failure to sense the alarm/indicator” work block

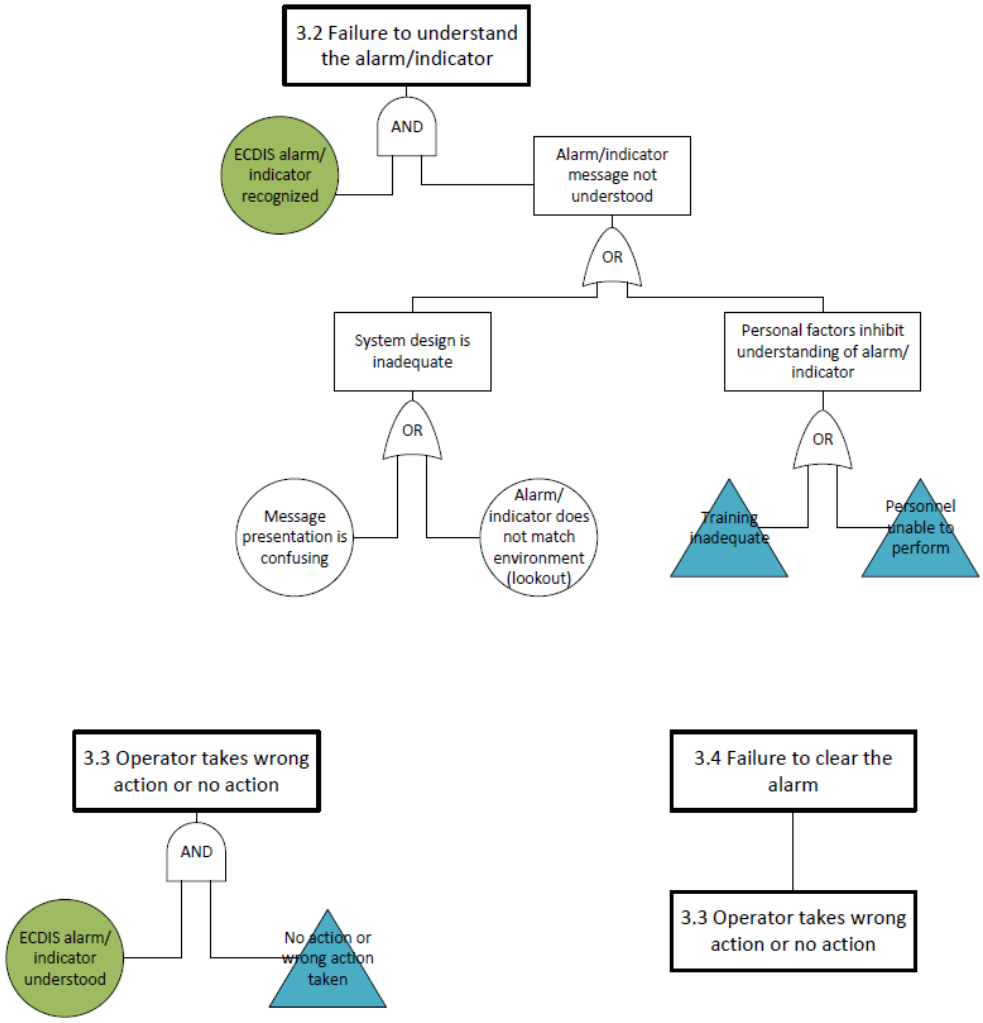

Figure 28. Top-level fault trees for the failures to respond to alarm/indicator work blocks

d. Fault Trees for Failure to Update Electronic Charts

Figure 29 shows logic combinations for the work blocks associated with updating electronic charts. Retrieval of electronic charts assumed that an information network is operational in order to facilitate download. Failures to maintain the network were included in the fault tree to indicate that supervisors and organizations have specific roles in the successful operation of ECDIS functions. Basic events referenced HFACS nanocodes for "Failure to Provide Adequate Manning or Staffing Resources (OS002)," "Pace of Ops-

Tempo or Workload (OP001),” and “Failure to Remove Inadequate or Worn-out Equipment in a Timely Manner (OR005).”

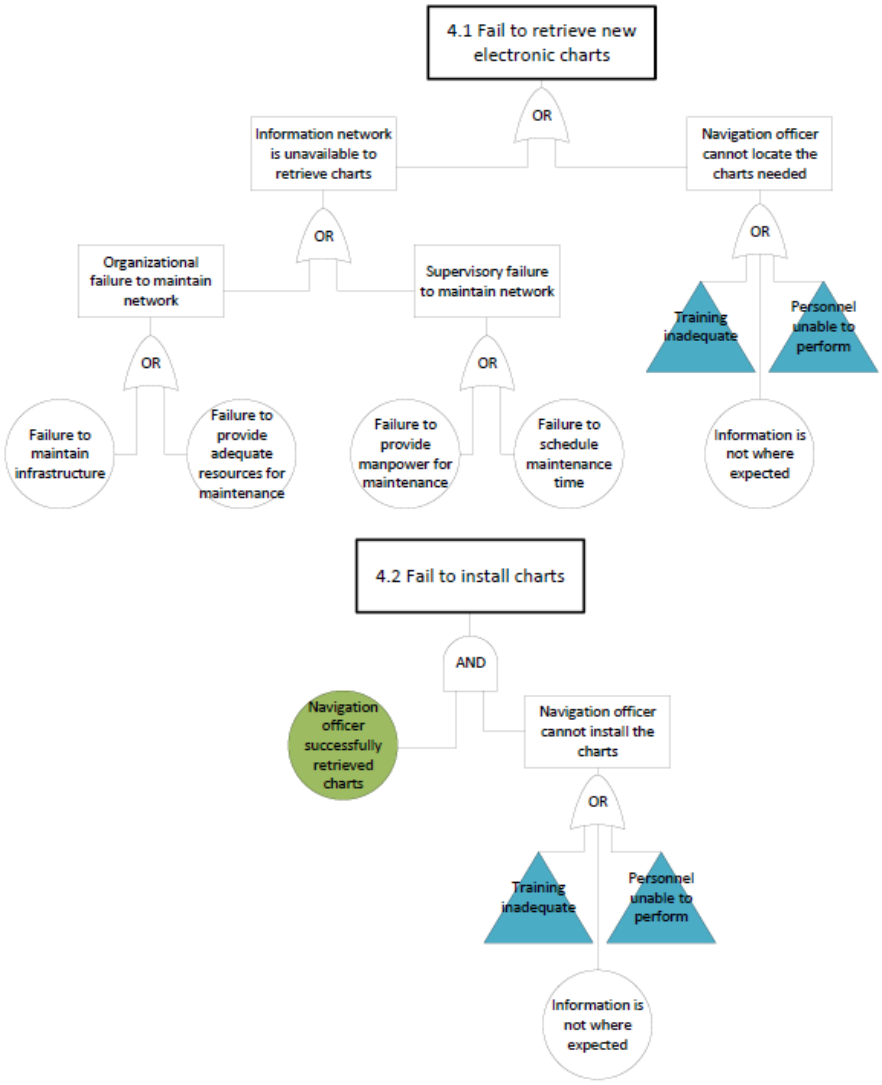

Figure 29. Top-level fault trees for electronic chart update work blocks

e. Fault Trees for Failure to Backup ECDIS

The fault trees for the work blocks representing ECDIS backup systems include a basic event that represents unavailability of the ECDIS (Figure 30). Gray circles depict a

hardware unavailability which, in combination with a human failure, prevents task completion.

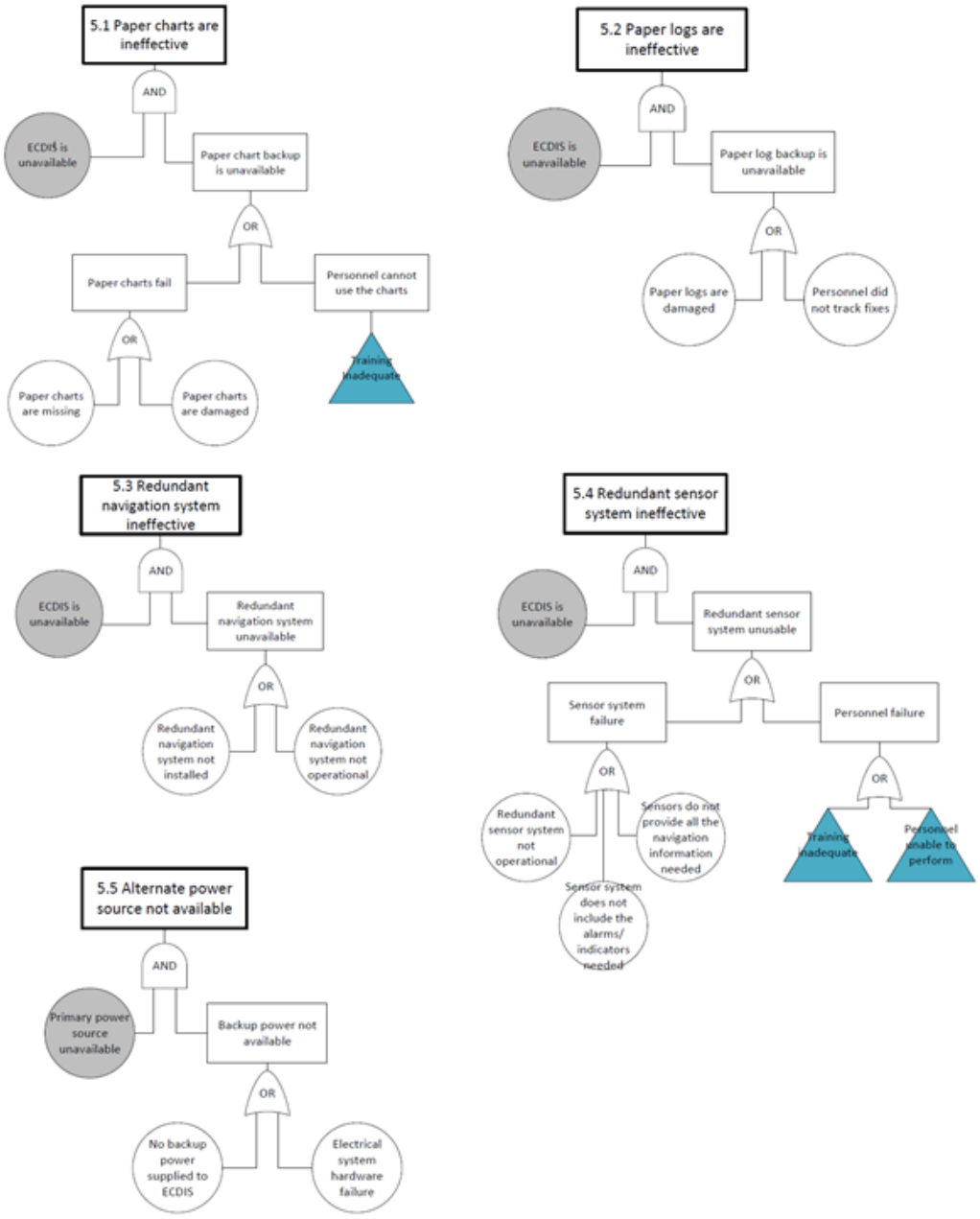

Figure 30. Fault tree for the ECDIS backup work blocks

f. Fault Trees for Inadvertent Shutdown of ECDIS

An additional top-level fault tree depicts inadvertent shutdown of ECDIS either by inadvertent operator action or by an operator's actions triggering an ECDIS shutdown or malfunction (Figure 31). This failure was not reflected in the action diagrams because the action diagrams reflect specific ECDIS system functions. Nevertheless, the inadvertent shutdown of ECDIS was captured as a work block going forward. This fault tree modeled both an operator action that causes ECDIS to shut down when not expected and a shutdown due to a recoverable system malfunction.

