SYSTEMS THEORETIC PROCESS ANALYSIS APPLIED TO AN OFFSHORE SUPPLY VESSEL DYNAMIC POSITIONING SYSTEM

by

Blake Ryan Abrecht

B.S. Systems Engineering with a Focus on Human Factors
United States Air Force Academy, 2014

SUBMITTED TO THE INSTITUTE FOR DATA, SYSTEMS, AND SOCIETY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN ENGINEERING SYSTEMS
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
JUNE 2016

Signature of Author: _____
Engineering Systems Division
06 May 2016

Certified by: _____
Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: _____
John N. Tsitsiklis
Clarence J. Lebel Professor of Electrical Engineering
IDSS Graduate Officer

Page intentionally left blank.

SYSTEMS THEORETIC PROCESS ANALYSIS APPLIED TO AN OFFSHORE SUPPLY VESSEL DYNAMIC POSITIONING SYSTEM

by
Blake Ryan Abrecht

B.S. Systems Engineering with a Focus on Human Factors
United States Air Force Academy, 2014

Submitted to the Institute for Data, Systems, and Society on 06 May, 2016
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Engineering Systems

ABSTRACT

This research demonstrates the effectiveness of Systems Theoretic Process Analysis (STPA) and the advantages that result from using this new safety analysis method compared to traditional techniques. To do this, STPA was used to analyze a case study involving Naval Offshore Supply Vessels (OSV) that incorporate software-intensive dynamic positioning in support of target vessel escort operations. The analysis begins by analyzing the OSVs in the context of the Navy's organizational structure and then delves into assessing the functional relationship between OSV system components that can lead to unsafe control and the violation of existing safety constraints. The results of this analysis show that STPA found all of the component failures identified through independently conducted traditional safety analyses of the OSV system. Furthermore, the analysis shows that STPA finds many additional safety issues that were either not identified or inadequately mitigated through the use of Fault Tree Analysis and Failure Modes and Effects Analysis on this system.

While showing the benefit of STPA through this case study, other general advantages that STPA has relative to traditional safety analysis techniques are also discussed. First, this thesis discusses how STPA generates results that are completely compliant with the requirements for system hazard analysis set forth in MIL-STD-882E and that STPA more completely satisfies the tasks in MIL-STD-882E than traditional safety analysis techniques. Next, the link between STPA and Causal Analysis using Systems Theory (CAST), two Systems Theoretic Application and Model Processes (STAMP) tools is discussed to highlight how using STPA for hazard analysis benefits subsequent accident investigations using the CAST framework.

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

Page intentionally left blank.

ACKNOWLEDGEMENTS

There are many people that I would like to thank who have helped me so much during my time here at MIT. Thank you to Dr. John Thomas, Dr. Dan Montes, Kip Johnson, Dajiang Suo, Jonas Helfer, Aubrey Samost, David Horney, John Mackovjak and everyone else in the Systems Engineering Research Lab who has made the lab a welcoming and enjoyable place to conduct research. Thank you also to the entire Air Force cohort here at MIT who are seeking advanced degrees. Your friendships have made the time here at MIT fly by.

Thank you to the Navy group who has provided invaluable technical expertise and feedback regarding Offshore Supply Vessels and dynamic positioning in particular. Steve Cumber, Stephen Sells, John Fish, Jason Fewkes, Jose Balderrama, Tim Cauthen, Joe Giaquinto, John Graziose, and everyone else who had a part in this project: thank you for your support. Thank you also to John Kuconis, Dave Dunmeyer, and everyone at Lincoln Laboratory who made my time out here possible through the Lincoln Laboratory Military Fellowship Program.

I am very thankful for my parents, Derric and Marcey Abrecht, and my brother, Evan Abrecht who have allowed me to vent my frustrations to them during the graduate school process. Without your guidance, support, and the wonderful examples you have set for me, I would never have been able to experience the level of success that I have up to this point in my life.

To my beautiful wife Julie: thank you for always putting up with me and for making my final year at MIT a blast. Thank you for hopping on this roller coaster ride with me. I cannot wait to see how our relationship grows as we move on from MIT into the operational Air Force and beyond. I love you more than words can describe.

Finally, I owe a huge debt of gratitude to my advisor- Professor Nancy Leveson for allowing me the opportunity to attend MIT and for introducing me to a new way of thinking about systems engineering and systems safety. Looking back at my statement of interest that I submitted during the MIT application process, I am amazed to see how my understanding of systems engineering and systems safety has evolved and matured because of your guidance in just two short years.

Page intentionally left blank.

Table of Contents

List of Figures

List of Tables

Page intentionally left blank.

1. Introduction

1.1. Motivation

Traditional safety analysis techniques, based on reliability theory, are often used by organizations to analyze their systems. These traditional methods were created forty or more years ago to address systems that included little or no software and were much less complex than systems being designed and fielded today. Attempts have been made to integrate the analysis of software and modern technologies into these traditional analysis methods; however, the underlying assumptions that make up the foundation of these techniques do not match current technology and fail to address many causes of accidents. As a result, these traditional methods are unable to adequately identify and address all the safety issues that must be mitigated for safe system operation. Systems Theoretic Process Analysis (STPA), a new hazard analysis method based not on reliability theory but on systems theory, was created to address this problem.

To demonstrate the effectiveness of STPA relative to traditional safety analysis techniques that are based on reliability theory, STPA was used to analyze Naval Offshore Supply Vessels (OSV) that utilize software-intensive dynamic positioning (DP) in support of target vessel escort operations. The use of STPA on this case study is relevant because “the industry trend is for dynamically positioned [vessels] to upgrade their DP systems with increased redundancy and hardware” [1] to promote safety. Whereas this focus promotes the use of safety analysis techniques based on reliability theory, this focus consequently fails to meaningfully address non-failure problems. STPA differs from traditional safety analysis techniques by treating safety as a control problem rather than a component failure problem. [2] Because of this much broader scope, STPA identifies and addresses not only component failures that can lead to a hazard but also system design flaws that current failure-based methods cannot. Furthermore, STPA includes in the analysis both the human operators of the system and software components, addressing both in a meaningful way and placing as much or more importance on their behavior relative to the electromechanical components of the system.

1.2. Background

DP systems are currently used in a number of different applications to provide a means of automatic vessel maneuvering and station keeping. While DP systems were first utilized in the early 1960's through the use of "conventional PID controllers in cascade with low-pass and/or notch filters" the technology advanced in the 1970's with the use of "more advanced control techniques…based on linear optimal control and Kalman filter theory" [3]. Today, DP systems are continuing to advance in sophistication and have been used on a wide array of vessels worldwide to include "survey vessels, drilling ships, work boats, semi-submersible floating rigs, diving support vessels, cable layers, pipe-laying vessels, shuttle tankers, trenching and dredging vessels, [and] supply vessels" [3].

The term DP system can refer to a number of different things. Some definitions of a DP system only refer to the actual control system of the vessel. Other definitions use the term DP system to "describe all vessel control systems required to keep position" such as "the power generation, power distribution, power management, and the thrusters as well as the control system itself" [1]. Throughout this thesis, the term DP system considers the various levels of automation that the DP system can operate with, the various sensors that allow for dynamic positioning to occur, and the signal processing unit within the DP system that communicates with the vessel's control subsystems, which are classified as separate system component (i.e. thrusters).

The American Bureau of Shipping (ABS) produces guidelines and regulations for vessels that utilize DP systems. As such, the ABS classifies DP systems into four separate categories. These categories include [4]:

- **DPS-0:** "For vessels, which are fitted with centralized manual position control and automatic heading control system to maintain the position and heading under the specified maximum environmental conditions."
- **DPS-1:** "For vessels, which are fitted with a dynamic positioning system which is capable of automatically maintaining the position and heading of the vessel under specified maximum environmental conditions having a manual position control system."