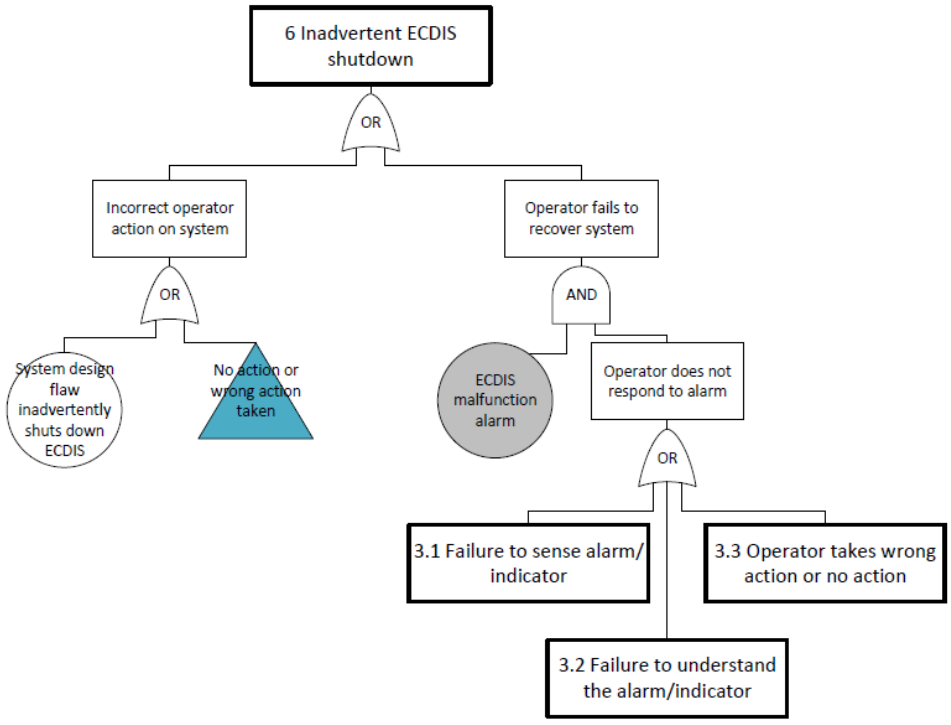

Figure 31. Inadvertent ECDIS shutdown fault tree

Because the ECDIS has been fielded for a number of years, examples of maritime accidents involving the ECDIS system exist. Often the accidents have more than one contributing factor. The Malta-flagged chemical tanker, *OVIT*, ran aground in 2013 after the officer of the watch failed to check a junior officer's unsafe voyage plan and the crew

had disabled the audible alarms (Marine Accident Investigation Branch [MAIB] 2015). The Spanish-flagged cargo ship, *MUROS*, ran aground after the crew had inactivated all audible alarms, which they found to be a distraction (Fukuoka 2019). The alarms would have alerted the crew to navigational safety hazards such as shallow water. The bridge team also viewed the monitored the route in "standard view" which did not show sufficient detail for safe passage through the strait (MAIB 2017). The Nautical Institute (2009) identified a number of different ferry groundings that resulted from improper settings of route watch vectors, display scales, depth contour settings, and depth alarms. These causes were traced back to a lack of training because these are basic topics covered in a training course (The Standard Club 2015). Integration of ECDIS on a bridge was also cited in an accident. An officer of the watch was unable to see the visual alarms on the ECDIS to his right because he was watching the ship traffic directly ahead of him (Nautical Institute 2014). This resulted in grounding of the bulk carrier. A German-flagged cargo carrier that did not sail with updated electronic charts ran aground because the electronic charts did not include the sailing directions found on paper charts (Nautilus International 2020). These mishaps lend credibility to the human failures selected for the fault trees.

The focus of CRUSH Step 4 was the identification of combinations of hardware, software, human, and environment conditions that could cause ECDIS function failures. The next CRUSH step focused specifically on the operator at the controls, the supervisor, and the organization. Many of the human actions and conditions assessed in Step 5 were included as basic events in the Step 4 fault trees.

B. ASSESSING SYSTEM RESILIENCE: CRUSH STEP 5

The Step 5 questionnaire posed questions reflecting the major HFACS categories Unsafe Acts, Preconditions to Unsafe Acts, Unsafe Supervision, and Organizational Influences (Shappell and Wiegmann 2000). The results of the questionnaire showed the conditions and categories of conditions that negatively affect completion of each work block. The basic events from CRUSH Step 4 provided input to CRUSH Step 5. If a questionnaire condition reflected a fault tree basic event, was plausible, or was cited as a factor in an ECDIS-related accident, the answer was marked Yes for the criterion. The

response did not evaluate the likelihood that the condition will exist. In CRUSH Step 5, if the potential for the condition existed, it was presumed the condition existed; the presumed probability of each condition is 1.0. In the calculation of human error probability for each work block in CRUSH Step 6, the human reliability requirements team did not assume each presented condition will occur. The team drew upon previous operational experience to judge the likelihood of each Step 6 question. This is a key difference between Steps 5 and 6. This is also a reason that the composition of the human reliability requirements team is important to the CRUSH process.

1. CRUSH Step 5 Question 1

The Step 5 questionnaire began with a question regarding operator fitness: "Can an operator who is unfit for duty prevent the work block from being completed?" This question led the evaluation team to consider the influence the operator role has on system performance and also determine the threshold conditions for fitness for duty. The ECDIS requires operators to view electronic charts, manipulate the chart views to extract geographical information, and interpret chart data to avoid dangerous conditions. This thesis found that the operator's present physical and mental fitness is required for successful task completion of all work blocks.

2. CRUSH Step 5 Question 2

The second question in Step 5 asked, "Can the following unsafe acts prevent the work block from being completed?" The question also included sub-parts to detail the types of unsafe acts that could apply:

a. Wrong decision or no decision

b. Wrong action or no action

c. Violation of known procedure.

Because navigation, charting, and steering are not automated, system success is dependent on human operators. The work blocks require an operator to make decisions and perform an action. In addition, the route planning tasks must adhere to a known safety management system procedure. Each of these questions was answered affirmatively for

route planning, route monitoring, response to alarms/indicators, and chart update. Inadvertent shutdown of ECDIS was proposed to result from an inadvertent operator action. For the ECDIS backup work block, operator performance on non-ECDIS systems could not be established because the extent of the involvement required by the ECDIS operator is unknown.

3. CRUSH Step 5 Question 3

The third question asked, "Can the following non-technical preconditions prevent the work block from being completed?" This question was followed by examples of non-technical conditions:

a. Physical environment negatively affects operator action or decision

b. Individual's medical or physiological condition

c. Individual's personality traits, psychosocial problems, psychological disorders, or inappropriate motivation

d. Individual's sensory inputs (visual, auditory, or vestibular) create a misperception of an object, threat or situation

e. Individual's attention management or awareness negatively affects the perception or performance of individuals

f. Interactions among individuals, crews, and teams.

This thesis assumed that all ECDIS equipment is located on an enclosed, climate-controlled bridge. However, the ship is still subject to variable sea-state conditions. Lighting conditions on the bridge will also vary by design, maintenance, and location of the ECDIS. Therefore, the potential for an adverse physical environment still exists. The tasks are heavily dependent upon receiving visual information from a graphical user interface, therefore many of the conditions affecting judgement and sensory perception apply, including conditions that increase mental and physical stress. Sensing and responding to alarms require perception, comprehension and interpretation. Route monitoring tasks require attention over the eight-hour shift, so attention management and awareness are essential. As a result, Questions 3b through 3e were answered affirmatively.

In response to Question 3f, each task is completed by a single individual who, as the watch officer, has supervisory influence over other watchstanders on the bridge. While teamwork is not required to plan or monitor the ECDIS route, teamwork was acknowledged for response to alarms since the operator may coordinate the alarm response with another watchstander.

4. CRUSH Step 5 Question 4

The next question addressed supervisory influences on the ECDIS operator and operational use of the system: "Can the following examples of poor supervision prevent the work block from being completed?" This question was followed by examples of poor supervision:

a. Supervisor willful disregard of instructions or policies

b. Supervisor failure to recognize and control risk

c. Inappropriate or improper supervision

d. Supervisor failure to provide guidance, training, or oversight.

The assessment of supervisory conditions considered the actions of the master and the watch officer. The master is the navigation officer's senior officer. Failures of the master as a supervisor include improper settings for watch vectors, failures to review personnel qualifications, and failure to review the planned voyage route. These failures were considered failures of oversight for Question 4d. During the voyage, the watch officer monitors the ECDIS in addition to his duties as watch officer. The second officer and two third officers each serve as watch officer for an eight-hour shift (Alexander Halliday, personal communication, July 8, 2020). Because it was previously judged that the ECDIS operator was subject to individual failures in Question 2, this thesis assumes that he could also commit supervisory failures as the watch officer.

5. CRUSH Step 5 Question 5

The final question in Step 5 focused on organizational influences that affect the ECDIS operator and ECDIS system support: "Can the following examples of poor

organizational influence prevent the work block from being completed?" This question was followed by examples of organizational influence:

a. Deficient or inadequate resources

b. Personnel selection and staffing

c. Policy and process issues, including pace and workload, training, and guidance

d. Organizational culture influences on individual actions.

Major organizational influences for ECDIS are limited to staffing and training of the navigation officer and maintenance of the information network to allow access to new electronic charts. With regard to ECDIS backup, organizational culture must support the use of paper charts and paper logs even as electronic charting is used as the main system for navigation. For additional navigation support, senior leaders must maintain the ship infrastructure that is includes sensor systems, alternate power sources, and installation of a redundant ECDIS system.

6. CRUSH Step 5: ECDIS Resiliency

The results from CRUSH Step 5 found that completion of ECDIS functions are impacted by individual actions and non-technical preconditions that affect an individual's judgement, perception, and awareness. The ECDIS is operated by a single individual who may coordinate alarm response with other watchstanders. The ECDIS is located in enclosed, climate-controlled area yet is subject to variable sea-state conditions. The results from Step 5 also found that the ECDIS operator is also subject to supervisory and organizational influences. The watch officer operates ECDIS in addition to performing supervisory duties during his shift. Organizational influences drive pace, personnel selection, and culture. Figure 32 shows summary results from CRUSH Step 5. Detailed CRUSH Step 5 results for all work blocks are located in Appendix B.

		1 Route Planning	2 Route Monitoring	3 Respond to Alarms/ Indicators	4 Update Charts	5 Backup ECDIS	6 Inadvertent Shutdown
1. Can an operator who is unfit for duty prevent the work block from being completed?		Yes	Yes	Yes	Yes	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?							
	a. Wrong decision or no decision	Yes	Yes	Yes	Yes	No	No
	b. Wrong action or no action	Yes	Yes	Yes	Yes	No	Yes
	c. Violation of known procedure	Yes	Yes	Yes	Yes	No	No
3. Can the following non-technical preconditions prevent the work block from being completed?							
	a. Physical environment negatively affects operator action or decision	Yes	Yes	Yes	Yes	Yes	Yes
	b. Individual's medical or physiological condition	Yes	Yes	Yes	No	No	No
	c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate	Yes	Yes	Yes	No	No	No
	d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	Yes	Yes	Yes	No	No	No
	e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes	Yes	Yes	Yes	Yes
	f. Interactions among individuals, crews, and teams	No	No	Yes	No	Yes	No
4. Can the following examples of poor supervision prevent the work block from being completed?							
	a. Supervisor willful disregard of instructions or	Yes	Yes	Yes	Yes	No	No
	b. Supervisor failure to recognize and control risk	Yes	Yes	Yes	Yes	No	No
	c. Inappropriate or improper supervision	Yes	Yes	Yes	Yes	No	No
	d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes	Yes	Yes	No	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?							
	a. Deficient or inadequate resources	No	No	No	Yes	Yes	No
	b. Personnel selection & staffing	Yes	Yes	Yes	Yes	Yes	Yes
	c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes	Yes	Yes	Yes	Yes
	d. Organizational culture influences on individual	Yes	Yes	Yes	No	No	No

Figure 32. CRUSH Step 5 questionnaire results for ECDIS functions

C. CALCULATING HUMAN ERROR POTENTIAL: CRUSH STEP 6

The Step 6 questionnaire evaluated the ECDIS system concept against the SPAR-H performance shaping factors: available time, fitness for duty, procedures, human-machine interface, complexity, training and experience, stress, and work processes. All PSF evaluation levels and multipliers used in the Step 6 evaluation are unchanged from those in SPAR-H (Gertman et al. 2005). The results of this step show the ECDIS attributes that increase the probability of human error and a calculated probability of human error for each task.

1. CRUSH Step 6 Question 1: Decision and Actions

The first question of CRUSH Step 6 asked, "Is the human mainly making decisions or taking action?" Each work block was considered to be either a decision or an action (Table 2). Following the SPAR-H guidance discussed in Chapter II, the starting HEP for a

decision is 0.01; the starting HEP for an action is 0.001. Work blocks for the systems that backup ECDIS were not scored in this section because their operation and support is outside the scope of ECDIS; there are no ECDIS requirements for these backup systems beyond that they are available.

Table 2. ECDIS Work Blocks: Decisions and Actions

Work Block		Decision	Action
1.1	Plan the route	X	
1.2	Input the route		X
1.3	Change the route		X
2.1	View the chart	X	
2.2	Change the view		X
2.3	Interpret the data	X	
3.1	Sense the alarm/ indicator	X	
3.2	Understand the alarm/ indicator	X	
3.3	Take action		X
3.4	Clear the alarm		X
4.1	Retrieve new charts		X
4.2	Install new charts		X
6	Inadvertent ECDIS shutdown		X

2. CRUSH Step 6 Question 2: Fitness for Duty

The second Step 6 question asked, "Will operators who are not physically or mentally fit for duty always be prevented from working?" When the answer for a work block was Yes, a follow-on question was presented: "Will operators always be excluded from duty if injured, fatigued, or while medicated?"

Watch officer schedules on MSC ships are set at eight hours on, 16 hours off. This schedule allows for large blocks of time to rest and attend to personal matters, but watchstanders could still be fatigued. This thesis assumes that a superior officer will remove a person who is physically or mentally unfit. The master and chief mate do not stand a watch but may be on the bridge at any time. In their absence, the watch officer is the superior officer. Conservatively, this thesis assumes that the watch officer will work if he feels he is able to do so. There are three allowable level for fitness for duty regardless

of whether the work block is a decision or an action: “unfit,” with a probability of failure of 1.0; “degraded fitness,” with a multiplier of 5; and “nominal,” with a multiplier of 1 (Gertman et al. 2005). The assessment of fitness for duty matched the criteria for a value of 5 because there is potential for the watch officer to be fatigued. This multiplier was applied across all work blocks because all operators have similar shift schedules and similar responsibilities.

3. CRUSH Step 6 Question 3: Available Time

The following questions assessed whether there is sufficient time to perform each ECDIS task:

- Will there be insufficient time to diagnose and act?
- Will there be more than 50x time needed to act?
- Will there be between 5–50 times the time needed to act?
- Will there be only enough time to diagnose or act?
- Will the system always be fully staffed?

A voyage will not occur without an approved navigation plan. The master allows the navigation officer sufficient time to plan and input the route, as well as update the necessary electronic charts prior to departure. This thesis assumed there is time to plan the route, input and review the route, and to make corrections before the master approves the planned route. For route monitoring, fixes are taken every 30 minutes during open ocean sail and as frequently as two minutes in restricted waters. Given that the IMO revised performance standard requires the standard display to be accessible by a single button push and route monitoring to be accomplished in a “convenient and timely manner (MSC 2006),” there is sufficient time to cycle through the chart views multiple times for situational awareness. Given the ECDIS default safety contour of 30 meters, the ECDIS alarm setting allows the operator enough time to understand what is needed from ECDIS, determine how to interact with ECDIS, and perform the necessary action during a voyage when safety parameters are set correctly.

The questions evaluating available time are presented in an order such that, once a condition has been met, subsequent questions are not assessed because all other multipliers are lower than for the met condition. Insufficient time to diagnose and act results in automatic failure probability of 1.0. More than 50 times the time needed to act results in a multiplier of 0.01; between five and 50 times the time needed to act results in a multiplier of 0.1. If there is only enough time to diagnose or act, the multiplier is 10. If none of the previous conditions is satisfied, a final question asks if the work block will always be fully staffed. If the work block will not be fully staffed, the assigned multiplier is 10; otherwise the assigned multiplier for available time is 1. For all conditions, there is more than sufficient time needed to complete the task. The assigned multiplier for available time is 0.1 for all work blocks because there is time to recover from errors.

4. CRUSH Step 6 Question 4: Procedures

The ECDIS procedures were assessed against the questions:

- Will procedures exist?
- Will procedures be complete?
- Will procedures be symptom or diagnosis oriented?

Available procedures to assist the watch officer include master's standing orders and procedures for the type-specific ECDIS. Master's standing orders dictate ECDIS safety parameters to be used by the watch officer and watchstanders. The Step 6 questions asked whether the procedures will be complete and whether the procedures will be symptom oriented. This thesis made the assumptions that the procedures will be complete because representative operating procedures from a USCG-approved system, ECDIS 24, are detailed and diagnosis-oriented (Raytheon Anschütz 2014). However, the operator manual contents are not guaranteed to be detailed and diagnosis-oriented. According to SPAR-H, a multiplier of 50 is assigned if procedures do not exist; a multiplier of 20 is assigned if procedures are incomplete; and a multiplier of 0.5 if the procedures are diagnosis-oriented. The nominal multiplier of 1 was assigned to ECDIS in the absence of additional information, in accordance with the guidance from Gertman et al. (2005). This multiplier

was applied to all work blocks because the same set of procedures are applicable to all work blocks.

5. CRUSH Step 6 Question 5: Ergonomics and Human-Machine Interface

The ECDIS system concept was evaluated against the CRUSH Step 6 questions for assessing ergonomics and HMI, as proposed in Chapter III:

- Will human machine interface be misleading?
- Will the system be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?
- Will the system be designed to support the human in any adverse physical environment?
- Will the system be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?
- Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?

Each question was evaluated separately to determine if the condition was evidenced in the ECDIS system concept or in the operational use of the ECDIS. Requirements for the human-machine interface specified in the revised performance standards include requirements for display, brightness, contrast, and physical controls. Watch officers toggle the day and night brightness and are able to zoom in for greater detail. A standard button on all ECDIS reverts the display to the minimum IMO-required information (IMO 2006). Though the ECDIS is located on an enclosed bridge that is climate controlled and protected from wind and rain, the entire ship is still subject to variable sea state and lighting conditions. Bridge personnel are not required to wear personal protective equipment. Considerations of how the system is physically integrated among the other equipment on the bridge is beyond the system designer's control. Another question asked whether the system will be designed to eliminate misinterpretation of instrumentation and visual/

auditory cues and warnings. While the intention of the design is to alert the watchstander of safety conditions and system malfunctions, the frequency of alarms overwhelms the operators. Because of the frequency of alarms, operators silence alarms without understanding them (MAIB 2017).

The SPAR-H evaluation levels for ergonomics and HMI allow for a multiplier of 50 if ergonomics and HMI are "misleading or missing;" a multiplier of 10 for "poor" ergonomics and HMI; and a multiplier of 0.5 if ergonomics is "good (Gertman et al. 2005)." According to the guidance in Gertman et al. (2005), the nominal value of 1 applies if there is insufficient data to make an evaluation. Despite the potential for many ergonomics and HMI problems resulting from the physical environment, workspace integration, alarm frequency, and chart interpretation, only a single evaluation is permitted according to the SPAR-H methodology. A multiplier of 10, indicating "poor" ergonomics and human-machine interface, was selected for all work blocks.

6. CRUSH Step 6 Question 6: Complexity

The ECDIS system concept was evaluated against the CRUSH Step 6 criteria that determine complexity. From the Chapter III discussion, the questions in Question 6 are:

- Will the system satisfy at least three of the five following conditions?
    a. Tasks are prioritized for the human.
    b. Diagnostic information is presented by the system.
    c. Controls and switches are clear and easily accessible.
    d. Instrumentation and warning systems are designed with the human in mind.
    e. The system will always be fully staffed.
- Will at least two of the above conditions apply?

The revised performance standard dictates the conditions that would result in an alarm or indicator to alert the operator of a dangerous situation or a system malfunction. The revised performance standard also dictates design of display, controls, and switches.

The Step 6 assessment considers whether a system will be fully staffed in order to maintain a normal workload. Because the ECDIS is the responsibility of one person during the watch and not a team, this thesis assumed the ECDIS will be staffed. Because of the number of mishaps attributed to the disabling of frequent alarm, this thesis assumed that instrumentation and warning systems could present a problem for the operator. Gertman et al. (2005) assign "highly complex" tasks a multiplier of 5 and "moderately complex" tasks a multiplier of 2. In accordance with the scoring described in Chapter III, the multiplier for complexity was assigned a value of 1, nominal, for all work blocks because at least three of the five criteria applied.

7. CRUSH Step 6 Question 7: Experience and Training

Two questions determined the multiplier for experience and training:

- Will all operators be trained on and retain knowledge on this system?
- Will only operators with previous experience operate this system?

Training on ECDIS operations is one of the required Standards of Training, Certification and Watchkeeping for Seafarers competencies for master, chief mate, and Officer in Charge of a Navigational Watch (USCG 2018). All watch officers are trained on ECDIS in the course of their licensure. Training content is dictated by the IMO sub-committee Standards of Training and Watchkeeping (IMO 2011). Schoolhouses use an ECDIS that is manufactured by Transas while MSC ships use a variety of ECDIS manufacturers, none of which are Transas (Maritime Institute of Technology and Graduate Studies n.d.). Employers are responsible for ECDIS operators being familiar with the specific ECDIS model installed on the ship, but there is no requirement to have prior experience on the manufacturer-specific ECDIS (IMO 2011). The Certificate of Competency issued following completion of a 40-hour training course is the only documentation needed to demonstrate the "required standard of competence has been achieved (IMO 2017b)." Though all ECDIS operators are trained, the absence of a requirement to have experience on a type-specific ECDIS prior to operation drives the training and experience multiplier to be "low," instead of "nominal" or "high (Gertman et

al. 2005).” Gertman et al. associated “low” with a multiplier of 10 for decisions, and a multiplier of 3 for actions. All work blocks were evaluated to be “low” for experience and training because though all operators have training requirements for licensure, the potential exists for all operators to be initially unfamiliar with the type-specific ECDIS on the ship.

8. CRUSH Step 6 Question 8: Stress

Two assessment questions determined the multiplier for stress:

- Could any system operator ever experience extreme stress?
- Could any system operator ever experience high stress?

Two sources of stress are operational pace and staffing levels. Military Sealift Command operations are more predictable than those of the Navy and of a higher tempo than commercial cargo ships because the MSC supports Navy operations such as refueling and replenishment. The MSC follows civilian commercial ship standards, including those for manning levels and personnel organization. The bridge personnel are typically the watch officer, helmsman, and lookout. The minimum staffing on the bridge is a watch officer and a helmsman. The bridge staff increases to as many as six people as complexity of operational environment increases. This thesis assumes that a majority of these conditions exist in the USCG-approved system and that the ship bridge will be staffed with at least the watch officer, helmsman, and lookout. However, in light of the MSC mission to support Navy operations, this thesis assumes that the work tempo for a watch officer is high. The duration of a ship assignment ranges from four months to the length of a career. Most second officers only stay for the minimum required duration of four months, as stated by Alexander Halliday (Force Navigator, Military Sealift Command), in discussion with the author, July 8, 2020. Gertman et al. (2005) set a multiplier of 2 for “high stress”; a value of 5 for “extreme stress”; and a nominal value of 1. Evaluation of personal stress levels of a typical MSC officer is outside the scope of this thesis. With regard to operational tempo and workload, this thesis assumed that operators may experience high stress but not extreme stress. The stress multiplier was assigned a value of 2 for all work blocks due to operational pressures.

9. CRUSH Step 6 Question 9: Work Processes

The final Step 6 assessment area evaluated pressures driven by organizational culture and leadership:

- Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?
- Will every supervisor perform and communicate continuous risk assessments?
- Will organizational culture always be exceptionally good?

Maritime mishaps often cite supervisor failure to perform real-time risk assessments. In this light, this thesis assumed that was possible for masters, chief mates, and watch officers to assume more risk than necessary to support operational tempo. For example, masters may fail to thoroughly review voyage plans, familiarize new crew with the ECDIS type on the bridge, or set safety contours that fail to allow enough time to respond to alarms. Gertman et al. (2005) allow for three evaluation levels of this PSF: "poor," "nominal," and "good." Given that poor leadership contributed to previous maritime incidents (MAIB 2015; Fukuoka 2019), the work processes multiplier was conservatively assigned to be poor, with a value of 5 for actions and 3 for decisions (Gertman et al. 2005).

10. CRUSH Step 6: ECDIS Human Error Probabilities

There are 13 work blocks evaluated. Detailed CRUSH Step 6 results for all work blocks are located in Appendix C. The results are similar for each work block because the tasks are all performed by the watch officer using the same equipment, the system concept has limited details to evaluate, and the evaluation levels provided by SPAR-H are broad. Two human error probabilities remain following consolidation of the results, one for decision tasks and another for action tasks. More than three multipliers were changed from the nominal value of 1 so that Equation 2 applied for both probabilities. The HEP for decision tasks is 0.669; the HEP for action tasks is 0.131 (Table 3).

Table 3. Human error probabilities for ECDIS tasks

Performance shaping factor	Decision	Action
Nominal human error probability	0.01	0.001
Fitness for duty	5	5
Available time	0.1	0.1
Procedures	1	1
Ergonomics/human-machine interface	10	10
Complexity	1	1
Experience and Training	10	3
Stress	2	2
Work processes	2	5
Human error probability	**0.669**	**0.131**

D. REVIEW AND RECOMMENDATIONS: CRUSH STEPS 7 AND 8

The calculated human error probabilities were further evaluated to determine if the findings were plausible and the extent to which performance shaping factors influenced the human error probabilities (Step 7). The final step (Step 8) of the CRUSH process formed recommendations to the program that would reduce human error probabilities and improve system resilience to human error.

1. CRUSH Step 7: Review of Results

The findings from CRUSH Step 5 are that the system is largely dependent on the navigation officer and ECDIS operator who interact directly with the ECDIS and who are also subject to the decisions, resources, and pace that leadership sets for the ship. While the analysis from Steps 4 and 5 indicate there are a number of conditions that would prevent completion of each ECDIS task, in practice there is enough time to weigh decisions and take corrective actions if needed. Concurrent activities such as paper charts, logs, and a lookout fortify navigation practices so that ECDIS is not the sole navigation system on the bridge. However, operation and support of the backup systems is not in the scope of the ECDIS program. Senior leaders are responsible for these backup systems to be functional and available on their own ships.

The findings from CRUSH Step 6 indicate it is likely that decision and action errors will be made during the lifetime of the ECDIS. The probability for decision-based tasks is

driven primarily by the multipliers for ergonomics/human-machine interface and training, and to a lesser degree by fitness for duty. The probability for action-based tasks is driven primarily by the ergonomics/human-machine interface, and to a lesser degree by the multipliers for fitness for duty and work processes. The human-machine interface is designed by the manufacturer, but the integration of the ECDIS on the bridge among other radar systems is beyond the manufacturer's control. Given that the IMO requirements provide criteria to establish only a basic interface design that is common to all ECDIS systems, this thesis assumed that the human-machine interface could be misunderstood. With over 30 different types of ECDIS systems, the displays, controls, and functions are slightly different. For instance, methods for zooming in to the viewable area, setting the safety depth and safety contour, and labels for the safety zone vary between models (Fukuoka 2019). The potential exists for the graphics-intensive system to have visual indicators and warnings that will be misinterpreted. Further, while the bridge environment is protected from most elements, the potential exists that sea state and lighting conditions may vary. Because integration on the bridge is not guaranteed, the design of type-specific ECDIS may vary, and the ship may encounter variable environmental conditions that affect the operator's perception and judgement, this thesis does not support reduction of the ergonomics/human interface multiplier from 10 to 1.