- **DPS-2:** “For vessels, which are fitted with a dynamic positioning system which is capable of automatically maintaining the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault, excluding a loss of compartment or compartments.”
- **DPS-3:** “For vessels, which are fitted with a dynamic positioning system which is capable of automatically maintaining the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault, including complete loss of a compartment due to fire or flood.”

For the case study discussed in this thesis, the OSVs that are analyzed incorporate a Class 2 DP system (DPS-2) and have the following relevant features [5]:

- Integrated 3-axis joystick control
- Automatic heading control
- Automatic position control
- Fully redundant control system
- Transit mode (DP system operating in assisted manual mode)
- Target follow mode (DP system operating in fully automatic mode)

The OSVs use the Class 2 DP system and these relevant features to provide automatic maneuvering of the OSV relative to a target vessel during OSV-target vessel escort operations.

It is vital to understand the nature of OSV-target vessel escort operations. In traditional applications where dynamic positioning is incorporated, such as in deep sea oil drilling where the vessel must maintain station relative to an almost static platform, one of the biggest threats to the reliability of the DP system is harsh waters [6]. However, during OSV-target vessel escort operations, while environmental conditions are a factor of concern, the target vessel itself poses another unique challenge that must be overcome by the DP system due to the speeds at which target following can occur. Given the extremely dynamic nature of escort operations and the additional stresses that the DP system can be subjected to during such an application at high speeds, it is paramount to understand the hazards associated with the use of a DP system during these escort operations.

Because of a reliance on traditional hazard analysis techniques, the identification of hazards that are associated with DP system use remain rather limited in scope and focus mainly on failures. In response to this reality, D. F. Philipps et al. stated in a 1998 Dynamic Positioning Conference that "regardless of the amount of hardware redundancy installed, all control systems could fail in an instant even if they were thought to be redundant" [1]. While this statement seeks to highlight that system redundancy alone is inadequate, the declaration hints at the failure-based focus surrounding DP system use. In contrast, Norwegian Shipowners' Association Captain H. Verhoeven et al. made the following assertion at a 2004 Dynamic Positioning Conference:

> To improve the safety of DP operation thus requires that all major elements in this human-machine system be taken into account. This requires that safety modeling and analyses should include not only technical system failures (e.g. covered by DP system FMEA studies), but also human operational failures, and interactions between these two types of failures. There has been limited risk modeling work carried out to meet the above requirement. Most studies on the safety of DP operation have been concentrated on DP technical system failures. Consequently, risk control and reduction measures address mainly the technological improvements. This may be effective at one time, but given the significant improvement of DP technology in recent years, there is a need to search potential improvements from a broader perspective, which particularly should take human and organizational contributions into account. [6]

The use of STPA during the hazard analysis process accounts for these human and organizational contributions to hazards in ways that traditional techniques cannot and also looks beyond failures to identify scenarios where hazards occur without failures. In doing so, STPA is able to address deficiencies that are inherent in traditional hazard analysis techniques and can be used to help design safety into systems.

1.3. Analysis Techniques

Traditional analysis techniques based on reliability theory have been mentioned in previous sections. While there are many hazard analysis techniques that are widely used, only two traditional hazard analysis techniques were chosen to compare the results obtained through the use of STPA on this case study. These two techniques, Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) were chosen as a standard of comparison because they have been used in previous, independently conducted analyses to assess the OSV DP system that

is part of this case study. Each of these techniques is briefly introduced in the following sections. Furthermore, given that both an STPA case study and CAST case study are presented in later chapters, both methods are also briefly introduced in the following sections.

1.3.1. Fault Tree Analysis

According to the Reliability Design Handbook, Fault Tree Analysis (FTA) is a "procedure that can be characterized as an iterative documented process of a systematic nature performed to identify basic faults, determine their causes and effects, and establish their probabilities of occurrence" [7]. Pioneered by Bell Laboratories in the 1960's, FTA has received wide popularity in industry and has become a widely used process in safety analysis and system reliability. FTA can be used for a number of different purposes, including "identifying potential causes of system failures before the failures actually occur" [8]. It "can also be used to evaluate the probability of a top event using analytical or statistical methods" [8]. To complete a FTA, the analyst begins with a general conclusion such as a fault condition and then constructs a logic diagram to postulate specific causes of the general conclusion. The general output of the FTA includes a "logic diagram that depicts all basic faults and conditions that…result in the hazardous condition(s)…a probability of occurrence for each hazardous condition… [and] a detailed fault matrix that provides…all basic faults, their occurrence probabilities and criticalities" [7]. For more detailed information regarding FTA, the Reliability Design Handbook can be referenced.

1.3.2. Failure Modes and Effect Analysis

FTA is often used in conjunction with other analysis techniques when analyzing a system. Figure 1 shows the relationship between FTA and FMEA.

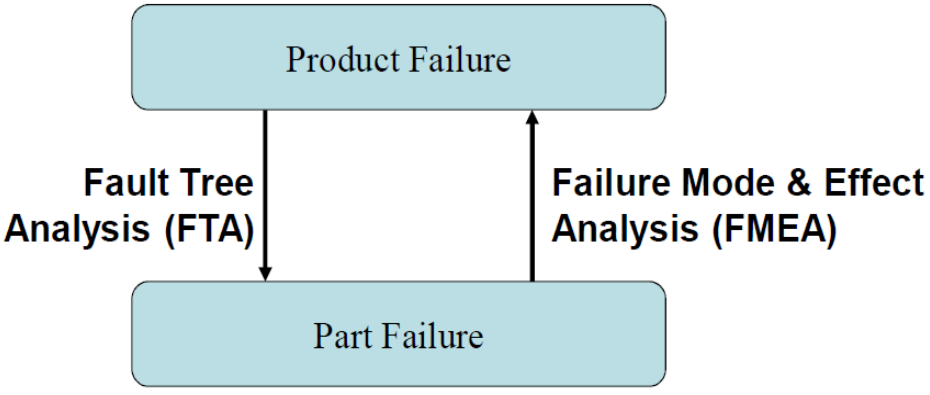


Figure 1: Relationship between FMEA & FTA [9]

Failure Modes, Effect, and Criticality Analysis (FMECA) was developed by NASA in the 1960's for use on the Apollo space program and consists of two parts, FMEA and criticality analysis [10]. The FMEA process consists of defining the system to be analyzed, constructing a logic block diagram that includes component reliability and analyzing failure modes of the system components and the effect that the failure modes have on the system [10]. According to NASA guidance, an assumption is made "that only the failure under consideration has occurred" and that "when redundancy or other means have been provided in the system to prevent undesired effects of a particular failure, the redundant element is considered operational and the failure effects terminate at this point in the system" [10]. As such, experts consider a good FMEA as one that "identifies known and potential failure modes… the causes and effects of each failure mode…prioritizes the identified failure modes according to the risk priority number…[and] provides for problem follow-up and corrective action" [11]. References 10 and 11 can be accessed for more detailed guidance on the use of FMEA.

1.3.3. Systems Theoretic Process Analysis

STPA is a relatively new hazard analysis technique that treats safety as a problem that involves unsafe control and the violation of system safety constraints. To do this, STPA begins by assessing the organizational control structure in which the system operates and then models the system's functional control structure, showing the hierarchical arrangement of feedback control loops within the system [2]. These feedback control loops are then rigorously analyzed to identify control actions that are unsafe (lead to a hazard) when not provided under certain conditions, control actions that are unsafe when provided under certain conditions, control actions that are unsafe when provided with incorrect timing or in the wrong order, and control actions that are unsafe when stopped too soon or provided for too long [2]. By analyzing the unsafe control actions that are found, system-level safety requirements and constraints are identified and causal scenarios that can lead to the occurrence of these control actions are generated to determine in more detail exactly how each unsafe control action can occur. From these scenarios, more detailed safety requirements are generated for use by designers in eliminating, preventing, or mitigating the unsafe control actions in the design and operation of the system. For more detailed information regarding the use of STPA, reference Chapter 8 in Engineering a Safer World.