Accident reports cite training failures as a reason for a number of human failures contributing to maritime accidents. These contributing factors range from a failure to view the display at a sufficient level of detail or with the correct scale, to a failure to understand the importance of updating electronic navigational charts prior to a voyage (MAIB 2017). Acquisition programs with the responsibility of creating navigation systems can invest resources in developing training, but recommendations for training delivery are outside the scope of the design effort. Fortunately, the USCG requires ECDIS training as a part of Officer in Charge of a Navigational Watch, master, and chief mate licensure which would justify a favorable training multiplier (USCG 2018). However, the performance shaping factor encompasses both training and experience. The International Maritime Organization does not require experience beyond familiarity to operate ECDIS (IMO 2017b); therefore the initial training and experience multiplier for a new navigation officer onboard a ship is

rated “poor.” This thesis offers that the training and experience multiplier can be reduced to 1 once an operator has gained experience using the ECDIS that is onboard the ship.

The fitness for duty and work process multipliers also increase the human error probability. This thesis considered that teammates might discourage an unfit operator from working, but given that the ECDIS operator is typically the watch officer and the bridge is minimally manned, the potential exists for an injured, fatigued, or medicated person to work. System designers could incorporate additional prompts to confirm operator actions, or incorporate algorithms to detect any lags in performance. Operational pace affects the importance and urgency of safe navigation. Changes to mission and organizational culture are beyond the control of the ECDIS operator and of the ECDIS system designers, though more information regarding the operational tempo could aid system designers in creating specialized features for complex situations.

With regard to ECDIS, there are additional opportunities to reduce human error probability through implementation of the system. Table 4 shows reduction to HEPs for decision-based tasks when selected PSFs are improved. The changes each reflect a single improvement to a SPAR-H evaluation level (Gertman et al. 2005) for a single PSF. Having an experienced operator making decision improves the experience and training level from “low” to “nominal,” with an associated multiplier of 1. Overall, this reduces the HEP from 0.669 to 0.168. Improving fitness for duty one evaluation level from “degraded fitness” to “nominal,” changes the multiplier from 5 to 1; the overall HEP is reduced from 0.669 to 0.288. Simultaneous improvement to experience, fitness for duty, and work process result in a reduced HEP of 0.020 for decision-based tasks.

Table 4. Human error probability changes in response to non-technical improvements—Decision-based tasks

Performance shaping factor	Original HEP	Experienced Operator	Improved Fitness for Duty	Improved Work Processes and Fitness for Duty with Experienced Operators
Nominal human error probability	0.01	0.01	0.01	0.01
Fitness for duty	5	5	1	1
Available time	0.1	0.1	0.1	0.1
Procedures	1	1	1	1
Ergonomics/human-machine interface	10	10	10	10
Complexity	1	1	1	1
Experience/training	10	1	10	1
Stress	2	2	2	2
Work processes	2	2	2	1
Human error probability	**0.669**	**0.168**	**0.288**	**0.020**

Table 5 shows similar reduction to HEPs resulting from improvements to key PSFs for action-based tasks. Referencing again the SPAR-H evaluation levels (Gertman et al. 2005), improving work processes one level from "poor" to "nominal" reduces the associated multiplier to 1, and the overall HEP from 0.131 to 0.029. Improving fitness for duty one evaluation level from "degraded fitness" to "nominal," changes the multiplier from 5 to 1, and reduces the overall HEP from 0.131 to 0.029. Simultaneous improvements to experience/training from "low" to "nominal," in addition to improvements to fitness for duty and work process, result in a reduced HEP of 0.002 for action-based tasks.

Table 5. Human error probability changes in response to non-technical improvements—Action-based tasks

Performance shaping factor	Original HEP	Improved Work Process	Improved Fitness for Duty	Improved Work Processes and Fitness for Duty with Experienced Operators
Nominal human error probability	0.001	0.001	0.001	0.001
Fitness for duty	5	5	1	1
Available time	0.1	0.1	0.1	0.1
Procedures	1	1	1	1
Ergonomics/human-machine interface	10	10	10	10
Complexity	1	1	1	1
Experience/training	3	3	3	1
Stress	2	2	2	2
Work processes	5	1	5	1
Human error probability	**0.131**	**0.029**	**0.029**	**0.002**

2. CRUSH Step 8: Recommendations

The ECDIS is a graphics-intensive system that integrates data from multiple types of electronic navigation charts and ship sensors. The navigation officer uses the system to plan and input a route, then the watch officer monitors the ship's position along the route during the voyage. Often the navigation officer also serves as the watch officer. The CRUSH results confirmed that system performance is dependent upon the decisions and actions of a single person during its operation. As such, personal factors including the operator's state of mind, and mental and physical fitness affect the successful accomplishment of each ECDIS function. Supervisors should continue to apply operational risk management to ensure that personnel are fit for duty.

Based on the CRUSH analysis, this thesis proposes four recommendations to reduce human error probability. The recommendations address the causes of the highest PSF multipliers: ergonomics and human-machine interface, and training and experience. Program managers will take into account the frequency and importance of each evaluated

task when applying the CRUSH recommendations. One recommendation addresses system design; the remaining recommendations address implementation and operation of ECDIS.

- **Recommendation 1:** Design alarms to be distinct from each other and provide technical manuals and training materials to help operators understand and remember the types of alarms used. The ECDIS uses the same data available to the operator on paper charts, but the system advantage is integration of the ship's current position and AIS onto the display of the electronic charts. ECDIS alerts the operator of dangerous conditions by displaying an indicator or sounding an alarm. Because the IMO dictates multiple navigational conditions that require alarms, there is potential for operators to be confused by the frequent alarms in the already fast-paced environment of the ship bridge. This causes the ergonomics/ HMI multiplier to be scored "poor" with a multiplier of 10, rather than "nominal" with a multiplier of 1.

The CRUSH analysis also identified contributions to human error potential in areas that are beyond the system designer's control: physical integration into the workspace, operator experience, and staffing. Three recommendations address implementation.

- **Recommendation 2:** Include guidance on a specific location for ECDIS on the ship's bridge. The ergonomics of the system is dependent on integration of ECDIS with other equipment on the ship's bridge. Operators should be able to physically interact with the system while continuing to maintain situational awareness of the ship's environment. Failure to integrate ECDIS into the bridge layout results in an ergonomics/HMI evaluation of "poor" with a multiplier of 10, rather than "nominal" with a multiplier of 1.

- **Recommendation 3:** Provide additional familiarization training to new navigation officers on the type-specific ECDIS. The training/experience multiplier currently has the same impact on the human error probability as the ergonomics multiplier. With experienced operators, the training and

experience multiplier is reduced from “low” to “nominal.” For decision-based tasks, the multiplier is reduced from 10 to 1; for action-based tasks, the multiplier is reduced from 3 to 1.

- **Recommendation 4:** Staff a dedicated ECDIS operator to reduce workload from supervisory tasks. The fast pace and high workload of the ECDIS operator, who is also the watch officer, results in an evaluation of “poor” for work processes. Removing the additional workload from the operator reduces this multiplier from 5 for action-based tasks to a “nominal” value of 1.

The results of the CRUSH analysis show that system designs alone are insufficient to guarantee system success. Automation assists the operator by analyzing all the sensor data and presenting clear information with increased reliability. However, if the system is not properly deployed into the operator’s environment, the operator could experience information overload (Fukuoka 2019). Technology must also be combined with overall workplace design, training for normal and emergency operations, and organizational improvements in order to increase safety.

E. VERIFICATION AND VALIDATION

The Validation Square (Pedersen et al. 2000) applies both qualitative and quantitative evaluation of method designs. Pedersen et al. recommend that the proposed method qualitatively demonstrates correctness by building a foundation using other validated methods and ensuring that information flows from the outputs into the inputs of sequential steps. They suggest that usefulness of the method is established by using the method, documenting the implementation, and obtaining a conclusion from the results. This thesis has accomplished this qualitative evaluation by combining elements of two validated methods, SPAR-H and HFACS, as the basis of CRUSH, and creating an eight-step process that starts with defining the human activities and conditions that are required for successful completion of each system function. The CRUSH steps and their development are detailed in Chapter III. Chapter IV describes how CRUSH is applied to the ECDIS as an example case.

Quantitative evaluation of the Validation Square examines the usefulness of the results from the example case and the dependency of those results on the elements proposed in the new method. Additional steps needed to complete quantitative validation of the CRUSH method is proposed in Chapter V as future work beyond the scope of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

The CRUSH method proposed in this thesis combines the thoroughness of the mishap investigation process with the probabilities assigned by the human reliability assessment method. Both human reliability analysis and mishap analysis involve systems-of-systems thinking to understand the individual, environment, and organizational factors that contribute to human errors in action and decision-making. Human reliability analysis considers the likelihood of events that have not yet occurred. Mishap investigations uncover contributing factors to a sequence of events that have already occurred.

A. SUMMARY

The research question for this thesis was to explore whether established methods from human reliability analysis and accident investigation could be applied to the system development to improve human-machine interaction that is critical to total system performance. Accident investigations result in specific and actionable recommendations to address human factors. The review of Navy collisions in 2017 found a number of engineering and procedural contributors, including design of helm controls and failure to continuously apply operational risk management (Davidson 2017). Similarly, the FAA will require a review of flight control systems and pilot training before the Boeing 737 MAX can return to service. This follows two aircraft accidents in 2018 involving the 737 MAX maneuvering characteristic augmentation system (Federal Aviation Administration 2019, 2020). System design is subject to cost, facilities, and resource constraints (Langford 2012). Operator and maintainer manning levels, skill levels, workload levels, and training levels are all affected by these constraints, and the effects on human performance may not be anticipated by the system designer. This thesis proposes a process to review the early system concept that incorporates functional analysis, failure mode analysis, and questionnaires based on human reliability and accident investigation inquiries. This thesis recommends this process be applied before system requirements are finalized and system design prototypes are completed. This process identifies design vulnerabilities similar to those found during mishap investigations – but before any accidents occur.

The literature review surveyed typical activities during the requirements development phase where this process will be used, specifically how technical specifications detail functional needs to be met in a system prototype. In this early phase of development, a number of activities are focused on risk reduction. Technical risk reduction activities, such as those outlined in the NAVSEA R&ME manual (NAVSEA 2017), do not consider all the individual, supervisory, and organizational factors that affect the risk contribution from humans. To address these shortcomings, the SPAR-H method was selected for this thesis from a survey of human reliability assessments in the literature review. Human error probability calculated by SPAR-H combines the evaluation of eight performance shaping factors and a nominal HEP. A similar survey of mishap investigation methods determined that the DOD HFACS was a suitable accident method to use for this thesis because of the investigative criteria examine interactions between people and technology in addition to safety culture, workplace, and organizational factors. The performance shaping factors and accident subcategories from SPAR-H and HFACS form the focal point of a method that leads requirements developers to reflect on the human roles and functions required by the physical system and whether the physical system impacts the human.

The proposed method uses SPAR-H and HFACS to determine the consequence of poor human systems integration on system success and the likelihood of human error for each human function within the system. Both consequence and likelihood are needed to describe system risk. The CRUSH method focuses risk reduction efforts on the human roles.

The CRUSH Step 5 questionnaire presents HFACS concepts summarizing each major HFACS category: unsafe acts, preconditions, supervisory actions, and organizational influences. Based on insights gained from the literature, the CRUSH Step 5 questions reflect HFACS subcategories rather than HFACS nanocodes, which have lower inter-rater agreement.

The CRUSH Step 6 questionnaire presents SPAR-H factors for evaluation in the order of greatest impact influence on the overall HEP. The result of CRUSH Step 6 is not

only the HEP for a specific operator action or decision, but the multipliers for each of the eight factors that contribute to the HEP.

The process concludes with a review of results and formation of recommendations based on the insights gained from examining system resiliency and the likelihood of human error. The recommendations formed in CRUSH Step 8 highlight the areas where the human error probability can be reduced through system design decisions.

A demonstration applied the CRUSH process to the ECDIS. The ECDIS is used by commercial mariners and the U.S. Navy to plan voyages and monitor a ship's route along a voyage path. The system is intended to improve safe navigation by automating the aggregation of ship data and charts presented to the operator and providing alerts to dangerous conditions. A ship's bridge, where ECDIS is located, is dependent on technology, people, organizational structure, and physical environment (National Research Council 1990). Technical SMEs from Military Sealift Command provided operational context for the ECDIS during this demonstration.

Work blocks depicted the ECDIS functions as specific decisions and actions that an individual would complete for each system function. The fault trees created in CRUSH Step 4 for each work block showed basic events such as failure to recall training and inadequate design of an audible alarm, which, in combination with other basic events, could prevent a system function from being completed. The analysis of Step 5 results showed that system performance is affected by the ECDIS operator and non-technical preconditions, with additional influence from supervisor actions and organizational pressures. Following completion of the Step 6 questionnaire for each work block, results showed that decision-based tasks have a HEP of 0.669 and that action-based tasks have a HEP of 0.131. The highest PSF multiplier for both decision-based and action-based tasks was ergonomics/HMI. For decision-based tasks, the HEP could be reduced from 0.669 to 0.168 if operators were required to be familiar with the type-specific ECDIS on the bridge. For action-based tasks the HEP could be reduced from 0.131 to 0.029 if either the work processes or fitness for duty multiplier were improved to the next SPAR-H evaluation level. Four recommendations based on the CRUSH analysis addressed: 1) the ability to distinguish the various audible and visual alarms; 2) the integration of ECDIS on the

bridge; 3) familiarity of the operator with type-specific ECDIS; and 4) additional staffing to allow the watch officer to concentrate on supervisory duties.

The demonstration of all eight steps of the process confirmed that the method can provide results similar to findings from maritime accidents investigation reports. Additional demonstrations of this method at later system development phases and on other MSC bridge systems are useful to support findings from this concept review and to gain confidence in the method.