1.3.4. Causal Analysis Based on Systems Theory

CAST is an accident analysis technique that provides "a framework or process to assist in understanding the entire accident process and identifying the most important systemic causal factors involved" in the accident [2]. The general approach that CAST uses consists of the following steps. First, the system and hazards involved in the loss are identified. Next, safety constraints and requirements associated with the hazard are identified and the existing safety control structure in place for the system is documented. Events leading to the loss are identified and the loss is analyzed at the physical system level as well as within the physical system level by looking at the relationship between system components and controllers. The analysis identifies the safety-related responsibilities of each system controller, potential flawed process models that contributed to unsafe control actions, and the context that led to the occurrence of these unsafe decisions. The output of the CAST process is safety recommendations and requirements that can be imposed on the system to promote safe operation [2]. For more detailed guidance on the use of CAST, Chapter 11 of Engineering a Safer World can be referenced.

1.4. Objectives and Approach

The thesis is organized around three primary objectives. These objectives are:

- **Apply STPA to a case study involving a software-intensive dynamic positioning system used on Offshore Supply Vessels for target vessel escort operations.**

  Chapter 2 uses STPA to perform a system-level hazard analysis of an OSV DP system. The functional relationship between the OSV DP system's components is modeled and the relationship between each applicable controller is analyzed to identify unsafe control actions and causal scenarios that can lead to the occurrence of a hazardous system state and potentially an accident or loss.

- **Compare the results obtained using STPA on the case study to independently conducted FTA and FMEA of the same system and show that the results are compliant with Department of Defense guidance for system hazard analysis.**

  Chapter 3 assesses the results obtained through the case study presented in Chapter 2 and compares the results to results obtained through independently conducted FTA and FMEA. The comparison begins by assessing the problem space that each method focuses on and then

discusses three specific examples that highlight generic differences in the analysis techniques as well as specific differences in the results obtained through the use of the three methods. After comparing STPA to FTA and FMEA, MIL-STD-882E, the Department of Defense guidance for hazard analysis is analyzed to show how STPA can be used to fulfill the requirements contained within this document.

- **Apply CAST to a case study involving an OSV incident that resulted from the use of a DP system and discuss how STPA can be used to inform the CAST accident analysis process.**

Chapter 4 uses CAST to analyze a fictionalized accident involving two OSVs that were utilizing DP systems and that collided during OSV testing. The CAST process is used to analyze the accident and generate safety recommendations. Given that STPA is used for hazard analysis and CAST is used for accident analysis, the link between the two methods is discussed to show how using STPA for hazard analysis reduces the amount of work that must be done to perform a subsequent accident analysis for the same system.

Page intentionally left blank.

2. STPA Case Study

This chapter provides a systems theoretic process analysis of the OSV DP system. Throughout the case study, the goal of STPA is to provide a systems-level hazard analysis of the DP system to identify scenarios that could result in unsafe control actions, which in turn could lead to hazards and ultimately an accident or loss. Each part of the STPA process is discussed incrementally and is dissected accordingly; however, it is important to note that because STPA is an iterative process, the analysis did not necessarily occur in the linear fashion in which it is presented.

First, the accident and hazard definitions that guided the analysis are presented. Next, a generic organizational control structure is presented that shows where the OSV fits into the Navy's overall structure. The OSV then receives further focus and the functionally related components within the OSV are modeled. The functional relationships between these components are analyzed in depth to identify sources of unsafe control and scenarios that can lead to unsafe control actions. These identified unsafe control actions and causal scenarios allow for safety constraints to be identified as well as possible safety requirements to be generated.

2.1. Accidents and Hazards

The first step in the STPA process is to identify the accidents that need to be prevented and the hazardous system states that can lead to these accidents. STPA defines an accident as "an undesired and unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc." [2]. For the purpose of this case study, three relevant accidents were defined:

A-1: Multi-vessel collision

- **A-1.1:** OSV/ OSV collision
- **A-1.2:** OSV / target vessel collision

A-2: OSV collision with external structure

- **A-2.1:** OSV collision with (static object) bridge
- **A-2.2:** OSV collision with (dynamic object) buoy

A-3: OSV running aground (shore or ocean floor)

STPA defines a hazard as “a system state or set of conditions that together with a worst-case set of environmental conditions will lead to an accident (loss)” [2]. Table 1 defines the applicable hazards that could lead to the defined accidents. Table 1 also illustrates the high-level safety constraints associated with these top-level hazards.

Table 1: Hazards and derived high-level safety constraints

Hazard	Definition	Safety Constraint (Requirement)
H1: Loss of minimum separation. *Can lead to:* *A-1, A-2, A-3*	Minimum separation is defined as the OSV coming into contact with another hard body/object (such as the terrain, an external structure, or another vessel). It is also defined as violating the current safe operating envelope.	The OSV must not violate minimum separation.
H1.1: Loss of minimum separation with the terrain. *Can lead to: A-3*		The OSV must not violate minimum separation with the surrounding terrain.
H1.2: Loss of minimum separation with an external structure. *Can lead to: A-2*		The OSV must not violate minimum separation with an external structure.
H1.3: Loss of minimum separation with another vessel. *Can lead to:* *A-1.1, A-1.2*		The OSV must not violate minimum separation with another vessel.
H2: Loss of OSV control. *Can lead to:* *A-1, A-2, A-3*	Loss of control is defined as the OSV operator being unable to control the OSV or the OSV responding in a manner unforeseen by the OSV Crew. Loss of control can be recoverable, unrecoverable, detected, and/or undetected.	There must not be a loss of OSV vessel control.

2.2. Overall Organizational Requirements

With the accidents and hazards identified, the next step in the STPA process is to analyze where the system fits into the overall organizational structure. A generic organizational safety control structure for the Offshore Supply Vessel/Target Vessel Escort Operation System is shown below in Figure 2.

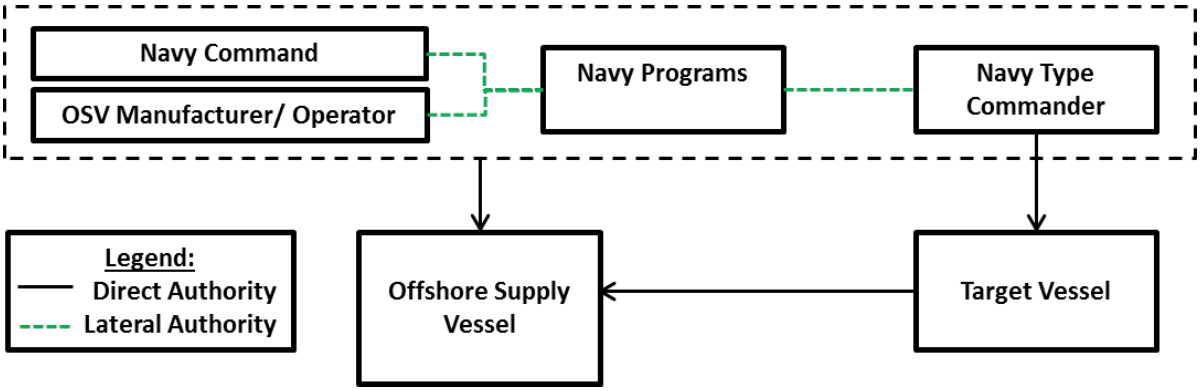


Figure 2: OSV/Target Vessel Escort Operation Organizational Safety Control Structure

The overall system goal for this organizational safety control structure, as applicable for this case study, is to provide traceable guidance, regulations, and orders for Navy systems operations. As such, each component within the organizational control structure is analyzed in terms of safety-related responsibilities.