B. DISCUSSION

1. Development of the CRUSH Process

Definitions of individual work tasks and failure logic are important to put the results in context of overall system performance. The evaluation of the system concept focuses on individual functions that require human interaction. Therefore, the process begins with guidance on how the human interactions are identified. The process continues with decomposition of identified human functions into tasks. Where task sequence is important, the sequence is also captured in the action diagrams for CRUSH Step 3. Failure analyses of each work block in CRUSH Step 3 comprise the fault tree logic in CRUSH Step 4. The smaller work blocks are used to inspect human integration with other system components, such as hardware and software, with other systems, and under organizational and physical environment constraints.

The initial intention of this thesis was to create an assessment whose findings are used to recommend specific physical design requirements be included in the technical specifications. However, addressing the findings of the assessment solely through updates to the technical specifications limits the ways the findings could be used to reduce risk reduction. Program managers define priorities in the system development cycle and devote resources in accordance with those priorities. Program managers use risk-based decision making to decide which activities to prioritize and resource. Step 5 of the CRUSH method identifies the extent to which individual acts, preconditions, supervisory actions, or organizational influence have impact on the system functions. Step 6 of the CRUSH method is used to estimate the likelihood that the human will err while performing a

necessary system function. Together consequence and likelihood, as assessed using the CRUSH method, inform the program manager of any human contributions to risks that were not previously anticipated by the system concept. The program manager can choose to accept the risks identified through use of the method, or mitigate risks using various approaches throughout the life cycle. Mitigations may include, but are not limited to, development of additional diagnostic information in the graphical user display, detailed procedures in the technical manual for system recovery, instructions for integrating the physical system into the operator's workspace, and recommendations for minimum staffing and training levels for the system being designed.

While deconstructing the evaluation levels of SPAR-H and the nanocodes from HFACS, limitations of each method became evident. The HFACS accident investigation method has 109 nanocodes and each is considered equally important in the application of the method. Instead of 109 nanocodes, Step 5 uses the 17 HFACS subcategories to which the nanocodes belong. This questionnaire provides the analyst with an overall understanding of the unsafe acts, preconditions, supervisory actions, and organizational influences that apply to the system. All Step 5 responses are considered equal, meaning that each Yes response to a Step 5 question indicates that a system function will not be completed. In contrast, the SPAR-H method has eight performance shaping factors, each with different numbers of evaluation levels and different ranges of multipliers. For example, Procedures has five evaluation levels ranging from 0.5 to 50, while Stress has three levels ranging from 1 to 5. Within each PSF, levels are not evenly distributed; the five Procedures multipliers are 0.5, 1, 5, 20, and 50. It is not possible to assign a Procedures multiplier between 20 and 50. Similarly, the only available multipliers for Ergonomics/ HMI are 0.5, 1, 10, and 50. This limits the fidelity of the Step 6 evaluation.

The CRUSH process is designed to be used by a diverse team of subject matter experts representing human factors, operational, and engineering expertise. Initially, the analysis was intended to be simple enough and descriptive enough to be completed by one person, but the analysis is enriched through the professional experiences of the team members. Each team member brings a different understanding of the system concept, human capabilities, and operational use and constraints. While the process steps are still

simple enough to be completed by one person, an unintended benefit from the team approach is that the quality of the inputs to the questionnaires is improved, and the recommendations are supported by a consensus of the human factors, engineering, and operational representatives.

2. Limitations of the Final CRUSH Process

The CRUSH process incorporates the major parts of SPAR-H and HFACS, namely the calculation of human error probability supported by the subcategories defined in HFACS. The SPAR-H human reliability method also includes additional calculations to account for dependencies beyond analysis of a single task. The error probability increases when one task is dependent upon the successful completion of a preceding task, or if multiple tasks are completed by the same crew with similar individual factors and similar training. Inclusion of dependencies is outside the scope of this thesis. For the purpose of this thesis, the tasks are evaluated independently with no dependence because the focus is on the evaluation factors that result in the HEP.

Six of the eight performance shaping factors have multiplier levels that result in decreased human error probability (Figure 33): available time, complexity, work processes, ergonomics and HMI, procedures, and experience and training. Three of them, available time, work processes, and procedures, are incorporated into the CRUSH Step 6 questionnaire. The detail needed to assess quality of training materials and applicability of previous operator experience level may not yet exist when the CRUSH process is applied the first time. The available time multiplier can be further revised after evaluating the human-machine interface of prototype designs. A detailed assessment of complexity and ergonomics is not yet possible at this stage when physical prototypes do not yet exist. In cases where there is insufficient information to make an evaluation, the default SPAR-H multiplier is 1. This neutral multiplier does not increase or decrease the HEP. When the CRUSH process is repeated in future development stages, additional system detail will be available for a more robust evaluation of current system design. Usability studies performed later in system development can examine whether ergonomics features reduce complexity. Future work on this topic can propose alternate multiplier scores to account

for the relationship between ergonomics and complexity to determine if reductions to both multipliers are warranted.

Figure 33. Performance shaping factor multipliers that decrease human error probability

In this thesis, the performance shaping factors are not further manipulated to account for the relationships between two or more performance shaping factors. For example, multiple performance shaping factors affect the available time. Poor ergonomics can result in inefficiency of movement, which will require more time to complete. Stress affects the operator's ability to recall. An operator can use experience to quickly diagnose an off-normal condition. The strength of the relationships between evaluated factors is not used in this thesis to further adjust the calculated HEP beyond its initial scoring.

C. RECOMMENDATIONS

The thesis recommends that acquisition programs use the CRUSH process during requirements development to implement specific recommendations for human considerations into the system design. Results from the method show where the system concept is most sensitive to human actions and decisions and the nature of those vulnerabilities. The method can be completed without proprietary software and with a

subset of the group of engineers that are assembled to write system requirements. This aids the usability and acceptance of the method and removes a barrier from implementation DOD-wide. Further, the individual analyses in Steps 2 through 4 can reuse other engineering analyses as input for these steps. The method can accept existing functional analyses developed for reliability analysis, human factors analysis, maintenance and logistics support, as input for the method steps. The analyses from process Steps 3 through 6 can support development of use cases, which also support requirements development, and can influence preparation for test and evaluation such as selection of test personnel and training in a later phase (Blanchard and Fabricky 2011; Buede and Miller 2016). The results from CRUSH can also be applied to a feasibility analysis that examines performance, effectiveness, maintenance, and cost criteria to determine the practicality of a system.

This thesis recommends that the program manager update the fault tree basic events with the resulting human error probabilities. The HEPs should be combined with the failure rates of the hardware and software failure to determine which failure scenarios are most likely. The logic may identify that multiple human errors are required before the system fails. The approach to examine the contribution of each PSF to the single HEP is sufficient for the purposes of the concept review. Used in this way, the system developers can focus on the factors that result in the most events with the highest probability of occurrence. If the human action or decision is a single-point failure or is identified as a common-cause failure in the fault trees, the probability calculated in Step 6 is more indicative of the probability of system failure.

In lieu of recommendations for new or revised technical specifications, the results of this multi-step process inform the program manager of current risk and risk drivers with respect to human systems integration. The program manager can choose to accept the risk of the concept as designed and evaluated or implement the specific recommendations that result from the evaluation. An example recommendation from CRUSH Step 5 is to include a backup or redundant function where the function is deemed critical and susceptible to human error. An example recommendation from CRUSH Step 6 is to propose additional personnel to offset workload and reduce complexity.

The CRUSH process can evaluate from the conceptual design the key factors important to human integration that increase reliability. This method is designed to be used immediately following concept development with the limited details regarding the physical architecture. A manufacturer can gain a competitive edge by making smart design choices that increase human reliability and usability. The CRUSH process can quantify the impacts of the design choices. As a risk assessment tool, the full method is applicable also to the design of user test events, both of proposed physical designs and completed prototypes, in conjunction with operational testing.

D. FUTURE WORK

This thesis recommends that validation of the CRUSH method continues in future work. The Validation Square (Pedersen et al. 2000) describes a path to validation that evaluates effectiveness and efficiency of the new method. According to Pedersen, effectiveness begins with acceptance of individual constructs that form the new method and that the method is consistent; efficiency shows usefulness of the method and that any usefulness is due to the method itself. To build confidence in CRUSH, this thesis selected two validated assessment tools as foundations for the proposed method. The work in this thesis then described how the outputs of each CRUSH step were used as inputs into the next step. Next, this thesis used the ECDIS for a demonstration example. To further study the internal consistency of the CRUSH method, specifically Steps 5 and 6, a human subjects test is proposed to determine the inter-rater agreement between teams using the CRUSH method on an early system concept. Teams of raters would use the CRUSH process questionnaires on the same work blocks to determine if agreement between the teams' results is statistically significant. At least 10 teams of raters are needed for statistical significance. For consistency, each team would complete the Step 5 and Step 6 questionnaires for the same work blocks. The teams will also be asked to form recommendations based on their own interpretation of their results. The teams will have access to the same information sources describing the system concept, including fault trees, in order to minimize the variations of assumptions used by each team. The results of interest from each team would be the major influences upon the system, as described by the Step 5 questionnaire criteria; and the multiplier and final HEP determined by the Step 6

questionnaire. In addition to inter-rater agreement for the questionnaires, an analysis of the results can also show if the background and experience of each team member impacts the results. An analysis of the results may also show that while questionnaire scoring may differ between teams, the final recommendations are similar. These test plans are subject to institutional review board approval.

The next step in the Validation Square is to show that the results are useful and that the usefulness of the results is derived from the method used. A demonstration on a state-of-the art ECDIS to compare the final ECDIS product with the recommendations from the ECDIS system concept evaluation, is out of scope for this thesis effort. A follow-on study is proposed to examine the effects of recommendations from this method to determine whether they are impactful against program metrics for mission performance, reliability, or cost-savings, for example. As there are a number of ECDIS systems available on the market, the CRUSH method can be applied to a variety of designs to determine which designs are the most human-centered and then compare the technical and business cases for each.

Additional demonstrations on systems of varying platform size and with varying numbers of operators would increase confidence in the method to gain acceptance for this method. The additional tests would help prove both the internal consistency of this method given a variety of example systems and would also add to the metrics collected to show that the system has useful results for a program. Success stories from programs who have implemented the method would benefit acceptance.

The CRUSH method described in this thesis successfully demonstrates that SPAR-H and HFACS can be used as the foundation to a process that takes a system concept as input and returns recommendations that improve human integration. The demonstration of this method on ECDIS is a first step towards verification and validation of the method. Follow-on studies by multiple assessment teams and on multiple system platforms is required for full validation and deployment of the method as a risk reduction tool.

APPENDIX A. CRUSH QUESTIONNAIRES

A. CRUSH STEP 5

1. Can an operator who is unfit for duty prevent the work block from being completed?		Yes/No
2. Can the following unsafe acts prevent the work block from being completed?		Yes/No
	a. Wrong decision or no decision	
	b. Wrong action or no action	
	c. Violation of known procedure	
3. Can the following non-technical preconditions prevent the work block from being completed?		Yes/No
	a. Physical environment negatively affects operator action or decision	
	b. Individual's medical or physiological condition	
	c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	
	d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	
	e. Individual's attention management or awareness negatively affects the perception or performance of individuals	
	f. Interactions among individuals, crews, and teams	
4. Can the following examples of poor supervision prevent the work block from being completed?		Yes/No
	a. Supervisor willful disregard of instructions or policies	
	b. Supervisor failure to recognize and control risk	
	c. Inappropriate or improper supervision	
	d. Supervisor failure to provide guidance, training, or oversight	
5. Can the following examples of poor organizational influence prevent the work block from being completed?		
	a. Deficient or inadequate resources	
	b. Personnel selection and staffing	
	c. Policy and process issues, including pace and workload, training, and guidance	
	d. Organizational culture influences on individual actions	

B. CRUSH STEP 6

1. Is the human mainly making decisions or taking action?		Nominal HEP of 0.01 for decisions or 0.001 for action
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		If Yes, then automatic P(failure) = 1.0, otherwise next question
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	If No, then F = 5 and move to next category, otherwise F = 1 and move to next category
3. Will there be insufficient time to diagnose and act?		If Yes, then automatic P(failure) = 1.0
	Will there be more than 50x time needed to act?	If Yes, then T = 0.01 and move to next category, otherwise next question
	Will there be between 5x-50x time needed to act?	if Yes, then T = 0.1 and move to next category, otherwise next question
	Will there be only enough time to diagnose or act?	If Yes, then T = 10 and move to next category, otherwise next question
	Will the system always be fully staffed?	If No, then T = 10 and move to next category, otherwise T = 1 and move to next category
4. Will procedures exist?		If No, then P = 50 and move to next category, otherwise next question
	Will procedures be complete?	If No, then P = 20 and move to next category, otherwise P = 1 and move to next category
	Will procedures be symptom or diagnosis oriented?	If Yes then P = 0.5 and move to next category, otherwise P = 1 and move to next category
5. Will human machine interface be misleading?		If Yes, then H = 50 and move to next category, otherwise next question
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	If No, then H = 10 and move to next category, otherwise next question
	Will the system function be designed to support the human in any adverse physical environment?	If No, then H = 10 and move to next category, otherwise next question
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?	If No, then H = 10 and move to next category, otherwise H = 1 then move to next category
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?	If Yes then H = 0.5 and move to next category, otherwise H = 1 then move to next category
6. Will the work block satisfy at least 3 of the 5 following conditions?		If Yes, then C = 1 and move to next category, otherwise next question
	a. Tasks are prioritized for the human	
	b. Diagnostic information is presented by the system	
	c. Controls and switches are clear and easily accessible	
	d. Instrumentation and warning systems are designed with the human in mind.	
	e. The system will always be fully staffed	
	Will at least 2 of the above conditions apply?	If Yes, then C = 2 and move to next category, otherwise C = 5 and move to next category
7. Will all operators be trained on and retain knowledge on this work block?		If No, then E = 10 for decisions or E = 3 for actions and move to next category, otherwise next question
	Will only operators with previous experience operate this system?	If No, then E = 10 for decisions or E = 3 for actions and move to next category, otherwise E = 1 and move to next category
8. Could any system operator ever experience extreme stress?		If Yes, then S = 5 and move to next category, otherwise next question
	Could any system operator ever experience high stress?	If Yes, then S = 2 and move to next category, otherwise S = 1 and move to next category
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		If Yes, then O = 2 for decisions or O = 5 for actions and move to next step, otherwise next question
	Will every supervisor perform and communicate continuous risk assessments?	If No, then O = 2 for decisions or O = 5 for actions and move to next step, otherwise next question
	Will organizational culture always be exceptionally good?	If Yes, then O = 0.8 for decisions or O = 0.5 for actions, otherwise O = 1 then end.