For the purpose of this case study, the Navy Type Commander has direct command of and communication with the target vessel's Commanding Officer (CO) and is responsible for passing directives, guidance, training, and support for target vessel operations. The Navy Command owns the OSVs and has authorized the OSV manufacturer to act as the OSV operator for the OSVs used in the target vessel escort operations system. Thus, the Navy Command and the OSV manufacturer/operator, along with the Navy Programs are bi-laterally responsible for passing guidance and training to the OSV crewmembers. During testing and mission operations, the target vessel Commanding Officer has ultimate authority over the OSV providing escort. The OSV Master is responsible for adhering to target vessel CO commands and may also choose to breakaway at his/her own discretion to ensure the safety of the vessels.

Because STPA can be used to derive emergent property requirements for a system, the STPA method can be used to analyze the organizational control structure in more detail to find unsafe control actions at this level. However, the focus of this case study does not delve into the unsafe control actions at the organizational-level and instead focuses on sources of unsafe control at the OSV system-level.

2.3. Functional Control Structure

One of the advantages of STPA is that it allows for analysis of the system at different hierarchical levels of decomposition. Figure 3 focuses on the Offshore Supply Vessel component in the organizational control structure and shows the high-level control structure at the OSV system-level.

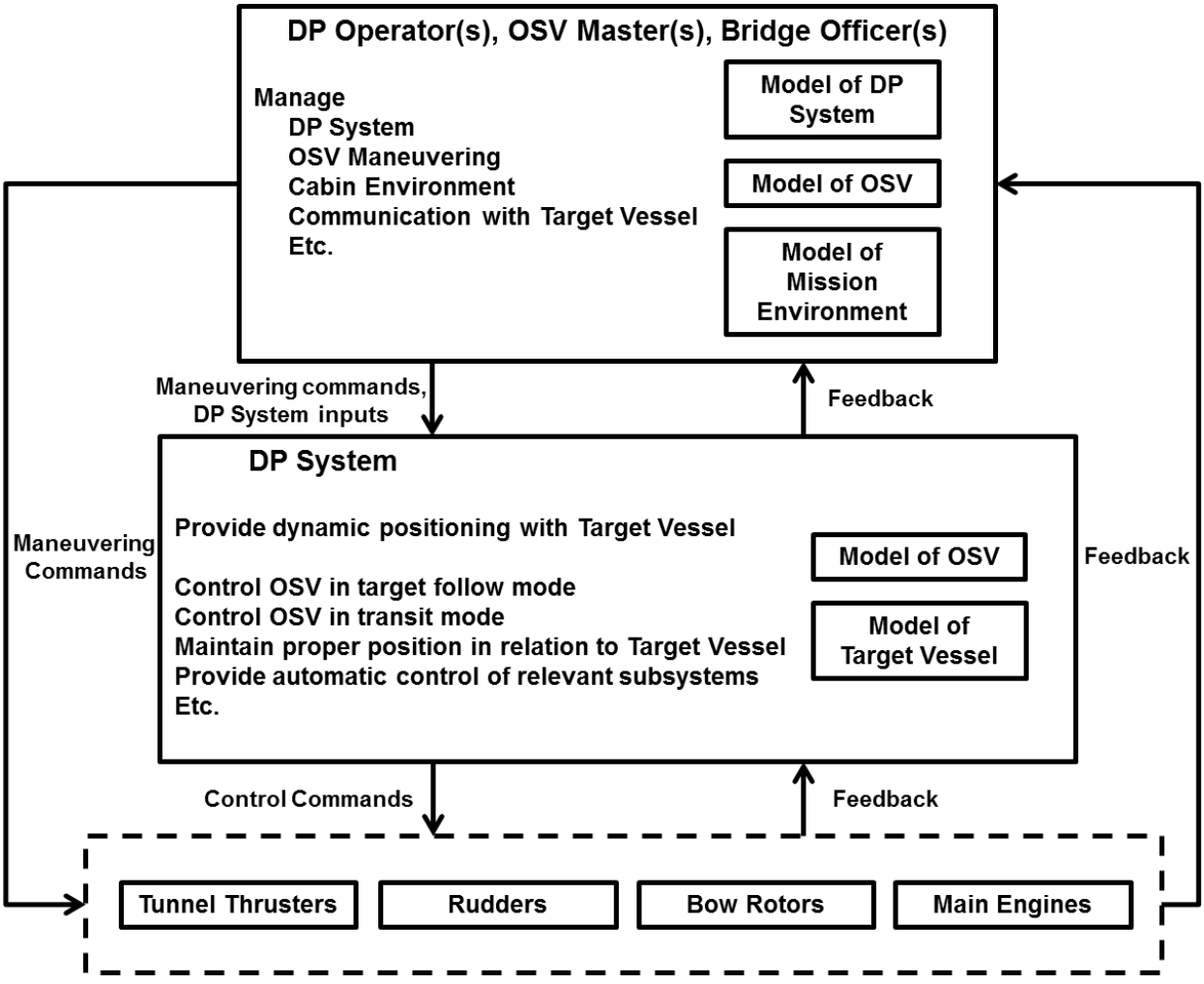


Figure 3: High-Level Control Structure at the OSV Level

This high-level control structure shows the relationship between the main components in the OSV system. Within the OSV system, DP Operator(s), OSV Master(s), and Bridge Officers(s) are responsible for maneuvering the OSV, managing the DP system, controlling the cabin environment in the OSV, and communicating with the target vessel during escort operations. In order to perform these tasks, each of these operators has a process model (a model of the current state of the controlled process) of the DP system, the OSV, and the mission environment that informs their decisions and action generation. Depending on the mode of operation, the DP Operator(s), OSV Master(s), and Bridge Officer(s) can control the OSV manually by providing maneuvering commands directly to the OSV's tunnel thrusters, rudders, bow rotors, and main engines. These operators can also control the OSV through the use of the DP system by providing maneuvering commands through the DP system interface and by setting the DP system to provide various levels of automatic control of the OSV. The DP system can thus provide control commands to the OSV control subsystems and has its own process model of the OSV and target vessel that informs its action generation.

It is important to understand the relationship between human and automated controllers. Figure 4 shows the relationship between human and automated controllers in general.

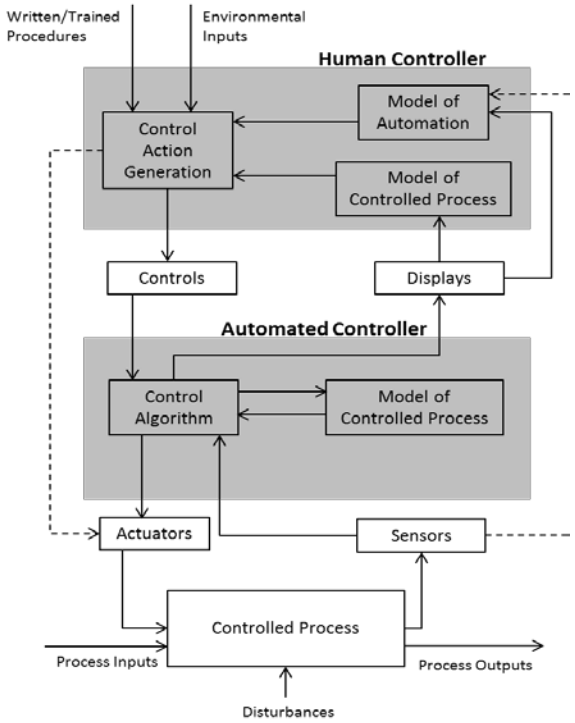


Figure 4: Relationship between Human and Automated Controllers [2]

Automated controllers have a model of the controlled process that is used by the control algorithm within the controller. However, human controllers have a model of the controlled process as well as a model of the automation that informs control action generation, along with various written procedures, training, and environmental inputs. This distinction becomes relevant in the identification of unsafe control actions in subsequent steps in the STPA analysis.

Expanding upon the control structure depicted in Figure 3, Figure 5 shows a more detailed model of the functional control structure for the OSV system.