APPENDIX B. ECDIS STEP 5 QUESTIONNAIRE

A. ROUTE PLANNING ASSESSMENT

	1 Route Planning		
	1.1 Plan the route	**1.2 Input the route**	**1.3 Change the route**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?			
a. Wrong decision or no decision	Yes	Yes	Yes
b. Wrong action or no action	Yes	Yes	Yes
c. Violation of known procedure	Yes	Yes	Yes
3. Can the following non-technical preconditions prevent the work block from being completed?			
a. Physical environment negatively affects operator action or decision	Yes	Yes	Yes
b. Individual's medical or physiological condition	Yes	Yes	Yes
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	Yes	Yes	Yes
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	Yes	Yes	Yes
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes	Yes
f. Interactions among individuals, crews, and teams	No	No	No
4. Can the following examples of poor supervision prevent the work block from being completed?			
a. Supervisor willful disregard of instructions or policies	Yes	Yes	Yes
b. Supervisor failure to recognize and control risk	Yes	Yes	Yes
c. Inappropriate or improper supervision	Yes	Yes	Yes
d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?			
a. Deficient or inadequate resources	No	No	No
b. Personnel selection and staffing	Yes	Yes	Yes
c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes	Yes
d. Organizational culture influences on individual actions	Yes	Yes	Yes

B. ROUTE MONITORING ASSESSMENT

	2 Route Monitoring		
	2.1 View the chart	**2.2 Change the view**	**2.3 Interpret the data**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?			
a. Wrong decision or no decision	Yes	Yes	Yes
b. Wrong action or no action	Yes	Yes	Yes
c. Violation of known procedure	Yes	No	No
3. Can the following non-technical preconditions prevent the work block from being completed?			
a. Physical environment negatively affects operator action or decision	Yes	Yes	Yes
b. Individual's medical or physiological condition	Yes	Yes	Yes
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	Yes	Yes	Yes
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	Yes	Yes	Yes
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes	Yes
f. Interactions among individuals, crews, and teams	No	No	Yes
4. Can the following examples of poor supervision prevent the work block from being completed?			
a. Supervisor willful disregard of instructions or policies	Yes	Yes	Yes
b. Supervisor failure to recognize and control risk	Yes	Yes	Yes
c. Inappropriate or improper supervision	Yes	Yes	Yes
d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?			
a. Deficient or inadequate resources	No	No	No
b. Personnel selection and staffing	Yes	Yes	Yes
c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes	Yes
d. Organizational culture influences on individual actions	Yes	Yes	Yes

C. ALARM AND INDICATOR RESPONSE ASSESSMENT

	3 Alarms and Indicators			
	3.1 Sense the alarm/ indicator	**3.2 Understand the alarm/ indicator**	**3.3 Take action**	**3.4 Clear the alarm**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes	Yes	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?				
a. Wrong decision or no decision	No	No	Yes	Yes
b. Wrong action or no action	No	No	Yes	Yes
c. Violation of known procedure	No	No	Yes	Yes
3. Can the following non-technical preconditions prevent the work block from being completed?				
a. Physical environment negatively affects operator action or decision	Yes	Yes	Yes	Yes
b. Individual's medical or physiological condition	Yes	Yes	Yes	Yes
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	No	Yes	Yes	No
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	Yes	No	No	Yes
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes	Yes	Yes
f. Interactions among individuals, crews, and teams	Yes	Yes	Yes	Yes
4. Can the following examples of poor supervision prevent the work block from being completed?				
a. Supervisor willful disregard of instructions or policies	Yes	Yes	Yes	Yes
b. Supervisor failure to recognize and control risk	Yes	Yes	Yes	Yes
c. Inappropriate or improper supervision	Yes	Yes	Yes	Yes
d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes	Yes	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?				
a. Deficient or inadequate resources	No	No	No	No
b. Personnel selection and staffing	Yes	Yes	Yes	Yes
c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes	Yes	Yes
d. Organizational culture influences on individual actions	No	No	No	No

D. ELECTRONIC CHART UPDATE ASSESSMENT

	4 Update charts	
	4.1 Retrieve new charts	**4.2 Install new charts**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?		
a. Wrong decision or no decision	Yes	Yes
b. Wrong action or no action	Yes	Yes
c. Violation of known procedure	Yes	Yes
3. Can the following non-technical preconditions prevent the work block from being completed?		
a. Physical environment negatively affects operator action or decision	Yes	Yes
b. Individual's medical or physiological condition	No	No
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	No	No
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	No	No
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes
f. Interactions among individuals, crews, and teams	No	No
4. Can the following examples of poor supervision prevent the work block from being completed?		
a. Supervisor willful disregard of instructions or policies	Yes	Yes
b. Supervisor failure to recognize and control risk	Yes	Yes
c. Inappropriate or improper supervision	Yes	Yes
d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?		
a. Deficient or inadequate resources	Yes	No
b. Personnel selection and staffing	Yes	Yes
c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes
d. Organizational culture influences on individual actions	No	No

E. ECDIS BACKUP ASSESSMENT

	5 Reliability, Availability, Backup				
	5.1 Paper chart	**5.2 Paper log**	**5.3 Redundant navigation system**	**5.4 Redundant sensor systems**	**5.5 Alternate power source**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes	Yes	Yes	Yes	Yes
2. Can the following unsafe acts prevent the work block from being completed?					
a. Wrong decision or no decision	No	No	No	No	No
b. Wrong action or no action	No	No	No	No	No
c. Violation of known procedure	No	No	No	No	No
3. Can the following non-technical preconditions prevent the work block from being completed?					
a. Physical environment negatively affects operator action or decision	Yes	Yes	Yes	Yes	Yes
b. Individual's medical or physiological condition	No	No	No	No	No
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	No	No	No	No	No
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	No	No	No	No	No
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes	Yes	No	No	No
f. Interactions among individuals, crews, and teams	Yes	Yes	No	No	No
4. Can the following examples of poor supervision prevent the work block from being completed?					
a. Supervisor willful disregard of instructions or policies	Yes	Yes	No	No	No
b. Supervisor failure to recognize and control risk	Yes	Yes	No	No	No
c. Inappropriate or improper supervision	Yes	Yes	No	No	No
d. Supervisor failure to provide guidance, training, or oversight	Yes	Yes	No	No	No
5. Can the following examples of poor organizational influence prevent the work block from being completed?					
a. Deficient or inadequate resources	No	No	Yes	Yes	Yes
b. Personnel selection and staffing	Yes	Yes	No	Yes	No
c. Policy and process issues, including pace and workload, training, and guidance	Yes	Yes	No	Yes	No
d. Organizational culture influences on individual actions	No	No	No	No	No

F. INADVERTENT ECDIS SHUTDOWN

	6 Inadvertent Shutdown **6** **Inadvertent ECDIS shutdown**
1. Can an operator who is unfit for duty prevent the work block from being completed?	Yes
2. Can the following unsafe acts prevent the work block from being completed?	
a. Wrong decision or no decision	No
b. Wrong action or no action	Yes
c. Violation of known procedure	No
3. Can the following non-technical preconditions prevent the work block from being completed?	
a. Physical environment negatively affects operator action or decision	No
b. Individual's medical or physiological condition	No
c. Individual's personality traits, psychosocial problems, psychological disorders or inappropriate motivation	No
d. Individual's sensory inputs (visual, auditory or vestibular) create a misperception of an object, threat or situation	No
e. Individual's attention management or awareness negatively affects the perception or performance of individuals	Yes
f. Interactions among individuals, crews, and teams	No
4. Can the following examples of poor supervision prevent the work block from being completed?	
a. Supervisor willful disregard of instructions or policies	No
b. Supervisor failure to recognize and control risk	No
c. Inappropriate or improper supervision	No
d. Supervisor failure to provide guidance, training, or oversight	Yes
5. Can the following examples of poor organizational influence prevent the work block from being completed?	
a. Deficient or inadequate resources	No
b. Personnel selection and staffing	Yes
c. Policy and process issues, including pace and workload, training, and guidance	Yes
d. Organizational culture influences on individual actions	No

APPENDIX C. ECDIS STEP 6 QUESTIONNAIRE

A. ROUTE PLANNING HUMAN ERROR PROBABILITY

		1 Route Planning					
		1.1	**1.1**	**1.2**	**1.2**	**1.3**	**1.3**
		Plan the route	**Plan the route**	**Input the route**	**Input the route**	**Change the route**	**Change the route**
1. Is the human mainly making decisions or taking action?		Decision	0.01	Action	0.001	Action	0.001
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		N		N		N	
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	N	5	N	5	N	5
3. Will there be insufficient time to diagnose and act?		N		N		N	
	Will there be more than 50x time needed to act?	N		N		N	
	Will there be between 5x-50x time needed to act?	Y	0.1	Y	0.1	Y	0.1
	Will there be only enough time to diagnose or act?						
	Will the system always be fully staffed?						
4. Will procedures exist?		Y		Y		Y	
	Will procedures be complete?	Y	1	Y	1	Y	1
	Will procedures be symptom or diagnosis oriented?						
5. Will human machine interface be misleading?		N		N		N	
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	Y		Y		Y	
	Will the system function be designed to support the human in any adverse physical environment?	N	10	N	10	N	10
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?						
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?						
6. Will the work block satisfy at least 3 of the 5 following conditions?		Y	1	Y	1	Y	1
	a. Tasks are prioritized for the human						
	b. Diagnostic information is presented by the system						
	c. Controls and switches are clear and easily accessible						
	d. Instrumentation and warning systems are designed with the human in mind.						
	e. The system will always be fully staffed						
	Will at least 2 of the above conditions apply?						
7. Will all operators be trained on and retain knowledge on this work block?		Y		Y		Y	
	Will only operators with previous experience operate this system?	N	10	N	3	N	3
8. Could any system operator ever experience extreme stress?		N		N		N	
	Could any system operator ever experience high stress?	Y	2	Y	2	Y	2
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		Y	5	Y	5	Y	5
	Will every supervisor perform and communicate continuous risk assessments?						
	Will organizational culture always be exceptionally good?						

B. ROUTE MONITORING HUMAN ERROR PROBABILITY

		2 Route Monitoring					
		2.1 View the chart	**2.1 View the chart**	**2.2 Change the view**	**2.2 Change the view**	**2.3 Interpret the data**	**2.3 Interpret the data**
1. Is the human mainly making decisions or taking action?		Decision	0.01	Action	0.001	Decision	0.01
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		N		N		N	
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	N	5	N	5	N	5
3. Will there be insufficient time to diagnose and act?		N		N		N	
	Will there be more than 50x time needed to act?	N		N		N	
	Will there be between 5x-50x time needed to act?	Y	0.1	Y	0.1	Y	0.1
	Will there be only enough time to diagnose or act?						
	Will the system always be fully staffed?						
4. Will procedures exist?		Y		Y		Y	
	Will procedures be complete?	Y	1	Y	1	Y	1
	Will procedures be symptom or diagnosis oriented?						
5. Will human machine interface be misleading?		N		N		N	
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	Y		Y		Y	
	Will the system function be designed to support the human in any adverse physical environment?	N	10	N	10	N	10
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?						
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?						
6. Will the work block satisfy at least 3 of the 5 following conditions?		Y	1	Y	1	Y	1
	a. Tasks are prioritized for the human						
	b. Diagnostic information is presented by the system						
	c. Controls and switches are clear and easily accessible						
	d. Instrumentation and warning systems are designed with the human in mind.						
	e. The system will always be fully staffed						
	Will at least 2 of the above conditions apply?						
7. Will all operators be trained on and retain knowledge on this work block?		N	10	N	3	N	10
	Will only operators with previous experience operate this system?						
8. Could any system operator ever experience extreme stress?		N		N		N	
	Could any system operator ever experience high stress?	Y	2	Y	2	Y	2
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		Y	5	Y	5	Y	5
	Will every supervisor perform and communicate continuous risk assessments?						
	Will organizational culture always be exceptionally good?						