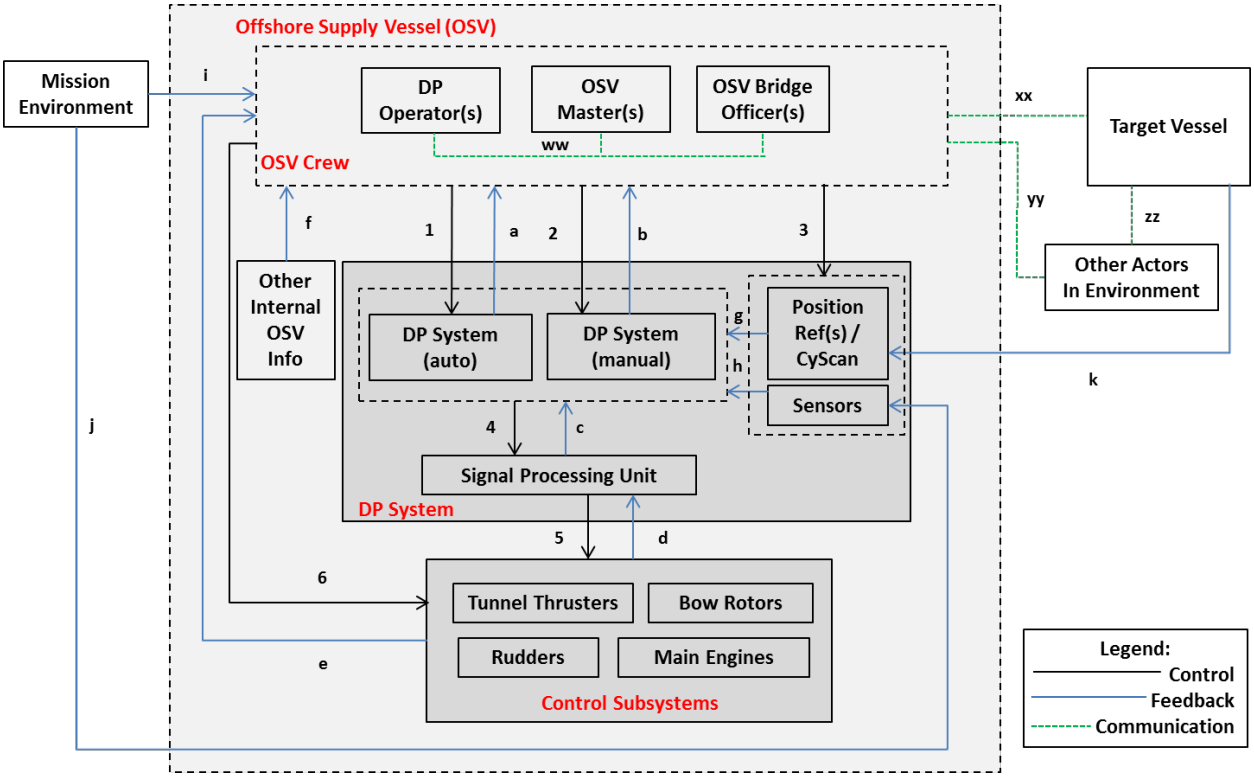


Figure 5: Functional Control Structure for the OSV System

The safety-related responsibilities, control actions, feedback and communication associated with the functional control structure are as follows:

2.3.1. Control Structure Safety-related Responsibilities

OSV Master(s):

- Provide command authority to other members of OSV Crew
- Ensure safe maneuvering of OSV
- Ensure proper functioning of DP system

- Ensure proper setup of DP system and other relevant sensors
- Implement breakaway procedures if necessary for vessel safety
- Maintain communication with target vessel
- Adhere to all commands given by the target vessel

DP Operator(s), Bridge Officer(s)

- Ensure safe maneuvering of OSV
- Ensure proper functioning of DP system
- Ensure proper setup of DP system and other relevant sensors
- Implement breakaway procedures if necessary for vessel safety
- Maintain communication with target vessel
- Adhere to all commands given by the target vessel

DP system (auto and manual)

- Provide safe maneuvering of OSV
- Provide accurate feedback to OSV Crew
- Implement all OSV Crew inputs
- Integrate valid sensor inputs
- Reject invalid sensor inputs

Signal Processing Unit

- Process and implement all received inputs
- Provide accurate feedback regarding control subsystems

Target Vessel

- Maintain communication with OSV providing escort
- Set up target reflectors for CyScan operations
- Command breakaway procedures if necessary

2.3.2. Control Structure Control Actions

1.) OSV Crew → DP system (auto)

- Activate/deactivate DP system (auto)
- Set user configurable parameters

2.) OSV Crew → DP system (manual)

- Activate/deactivate DP system (manual)

- Set user configurable parameters
    - Provide directional commands

3.) OSV Crew → Position Ref(s)/CyScan/Sensors
- Turn CyScan ON/OFF
- Set sensor parameters

4.) DP system → Signal Processing Unit
- Signal directional command

5.) Signal Processing Unit→ Control Subsystems
- Implement directional command

6.) OSV Crew → Control Subsystems
- Activate/deactivate full manual mode
- Provide directional command

2.3.3. Control Structure Feedback

a) DP system (auto) → OSV Crew
- Graphical display information
- Subsystem status/information
- Visual sensory feedback
- Proprioceptive feedback
- Auditory sensory feedback

b) DP system (manual) → OSV Crew
- Graphical display information
- Subsystem status/information
- Visual sensory feedback
- Proprioceptive feedback
- Auditory sensory feedback

c) Signal Processing Unit → DP system
- Actuator Feedback

d) Control Subsystems → Signal Processing
- Raw data

e) Control Subsystems → OSV Crew
- Visual sensory feedback

- Proprioceptive feedback
- Auditory sensory feedback

f) Other internal OSV Info→ OSV Crew
- Graphical display information
- Subsystem status/information
- Visual sensory feedback
- Proprioceptive feedback
- Auditory sensory feedback

g) Position Ref(s)/CyScan → DP system (manual)
- Raw data

h) Other DP system Related Sensors → DP system (manual)
- Raw data

i) Mission Environment→ OSV Crew
- Visual sensory feedback
- Proprioceptive feedback
- Auditory sensory feedback
- Tactile feedback

j) Mission Environment→ Sensors
- Environmental information

k) Target Vessel/ OSV → Position Ref(s)/CyScan
- CyScan reflections

2.3.4. Control Structure Communication

ww) Communication between OSV Crew

xx) Communication between OSV Crew and Target Vessel

yy) Communication between OSV Crew and other actors in the environment

zz) Communication between other actors in the environment and Target Vessel

2.4. Identifying Unsafe Control Actions

With the functional control structure established, unsafe control actions were identified by assessing each respective control loop within the functional control structure.

2.4.1.1. UCAs between the OSV Crew and DP System (auto)

Figure 6 shows the focus on the functional control structure for this section of the analysis.

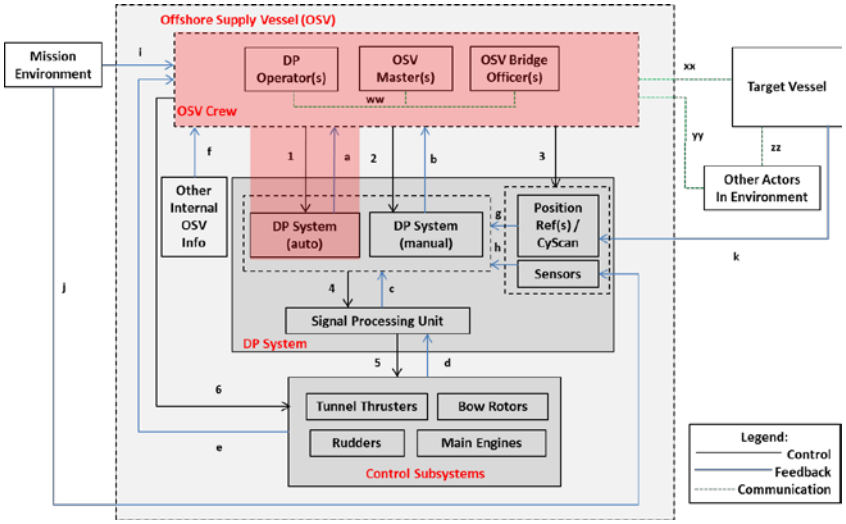


Figure 6: UCA Focus between OSV Crew and DP System (Auto)

Table 2 shows one row of unsafe control actions that were identified between the OSV Crew and the DP system (auto), which refers to the OSV operating in target follow mode. The full list of unsafe control actions identified in this section of the analysis is presented in Appendix A.

Table 2: Partial List of UCAs between OSV Crew and DP System (auto)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Activate DP system (auto)	UCA1: OSV Crew does not activate DP system (auto) when the OSV Crew believes that the DP system (auto) is controlling the OSV.[H-1, H-2]	UCA2: OSV Crew activates DP system (auto) with unsafe parameter set. [H-1, H-2]	UCA4: OSV Crew activates DP system (auto) before prescribed checklist procedures are complete. [H-1, H-2]	N/A
		UCA3: OSV Crew activates DP system (auto) during unsafe sea state. [H-1, H-2]	UCA5: OSV Crew waits to activate DP system (auto) x amount of time after actively relinquishing manual control of the vessel. [H-1, H-2]	

Each identified unsafe control action has traceable safety requirements/constraints that can be incorporated to mitigate the identified unsafe control action. The safety requirements/constraints associated with the five unsafe control actions in Table 2 are as follows:

SC1: The control mode that is controlling the OSV must be depicted at all times. [UCA1]

SC2: The OSV Crew must not activate DP system (auto) with unsafe parameters set. [UCA2]

SC3: The OSV Crew must not activate DP system (auto) during an unsafe sea state. [UCA3]

SC4: The OSV Crew must not activate DP system (auto) before all prescribed checklist procedures have been completed. [UCA4]

SC5: The OSV Crew must not relinquish active control of the OSV until it is verified that automatic operations have been started. [UCA5]

A full list of the safety requirements/constraints associated with the full list of unsafe control actions identified between the OSV Crew and DP system (auto) are presented in Appendix A.

2.4.1.2. Causal Scenario Analysis of Identified UCAs

With the unsafe control actions identified for this section of the analysis, the next step is to analyze each individually and create causal scenarios to determine how each unsafe control action can occur. These causal scenarios can be used to create more specific safety requirements that can be imposed on the system to promote safe operation. A full list of causal scenarios and the associated generated requirements is given in Appendix A. The causal scenarios for the first two identified unsafe control actions listed in Table 2 are presented below.

Unsafe Control Action- UCA1: OSV Crew does not activate DP system (auto) when the OSV Crew believes that the DP system (auto) is controlling the OSV. [H-1, H-2]

Scenario 1: During OSV /Target Vessel escort operations, manual mode is the default mode for OSV control. To implement automatic mode where the DP system has control of the OSV, a number of steps are required to set up the automatic operation. Among the first items on the specific OSV / Target Vessel automatic operations checklist is the general set up page. Furthermore, once general setup is completed, subsequent checklist items are in place for the human operator to complete before transitioning to automatic operations. To begin target following automatic operations, the operator obtains permission to take station, maneuvers the OSV appropriately, checks sensors and other relevant parameters to verify correct operation, and

initializes target follow mode, which transfers control of the OSV to the DP system in automatic mode. Reasons that the OSV Crew might not activate the DP system (auto) could include:

a) Each OSV Crew member believes that another crew member is responsible for checklist items needed to implement DP system (auto). This could occur due to changing crew roles during mode transition.
b) Crew members sign off on checklist items that have not been completed. This could be a result of excessive workload, normalization of deviance, etc.
c) The OSV Crew follows the correct procedures but equipment failure results in the DP system (auto) not being implemented.
d) Depending on the maneuvering characteristics of the OSV, the human operator could incorrectly believe that target follow mode has been initialized when in actuality it has not begun.

Possible requirements for Scenario 1:

1. The active control mode must be depicted to the OSV Crew and noticeable to prevent mode confusion.
2. Information between the two DP consoles must be the same and must accurately portray the DP system state and the OSV operation.
3. The DP system must not change the mode without being commanded to do so by the OSV Crew. Any change in control mode must be audibly and visually annunciated to the OSV Crew.
4. Procedures must be in place that outlines the role of OSV crewmembers in controlling the OSV. If any member of the OSV Crew besides the current active controller changes the control mode for any reason, the change must be communicated among OSV crewmembers.
5. Any component failure that prevents mode changes must be identifiable and give feedback to the OSV Crew that the mode change has not occurred.

Unsafe Control Action- UCA2: OSV Crew activates DP system (auto) with unsafe parameter set. [H-1, H-2]

Scenario 2: The OSV Crew activates the DP system (auto) because the crew believes that the parameter values are safe (the OSV Crew has a flawed process model). Reasons for a flawed process model could include:

a) DP system set up is correct for a different operation, but incorrect for the current operation. This could cause the OSV crewmembers to mistakenly believe the parameter set is correct.
b) The OSV Crew does not notice that a parameter value is unsafe.
c) The OSV Crew changed the parameter value and did not realize that the change was incorrect.
d) The OSV Crew made an invalid parameter change and the DP system reverted to the default parameter value.
e) The OSV Crew performs a checklist item that is not implemented correctly by the DP system.

Possible requirements for Scenario 2:

1. DP system parameters must be verified and confirmed before activating DP system (auto) to ensure that input parameters promote safe vessel operation.
2. Means must be available to determine if parameter values in DP system setup are safe.
3. Default parameter values should be distinguishable from non-default values so that the OSV Crew knows when a parameter value is set to the default value.
4. The OSV Crew must receive feedback if an invalid parameter value is input during DP system setup.
5. Malfunctions with the DP system that result in an input not being implemented by the DP system must result in a noticeable alert to the OSV Crew.

Scenario 2a: The OSV Crew activates the DP system (auto) with an unsafe parameter set because crewmembers believe that another member has changed the parameter values (incorrect process model). Reasons for an incorrect process model could include:

a) A situation arises during DP system setup that requires the DP operator to change prior to activating the DP system (auto).
b) An OSV crewmember signs off on the setup checklist without verifying the checklist procedures.

Possible requirements for Scenario 2a:

1. If the DP Operator changes during checklist procedures, the set up procedures must be started again from the beginning.
2. If possible, OSV crewmembers must actively confirm checklist actions before signing off on the checklist item.

2.4.2.1. UCAs between the DP System and Signal Processing Unit

Figure 7 shows the focus on the functional control structure for this section of the analysis.

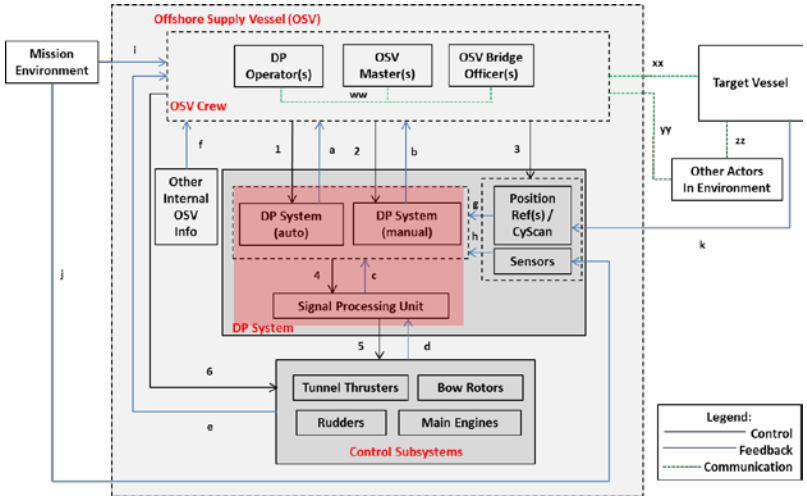


Figure 7: UCA Focus between DP System and Signal Processing Unit

Table 3 shows one row of unsafe control actions that were identified between the DP system and the Signal Processing Unit The full list of unsafe control actions identified in this section of the analysis is presented in Appendix B.