C. ALARMS AND INDICATORS HUMAN ERROR PROBABILITY

		3 Alarms and Indicators							
		3.1 Sense the alarm/ indicator	**3.1 Sense the alarm/ indicator**	**3.2 Understand the alarm/ indicator**	**3.2 Understand the alarm/ indicator**	**3.3 Take action**	**3.3 Take action**	**3.4 Clear the alarm**	**3.4 Clear the alarm**
1. Is the human mainly making decisions or taking action?		Decision	0.01	Decision	0.01	Action	0.001	Action	0.001
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		N		N		N		N	
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	N	5	N	5	N	5	N	5
3. Will there be insufficient time to diagnose and act?		N		N		N		N	
	Will there be more than 50x time needed to act?	N		N		N		N	
	Will there be between 5x-50x time needed to act?	Y	0.1	Y	0.1	Y	0.1	Y	0.1
	Will there be only enough time to diagnose or act?								
	Will the system always be fully staffed?								
4. Will procedures exist?		Y		Y		Y		Y	
	Will procedures be complete?	Y	1	Y	1	Y	1	Y	1
	Will procedures be symptom or diagnosis oriented?								
5. Will human machine interface be misleading?		N		N		N		N	
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	Y		Y		Y		Y	
	Will the system function be designed to support the human in any adverse physical environment?	N	10	N	10	N	10	N	10
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?								
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?								
6. Will the work block satisfy at least 3 of the 5 following conditions?		Y	1	Y	1	Y	1	Y	1
	a. Tasks are prioritized for the human								
	b. Diagnostic information is presented by the system								
	c. Controls and switches are clear and easily accessible								
	d. Instrumentation and warning systems are designed with the human in mind.								
	e. The system will always be fully staffed								
	Will at least 2 of the above conditions apply?								
7. Will all operators be trained on and retain knowledge on this work block?		Y		Y		Y		Y	
	Will only operators with previous experience operate this system?	N	10	N	10	N	3	N	3
8. Could any system operator ever experience extreme stress?		N		N		N		N	
	Could any system operator ever experience high stress?	Y	2	Y	2	Y	2	Y	2
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		Y	5	Y	5	Y	5	Y	5
	Will every supervisor perform and communicate continuous risk assessments?								
	Will organizational culture always be exceptionally good?								

D. CHART UPDATE HUMAN ERROR PROBABILITY

		4 Update charts			
		4.1 Retrieve new charts	**4.1 Retrieve new charts**	**4.2 Install new charts**	**4.2 Install new charts**
1. Is the human mainly making decisions or taking action?		Action	0.001	Action	0.001
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		N		N	
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	N	5	N	5
3. Will there be insufficient time to diagnose and act?		N		N	
	Will there be more than 50x time needed to act?	N		N	
	Will there be between 5x-50x time needed to act?	Y	0.1	Y	0.1
	Will there be only enough time to diagnose or act?				
	Will the system always be fully staffed?				
4. Will procedures exist?		Y		Y	
	Will procedures be complete?	Y	1	Y	1
	Will procedures be symptom or diagnosis oriented?				
5. Will human machine interface be misleading?		N		N	
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	Y		Y	
	Will the system function be designed to support the human in any adverse physical environment?	N	10	N	10
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?				
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?				
6. Will the work block satisfy at least 3 of the 5 following conditions?		Y	1	Y	1
	a. Tasks are prioritized for the human				
	b. Diagnostic information is presented by the system				
	c. Controls and switches are clear and easily accessible				
	d. Instrumentation and warning systems are designed with the human in mind.				
	e. The system will always be fully staffed				
	Will at least 2 of the above conditions apply?				
7. Will all operators be trained on and retain knowledge on this work block?		Y		Y	
	Will only operators with previous experience operate this system?	N	3	N	3
8. Could any system operator ever experience extreme stress?		N		N	
	Could any system operator ever experience high stress?	Y	2	Y	2
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		Y	5	Y	5
	Will every supervisor perform and communicate continuous risk assessments?				
	Will organizational culture always be exceptionally good?				

E. INADVERTENT ECDIS SHUTDOWN HUMAN ERROR PROBABILITY

		6 Inadvertent shutdown	
		6 Inadvertent ECDIS shutdown	**6 Inadvertent ECDIS shutdown**
1. Is the human mainly making decisions or taking action?		Action	0.001
2. Will operators who are not physically or mentally fit for duty always be prevented from working?		N	
	Will operators always be excluded from duty if injured, fatigued, or while medicated?	N	5
3. Will there be insufficient time to diagnose and act?		N	
	Will there be more than 50x time needed to act?	N	
	Will there be between 5x-50x time needed to act?	N	
	Will there be only enough time to diagnose or act?	N	
	Will the system always be fully staffed?	Y	1
4. Will procedures exist?		Y	
	Will procedures be complete?	Y	1
	Will procedures be symptom or diagnosis oriented?		
5. Will human machine interface be misleading?		Y	
	Will the system function be designed to address ergonomics including workspace compatibility, seating, controls, switches, and compatibility with any personal protective equipment?	Y	
	Will the system function be designed to support the human in any adverse physical environment?	N	10
	Will the system function be designed to eliminate misinterpretation of instrumentation and visual/auditory cues and warnings?		
	Will the controls, switches, communication equipment, personal equipment, and workspace be adequate?		
6. Will the work block satisfy at least 3 of the 5 following conditions?		Y	1
	a. Tasks are prioritized for the human	Y	
	b. Diagnostic information is presented by the system		
	c. Controls and switches are clear and easily accessible		
	d. Instrumentation and warning systems are designed with the human in mind.		
	e. The system will always be fully staffed		
	Will at least 2 of the above conditions apply?		
7. Will all operators be trained on and retain knowledge on this work block?		Y	
	Will only operators with previous experience operate this system?	N	3
8. Could any system operator ever experience extreme stress?		N	
	Could any system operator ever experience high stress?	Y	2
9. Could the organizational culture ever be fast paced, demand a high workload, or be understaffed for the amount of tasking?		Y	5
	Will every supervisor perform and communicate continuous risk assessments?		
	Will organizational culture always be exceptionally good?		

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AcqNotes. 2018. “Acquisition Process: Milestone B.” May 24, 2018. http://acqnotes.com/acqnote/acquisitions/milestone-b#:~:text=Milestone%20B%20is%20considered%20the,defined%20Entrance%20and%20Exit%20Criteria.

Angerman, William S. 2004. “Coming Full Circle With Boyd’s OODA Loop Ideas: An Analysis of Innovation, Diffusion, and Evolution.” Master’s thesis, Air Force Institute of Technology. https://apps.dtic.mil/dtic/tr/fulltext/u2/a425228.pdf.

Baker, Clifford C., and Ah Kuan Seah. 2004. “Maritime Accidents and Human Performance: The Statistical Trail.” In *MarTech 2004: Proceedings of the International Conference* 225–240. Singapore.

Basnyat, S., N. Chozos, C. Johnson, and P. Palanque. 2006. “Incident and Accident Investigation Techniques to Inform Model-Based Design of Safety-Critical Interactive Systems.” *Interactive Systems: Design, Specification, and Verification* 3941: 51–66.

Bauk, S., and R. Radlinger. 2013. “Inciting the Development of Engaging Screencasts in Teaching ECDIS.” In *Marine Navigation and Safety of Sea Transportation Advances in Marine Navigation*, edited by Adam Weintrit, 29–36. Leiden: CRC Press/Balkema.

Bilbro, Jason. 2013. “An Inter-Rater Comparison of DOD Human Factors Analysis and Classification System (HFACS) and Human Factors Analysis and Classification System Maritime (HFACS-M).” Master’s thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/37586.

Blanchard, Benjamin S., and W. J. Fabrycky. 2011. *Systems Engineering and Analysis*. 5th ed. Boston: Prentice Hall.

Boring, Ronald, and Harold Blackman. 2016. *A Short Course on Human Reliability Analysis*. Idaho National Laboratory.

Boring, Ronald, and David Gertman. 2016. *P-203: Human Reliability Analysis (HRA) Training Course*. Idaho National Laboratory.

Buede, Dennis M., and William D. Miller. 2016. *The Engineering Design of Systems: Models and Methods*. 3rd ed. Hoboken, NJ: Wiley.

Bye, Rolf J., and Asbjørn L. Aalberg. 2018. “Maritime navigation accidents and risk indicators: An exploratory statistical analysis using AIS data and accident reports.” *Reliability Engineering and System Safety 176*: 174–186. https://doi.org/10.1016/j.ress.2018.03.033.

Chairman of the Joint Chiefs of Staff. 2018. “Charter Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS).” Chairman of the Joint Chiefs of Staff Instruction 5123.01H. Washington, DC: Joint Chiefs of Staff.

Chen, Shih-Tzung, and Yu-Hsin Chou. 2012. “Examining Human Factors for Marine Casualties Using HFACS - Maritime Accidents (HFACS-MA).” In *2012 12th International Conference on ITS Telecommunications* 391–96. IEEE. https://doi.org/10.1109/ITST.2012.6425205.

Davidson, P. S. 2017. *Comprehensive Review of Recent Surface Force Incidents.* Norfolk, VA: U.S. Fleet Forces Command, Department of the Navy.

De Felice, F., A. Petrillo, and F. Zomparelli. 2016. “A Hybrid Model for Human Error Probability Analysis.” *8th IFAC Conference on Manufacturing Modelling, Management and Control* 49 (12): 1673–78. https://doi.org/10.1016/j.ifacol.2016.07.821.

Defense Acquisition University. 2011. *Defense Acquisition Guidebook.* Fort Belvoir, VA: Defense Acquisition University.

Department of Defense. 2011. *Logistics Assessment Guidebook.* Washington, DC: Department of Defense.

Department of Defense. 2015. *Operation of the Defense Acquisition System*. DOD Instruction 5000.02. Washington, DC: Department of Defense.

Department of Defense. 2019. *Design Criteria Human Engineering*. Military Standard 1472G, Change 1. Washington, DC: Department of Defense.

Ergai, Awatef. 2013 “Assessment of the Human Factors Analysis and Classification System (HFACS): Intra-rater and Inter-rater Reliability.” PhD diss., Clemson University.

Federal Aviation Administration (FAA). 2019. *Boeing 737 MAX Flight Control System—Observations, Findings, and Recommendations*. Joint Technical Authority Review. https://www.faa.gov/news/media/attachments/Final_JATR_Submittal_to_FAA_Oct_2019.pdf.

Federal Aviation Administration. 2020. “Press Release—FAA Administrator Dickson Testifies before Senate on Boeing 737 MAX.” June 17, 2020. https://www.faa.gov/news/press_releases/news_story.cfm?newsId=25057.

Fein, Geoff. 2005. “New Navigation System Will Save Navy Money, Time and Paper.” *Defense Daily; Potomac* 227 (9): 1–4. https://search.proquest.com/docview/234071193.

Filipkowski, D. 2013. “See More—Analysis of Possibilities of Implementation AR Solutions During Bridge Watchkeeping.” In *Marine Navigation and Safety of Sea Transportation Advances in Marine Navigation*, edited by Adam Weintrit, 255–260. Leiden: CRC Press/Balkema.

Franciosi, Chiara, Valentina Di Pasquale, Raffaele Iannone, and Salvatore Miranda. 2019. “A Taxonomy of Performance Shaping Factors for Human Reliability Analysis in Industrial Maintenance.” *Journal of Industrial Engineering and Management* 12 (1). https://doi.org/10.3926/jiem.2702.

Fukuoka, Koji. 2019. “Contributing Factors of Accident Occurrence.” In *Safer Seas: Systematic Accident Prevention*, 1st ed., 37–109. CRC Press. https://doi.org/10.1201/9780429424250-4.

Gertman, D. I., H. S. Blackman, J. L. Marble, J. C. Byers, and C. L. Smith. 2005. “The SPAR-H Human Reliability Analysis Method.” NUREG/CR-6883/INL/EXT-05-00509. Washington, DC: Department of Energy.

Giachetti, Ronald. 2016. *Systems Engineering Thesis Method*s. Monterey, CA: Naval Postgraduate School. https://www.nps.edu/documents/106186412/0/ThesisInSE-4/34166545-3579-454c-9653-14fc26688adb.

Giuntini, R. E. 2000. “Mathematical Characterization of Human Reliability for Multi-Task System Operations.” *2000 IEEE International Conference on Systems, Man and Cybernetics*, 2 (0):1325–1329. Piscataway, NJ: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICSMC.2000.886037.

Greiner, Michelle C., David R. Stark, and Jeffrey L. Girsch. 2019. “How Would Bowditch Navigate Today? The Centuries-Old Quest for Resilience in Navigation.” *Johns Hopkins APL Technical Digest* 34 (4): 431–440. https://www.jhuapl.edu/Content/techdigest/pdf/V34-N04/34-04-Greiner.pdf.

Griggs, Forrest J. 2012. “A Human Factors Analysis and Classification System (HFACS) Examination of Commercial Vessel Accidents.” Master’s thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/17373.

Groth, Katrina. 2009.”A Data-Informed Model of Performance Shaping Factors for Use in Human Reliability Analysis.” PhD diss., University of Maryland, College Park. https://drum.lib.umd.edu/bitstream/handle/1903/9975/Groth_umd_0117E_10944.pdf.

Havlikova, Marie, and Sona Sediva. 2012. “Reliability analysis of the human operator.” In *Proceedings of 13th International Carpathian Control Conference*. May 2012: 209–214. https://doi.org/10.1109/CarpathianCC.2012.6228641.

Hermann, Thomas. 2014. “Revisiting Socio-technical System Design.” In *Proceedings of the 2014 European Conference on Cognitive Ergonomics*. September 2014: 1. http://dx.doi.org/10.1145/2637248.2637251.