Table 3: Partial List of UCAs between DP System and Signal Processing Unit

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Provide directional command (DP Manual)	UCA24: DP system (manual) does not signal the SPU when the OSV Crew gives a directional command to the control subsystems. [H-1, H-2]	UCA25: DP system (manual) signals the SPU with a control command differently than the OSV Crew intends. [H-1, H-2]	UCA26: DP system (manual) signals the SPU x time after the OSV Crew gives a command to the control subsystems. [H-1, H-2]	UCA27: DP system (manual) stops signaling the SPU before the control command is implemented. [H-1, H-2]

Each identified unsafe control action has traceable safety requirements/constraints that can be incorporated to mitigate the identified unsafe control action. The safety requirements/constraints associated with the four unsafe control actions in Table 3 are as follows:

SC19: The DP system (manual) must immediately signal directional commands given by the OSV Crew to the SPU. [UCA24, UCA26]

SC20: The DP system (manual) must never signal the SPU to make a directional command if the command is not provided by the OSV Crew. [UCA25]

SC21: The DP system (manual) must continue signaling the SPU to control the OSV control subsystems until the command is successfully implemented. [UCA27]

A full list of the safety requirements/constraints associated with the full list of unsafe control actions identified between the DP system and Signal Processing Unit are presented in Appendix B.

2.4.2.2. Causal Scenario Analysis of Identified UCAs

With the unsafe control actions identified for this section of the analysis, the next step is to analyze each individually and create causal scenarios to determine how each unsafe control action can occur. As stated previously, these causal scenarios can be used to create more specific safety requirements that can be imposed on the system to promote safe operation. A full list of causal scenarios and the associated generated requirements is given in Appendix B. The causal scenario for the first identified unsafe control action listed in Table 3 is presented below.

Unsafe Control Action- UCA24: DP System (manual) does not signal the SPU when the OSV Crew gives a directional command to the control subsystems. [H-1, H-2]

Scenario 24: The DP system allows the OSV Crew to use a joystick and various control knobs to control different aspects of the OSV while the DP system controls other parts of the OSV when in various DP system (manual) modes. Therefore, depending on the DP system (manual) control mode selected by the OSV Crew, the OSV Crew could get mode confusion and be unaware that a control input is not applicable for the given mode that is selected, resulting in the DP system not signaling the SPU when the OSV Crew gives a directional command.

Possible requirements for Scenario 24:

1. The specific control mode currently selected to control the OSV must be readily displayed to the OSV Crew.
2. Feedback must be given to the OSV Crew stating which control mechanisms require manual input and what each control mechanism is controlling given the selected control mode.
3. If a control mechanism is inactive for a given control mode, noticeable feedback should be given to the OSV Crew if the OSV Crew provides an input to the inactive control mechanism.

Scenario 24a: The DP system stops working but does not alert the OSV Crew that it is not working. In certain situations, the only way to realize that the DP system has stopped functioning properly is to notice that the DP system display has no movement and the time clock is not updating. If the OSV Crew does not notice this malfunction immediately, they will not realize that the DP system is not signaling the SPU in response to a command given prior to the malfunction.

Possible requirements for Scenario 24a:

1. Sensors must be added to alert the OSV Crew if the DP system has stopped and the DP console screen is frozen.

2.4.3.1. UCAs between the OSV Crew and Position Refs/CyScan

Figure 8 shows the focus on the functional control structure for this section of the analysis.

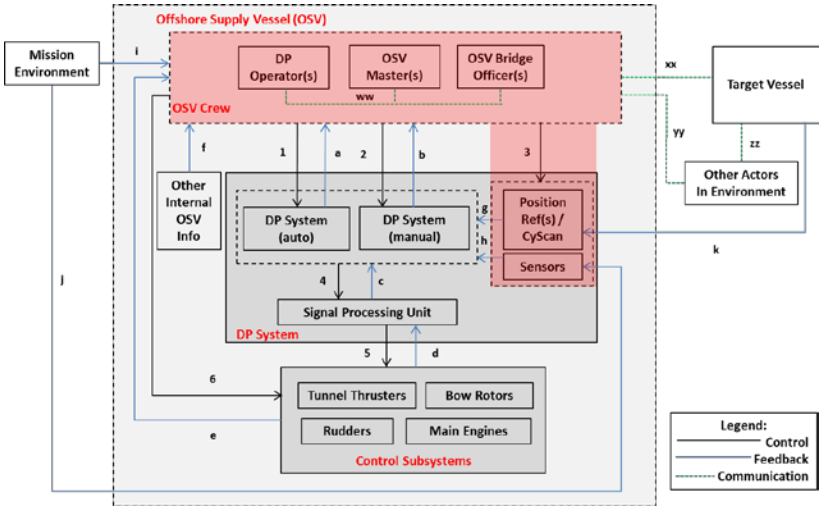


Figure 8: UCA Focus between DP System and Signal Processing Unit

Table 4 shows one row of unsafe control actions that were identified between the OSV Crew and the Position References/CyScan. The full list of unsafe control actions identified in this section of the analysis is presented in Appendix C.

Table 4: Partial List of UCAs between the OSV Crew and Position Refs/CyScan

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Turn CyScan OFF	UCA30: OSV Crew does not turn CyScan OFF and assume manual control when the CyScan malfunctions. [H-1, H-2]	UCA31: OSV Crew turns CyScan off during automatic operations while target follow mode is active. [H-1, H-2]	UCA32: OSV Crew turns CyScan off before switching to manual control of the OSV. [H-1, H-2]	N/A

Each identified unsafe control action has traceable safety requirements/constraints that can be incorporated to mitigate the identified unsafe control action. The safety requirements/constraints associated with the three unsafe control actions in Table 4 are as follows:

SC24: The OSV Crew must always turn CyScan sensors off and assume full manual control of the OSV when a CyScan malfunction occurs. [UCA30]

SC25: Automatic operations must never continue if CyScan sensors are turned off. [UCA31]

SC26: The OSV Crew must immediately assume full manual control of the OSV when CyScan sensors are turned off. [UCA32]

A full list of the safety requirements/constraints associated with the full list of unsafe control actions identified between the OSV Crew and the Position Refs/CyScan are presented in Appendix C.

2.4.3.2. Causal Scenario Analysis of Identified UCAs

With the unsafe control actions identified for this section of the analysis, the next step is to analyze each individually and create causal scenarios to determine how each unsafe control action can occur. As stated previously, these causal scenarios can be used to create more specific safety requirements that can be imposed on the system to promote safe operation. A full list of causal scenarios and the associated generated requirements is given in Appendix C. The causal scenario for the first identified unsafe control action listed in Table 4 is presented below.

Unsafe Control Action- UCA30: OSV Crew does not turn CyScan OFF and assume manual control when the CyScan malfunctions. [H-1, H-2]

Scenario 30: The CyScan sends invalid and faulty data to the DP system. The DP system does not recognize that the data is faulty and thus does not alert the OSV Crew that the CyScan has malfunctioned. This could result from one CyScan reflection being intentionally eliminated from the data input (due to weak signal, failure, etc.) and the remaining two CyScan reflections sending faulty data to the DP system. With only two reflections available, divergence will not be detected and the OSV Crew would not remove the CyScan from the DP system inputs.

Possible requirements for Scenario 30:

1. Automatic operations must not occur when CyScan redundancy is diminished.
2. The OSV Crew must have noticeable feedback any time that a sensor cannot use median testing to detect divergence.

Scenario 30a: The DP system detects a CyScan malfunction but does not provide an adequate alert the OSV Crew that a CyScan malfunction has occurred.