Hollnagel, Erik. 1998. *Cognitive Reliability and Error Analysis Method (CREAM)*. London: Elsevier Science. https://doi.org/10.1016/B978-0-08-042848-2.X5000-3.

Institute of Electrical and Electronics Engineers. 2017. “IEEE Guide for Incorporating Human Reliability Analysis into Probabilistic Risk Assessments for Nuclear Power Generating Stations and Other Nuclear Facilities.” IEEE Standard 1082–2017. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

International Civil Aviation Organization. 2012. *Safety Management Manual*. 2nd ed. Doc 9859. Montreal: International Civil Aviation Organization.

International Council on Systems Engineering. n.d. “Definition of a System: General Case.” Accessed July 29, 2020. https://www.incose.org/about-systems-engineering/system-and-se-definition/general-system-definition.

International Maritime Organization. 2004. *Performance Standards for the Presentation of Navigation-Related Information on Shipborne Navigational* Displays. Resolution MSC.191(79). MSC 79/23/Add.2. London: International Maritime Organization.

International Maritime Organization. 2006. Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS). Resolution MSC.232(82). MSC 82/24/Add.2. London: International Maritime Organization.

International Maritime Organization. 2011. *Validation of Model Training Courses*. STW 43/3/1. London: International Maritime Organization.

International Maritime Organization. 2017a. *ECDIS—Guidance for Good Practice*. MSC.1/Circ.1503/Rev.1. London: International Maritime Organization.

International Maritime Organization. 2017b. International Convention of Standards of Training, Certification and Watchkeeping for Seafarers (STCW). STCW.7/ Circ.24. London: International Maritime Organization.

Katsakiori, Panagiota, Aristomenis Kavvathas, George Athanassiou, Stavros Goutsos, and Emmanuel Manatakis. 2010. “Workplace and Organizational Accident Causation Factors in the Manufacturing Industry.” *Human Factors and Ergonomics in Manufacturing & Service Industries* 20 (1): 2–9. https://doi.org/ 10.1002/hfm.20154.

King, Raymond E., Timothy Strongin, Jeffrey Lawson, and Erik Kuhlmann. 2015. “The Development and Inter-Rater Reliability of the Department of Defense Human Factors Analysis and Classification System, Version 7.0.” Final Technical Report. USAF School of Aerospace Medicine, Wright-Patterson AFB, Ohio.

Kirwan, Barry. 1996. “The Validation of Three Human Reliability Quantification Techniques — THERP, HEART and JHEDI: Part 1 — Technique Descriptions and Validation Issues.” *Applied Ergonomics* 27 (6): 359–73. https://doi.org/10.1016/S0003-6870(96)00044-0.

Kolaczkowski, A., J. Forester, L. Lois, and S. Cooper. 2005. “Good Practices for Implementing Human Reliability Analysis.” Final Report. NUREG-1792. Washington, DC: Department of Energy.

Kos, S., D. Brčić, and D. Pušić. 2013. “Protection and Risks of ENC Data Regarding Safety of Navigation.” In *Marine Navigation and Safety of Sea Transportation Advances in Marine Navigation*, edited by Adam Weintrit, 49–56. Leiden: CRC Press/Balkema.

L’Her, Guillaume, Douglas L. Van Bossuyt, Bryan M. O’Halloran. 2017. “Prognostic Systems Representation In A Function-based Bayesian Model During Engineering Design.” *International Journal of Prognostics and Health Management* 8 (2): 1–23.

Langford, Gary O. 2012. *Engineering Systems Integration Theory, Metrics, and Methods*. Boca Raton: CRC Press/Taylor & Francis.

Lenahan, Jack, Don Pacetti, Scott Heller, Rebecca Reed, and Paul Mori. 2009. “Interoperability Risk Mitigation Through The Application Of Operational Capability Based Engineering.” In *14th International Command and Control Research and Technology Symposium (ICCRTS)*. http://hdl.handle.net/10945/37497.

Leveson, Nancy. 2004. “A new accident model for engineering safer systems.” *Safety Science* 42 (4): 237–270. https://doi.org/10.1016/S0925-7535(03)00047-X.

Majewicz, Peter J., Paul Blessner, Bill Olson, and Timothy Blackburn. 2020. “Estimating the Probability of Human Error by Incorporating Component Failure Data from User-Induced Defects in the Development of Complex Electrical Systems.” *Risk Analysis* 40 (1): 200–214. https://doi.org/10.1111/risa.12798.

Marine Accident Investigation Branch (MAIB). 2015. “Grounding of oil/chemical tanker Ovit.” January 23, 2015 https://www.gov.uk/maib-reports/grounding-of-oil-chemical-tanker-ovit-on-the-varne-bank-in-the-dover-strait-off-the-south-east-coast-of-england.

MAIB. 2017. “Grounding of bulk carrier Muros.” October 19, 2017. https://www.gov.uk/maib-reports/grounding-of-bulk-carrier-muros.

Maritime Institute of Technology and Graduate Studies (MITAGS). 2020. “Electronic Chart Display Information System.” Accessed July 14, 2020. https://www.mitags.org/course/electronic-chart-display-information-system/.

Military Sealift Command (MSC). 2009. Nautical Chart and Publications Allowances. COMSC Instruction 3145.1D. Washington, DC: Military Sealift Command.

MSC. n.d.a “About MSC.” Accessed July 1, 2020. https://www.msc.navy.mil/mission/.

MSC. n.d.b “MSC Personnel.” Accessed July 1, 2020. https://www.msc.navy.mil/people/.

National Research Council. *Crew Size and Maritime Safety*. 1990. Washington, D.C.: National Academies Press.

Naval Sea Systems Command. 2017. “Reliability and Maintainability Engineering (R&ME) Manual.” Design Practices and Criteria Manual. T9070-BS-DPC-010/076-1.

The Nautical Institute. 2009. “200930 ECDIS-assisted grounding.” May 4, 2009. https://www.nautinst.org/resources-page/200930-ecdis-assisted-grounding.html.

The Nautical Institute. 2014. “ECDIS errors caused bulk carrier grounding.” *The Navigator*, February 2014.

Nautilus International. 2020. “ECDIS blamed for LNG carrier grounding off Indonesia.” April 7, 2020. https://www.nautilusint.org/en/news-insight/news/ecdis-blamed-for-lng-carrier-grounding-off-indonesia.

Norman, Donald A. 2005. “Human-Centered Design Considered Harmful.” *Interactions* 12, no. 4: 14–19. https://doi-org.libproxy.nps.edu/10.1145/1070960.1070976.

O’Connor, P. 2008. “HFACS with an Additional Layer of Granularity: Validity and Utility in Accident Analysis.” *Aviation Space and Environmental Medicine* 79 (6): 599–606. https://doi.org/10.3357/ASEM.2228.2008.

Office of the Chief of Naval Operations. 2001. *Implementation of the Electronic Chart Display and Information System-Navy (ECDIS-N) Certification Process*. OPNAV Instruction 9420.2. Washington, DC: Department of the Navy.

Office of the Chief of Naval Operations. 2005. *Navy and Marine Corps Mishap and Safety Investigation, Reporting, and Recordkeeping Manual*. OPNAV Instruction 5102.1D/MCO P5102.1B. Washington, DC: Department of the Navy.

Office of the Chief of Naval Operations. 2011. *Navy Safety and Occupational Health Program Manual*. OPNAV Instruction 5100.23G CH-1. Washington, DC: Department of the Navy.

Office of the Secretary of Defense Manufacturing Technology Program. 2015. *Manufacturing Readiness Level (MRL) Deskbook*. v2.3. Washington, DC: Department of Defense. http://www.dodmrl.com/MRL_Deskbook_V2May_2015.pdf

Papakonstantinou, Nikolaos, Markus Porthin, M. O'Halloran, and D. Van Bossuyt. 2016. "A Model-Driven Approach for Incorporating Human Reliability Analysis in Early Emergency Operating Procedure Development." In *2016 Annual Reliability and Maintainability Symposium (RAMS)* 2016:1–6. IEEE. https://doi.org/10.1109/RAMS.2016.7447977.

Pedersen, Kjartan, Jan Emblemsvåg, Reid Bailey, Janet K. Allen, and Farrokh Mistree. 2000. "Validating Design Methods and Research: The Validation Square." In *Proceedings of 2000 ASME Design Engineering Technical Conferences*. DETC2000/DTM-14579. https://pdfs.semanticscholar.org/bc6a/f0e32ad3e9f0bb317590b72e6f23fe874612.pdf.

Rangra, Subeer, Mohamed Sallak, Walter Schon, and Frederic Vanderhaegen. 2017. "A Graphical Model Based on Performance Shaping Factors for Assessing Human Reliability." *IEEE Transactions on Reliability* 66 (4): 1120–1143. https://doi.org/10.1109/TR.2017.2755543.

Raytheon Anschütz. 2014. *ECDIS 24 Operator Manual*. Germany: Raytheon Anschütz GmBH. https://www.raytheon-anschuetz.com/fileadmin/content/Operation_Manuals/ECDIS/4203_ECDIS_24.pdf.

Reason, James. 1990. "The Contribution of Latent Human Failures to the Breakdown of Complex Systems." *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences (1934-1990)* 327 (1241): 475–84. https://doi.org/10.1098/rstb.1990.0090.

Schmidt, John, Dylan Schmorrow, and Robert Figlock. 2000. "Human Factors Analysis of Naval Aviation Maintenance Related Mishaps." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 44 (22): 775–78. https://doi.org/10.1177/154193120004402273.

Schweighardt, Edward Joseph. 2001. *Electronic Chart Display and Information System-Navy: Analysis and Recommendations*. Master's thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/10894.

Shappell, Scott A., and Douglas A. Wiegmann. 2000. “The Human Factors Analysis and Classification System—HFACS.” Final Report .Washington, DC: Office of Aviation Medicine, U.S. Dept. of Transportation, Federal Aviation Administration.

Shattuck, Lawrence G., and Nita Lewis Miller. 2016. “Extending Naturalistic Decision Making to Complex Organizations: A Dynamic Model of Situated Cognition.” *Organization Studies* 27 (7): 989–1009. https://doi.org/10.1177/0170840606065706.

The Standard Club. 2015. “Standard Safety Special Edition: ECDIS assisted grounding.” *Standard Safety* April 2015. https://www.standard-club.com/media/1738472/standard-safety-special-edition-ecdis-assisted-grounding-april-2015.pdf.

Swain, A. 1987. “Accident Sequence Evaluation Program: Human reliability analysis procedure.” United States. https://doi.org/10.2172/6370593. https://www.osti.gov/servlets/purl/6370593.

Swain, A.D., and H.E. Guttman. 1983. “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.” Final Report. NUREG/CR-1278. Washington, DC: Department of Energy. https://www.nrc.gov/docs/ML0712/ML071210299.pdf

Tan, James, Kevin Otto, and Kristin Wood. 2017. “Relative Impact of Early Versus Late Design Decisions in Systems Development.” *Design Science* 3. https://doi.org/10.1017/dsj.2017.13.

Taranto, Matthew T. 2013. “A Human Factors Analysis of USAF Remotely Piloted Aircraft Mishaps.” Master’s thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/34751.

Ulrich, Karl T., and Steven D. Eppinger. 2016. Product Design and Development 6th ed. New York: McGraw-Hill/Irwin.

United States Coast Guard. 2018. Change 1 to Guidelines on Qualification for STCW Endorsements as Master or Officer in Charge of a Navigational Watch of Vessels of Less than 500 GT Limited to Near-Coastal Waters. COMDTCHANGENOTE 16721, NVIC 13–14. Washington, DC: Department of Homeland Security.

United States Coast Guard. 2020. “USCG Maritime Information Exchange Approved Equipment List.” July 20, 2020. https://cgmix.uscg.mil/equipment/Default.aspx.

Wagner, Daniel H., W. Charles Mylander, and Thomas J. Sanders. 1999. *Naval Operations Analysis*. 3rd ed. Annapolis, Maryland: Naval Institute Press.

Wu, Bing, Xinping Yan, Yang Wang, and C. Guedes Soares. 2017. “An Evidential Reasoning-Based CREAM to Human Reliability Analysis in Maritime Accident Process.” *Risk Analysis* 37 (10): 1936–1957. https://doi.org/10.1111/risa.12757.

Xi, Y.T., Z. L. Yang, Q. G. Fang, W. J. Chen, and J. Wang. 2017. “A New Hybrid Approach to Human Error Probability Quantification–applications in Maritime Operations.” *Ocean Engineering* 138 (July): 45–54. https://doi.org/10.1016/j.oceaneng.2017.04.018.

Yilmaz, H., E. Basar, and E. Yüksekyildiz. 2013. “Investigation of Officers’ Navigation and Port Watches Exposed to Excessive Working Hours.” In *Marine Navigation and Safety of Sea Transportation Advances in Marine Navigation*, edited by Adam Weintrit. Leiden: CRC Press/Balkema.

Yoshimura, Kenji, Takahiro Takemoto, and Nobuo Mitomo. 2015. “The Support for Using the Cognitive Reliability and Error Analysis Method (CREAM) for Marine Accident Investigation.” In *2015 International Conference on Informatics, Electronics Vision (ICIEV)*, 1–4. https://doi.org/10.1109/ICIEV.2015.7334041.

Zhou, Tuqiang, Junyi Zhang, and Dashzeveg Baasansuren. 2018. “A Hybrid HFACS-BN Model for Analysis of Mongolian Aviation Professionals’ Awareness of Human Factors Related to Aviation Safety.” *Sustainability* 10 (12). https://doi.org/10.3390/su10124522.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California