Possible requirements for Scenario 30a:

1. Further testing must be conducted to assess current DP system alarms. Testing should determine if any new alarms need to be added or if current alarms do not provide adequate information for the OSV Crew to adequately understand and respond to the alarm.
2. System critical alarms should be distinguished from non-critical alarms.

2.4.4.1. UCAs between the OSV Crew and DP System (manual)

Figure 9 shows the focus on the functional control structure for this section of the analysis.

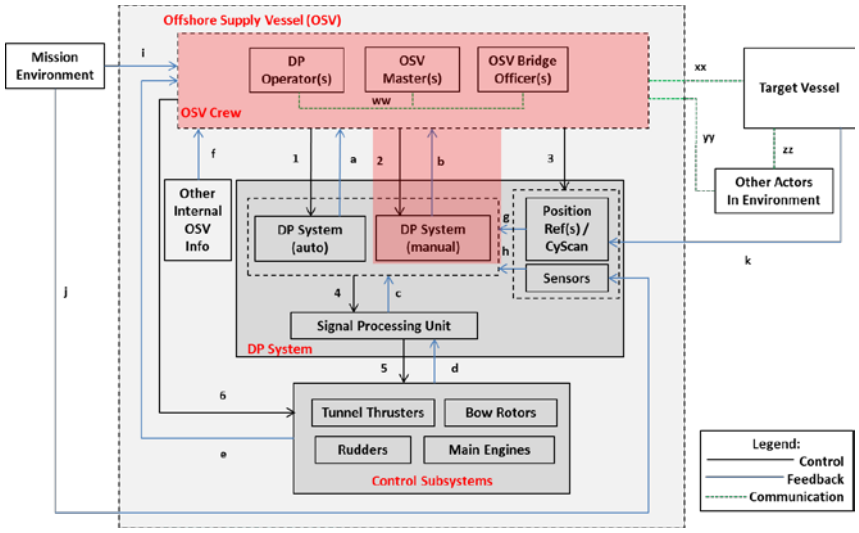


Figure 9: UCA Focus between OSV Crew and the DP System (manual)

Table 5 shows one row of unsafe control actions that were identified between the OSV Crew and the DP system (manual). The full list of unsafe control actions identified in this section of the analysis is presented in Appendix D.

Table 5: Partial List of UCAs between OSV Crew and the DP System (manual)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Activate DP system (manual)	UCA33: OSV Crew does not activate DP system (manual) and actively assert manual control of the OSV when manual control is required. [H-1, H-2]	UCA34: OSV Crew activates DP system (manual) when the OSV Crew believes that DP system (auto) has active control of the OSV. [H-1, H-2]	UCA35: OSV Crew activates DP system (manual) x amount of time before beginning to exert active control of the OSV. [H-1, H-2]	N/A

Each identified unsafe control action has traceable safety requirements/constraints that can be incorporated to mitigate the identified unsafe control action. The safety requirements/constraints associated with the three unsafe control actions in Table 5 are as follows:

SC27: The OSV Crew must activate DP system (manual) and actively assert manual control of the relevant OSV Control subsystems when DP system (manual) control is required. [UCA33]

SC28: The OSV Crew must never activate DP system (manual) without immediately providing the required control inputs associated with DP system (manual) control. [UCA34, UCA35]
A full list of the safety requirements/constraints associated with the full list of unsafe control actions identified between the OSV Crew and the DP system (manual) are presented in Appendix D.

2.4.4.2. Causal Scenario Analysis of Identified UCAs

With the unsafe control actions identified for this section of the analysis, the next step is to analyze each individually and create causal scenarios to determine how each unsafe control action can occur. As stated previously, these causal scenarios can be used to create more specific safety requirements that can be imposed on the system to promote safe operation. A full list of causal scenarios and the associated generated requirements is given in Appendix D. The causal scenario for the first identified unsafe control action listed in Table 5 is presented below.

Unsafe Control Action- UCA33: OSV Crew does not activate DP System (manual) and actively assert manual control of the OSV when manual control is required. [H-1, H-2]

Scenario 33: The DP system is controlling the OSV in automatic mode when a malfunction occurs or the DP system is still able to operate but loses redundancy and is thus less safe. The current situation is such that full manual mode may be unsafe; therefore, use of the DP system is still required, but in manual control mode through the DP system. The OSV Crew may not know to activate DP system (manual) because:

a) The loss of functionality in automatic mode in unannounced and the OSV Crew does not know that automatic mode has lost functionality.
b) The DP system announces that a malfunction has occurred, but the OSV Crew does not take the alert seriously and change control modes.
c) The DP system announces that a malfunction has occurred, but the OSV Crew takes an incorrect action to resolve the problem.

Possible requirements for Scenario 33:

1. False alarms must be minimized while still keeping an adequate threshold for detection of DP system issues.

2. Alarms that require changing control modes must include this information in the feedback that is given to the OSV Crew when the alarm is activated.

2.4.5.1. UCAs between the SPU and OSV Control Subsystems

Figure 10 shows the focus on the functional control structure for this section of the analysis.

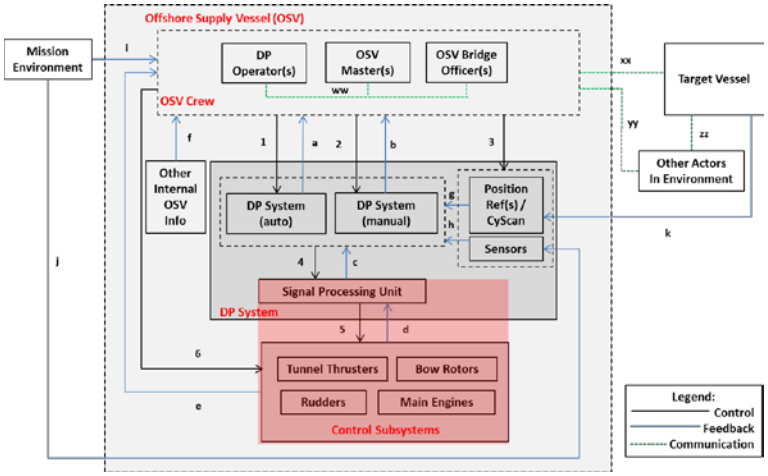


Figure 10: UCA Focus between the SPU and OSV Control Subsystems

Table 6 shows the unsafe control actions that were identified between the SPU and OSV Control Subsystems.

Table 6: Full List of UCAs between SPU and OSV Control Subsystems

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Implement directional command	UCA43: SPU does not implement a processed directional command to the OSV control subsystems when a directional command is needed to avoid an OSV collision. [H-1, H-2]	UCA44: SPU implements a directional command to the OSV control subsystems that is not commanded by the DP system or OSV Crew. [H-1, H-2]	UCA45: SPU takes too long to implement a processed directional command to the OSV control subsystems when the directional command is time sensitive. [H-1, H-2]	UCA46: SPU stops implementing a directional command to the OSV control subsystems before the maneuver is complete. [H-1, H-2]

Each identified unsafe control action has traceable safety requirements/constraints that can be incorporated to mitigate the identified unsafe control action. The safety requirements/constraints associated with the four unsafe control actions in Table 6 are as follows:

SC35: The SPU must always implement directional commands that have been provided by the OSV Crew within x amount of time. [UCA43, UCA45]

SC36: The SPU must never implement a directional command that had not been commanded. [UCA44]

SC37: The SPU must not stop implementing a directional command before the maneuver is completed. [UCA46]

2.4.5.2. Causal Scenario Analysis of Identified UCAs

With the unsafe control actions identified for this section of the analysis, the next step is to analyze each individually and create causal scenarios to determine how each unsafe control action can occur. As stated previously, these causal scenarios can be used to create more specific safety requirements that can be imposed on the system to promote safe operation. The causal scenario for the four identified unsafe control action listed in Table 6 are presented below.

Unsafe Control Action- UCA43: SPU does not implement a processed directional command to the OSV control subsystems when a directional command is needed to avoid an OSV collision. [H-1, H-2]

Scenario 43: The SPU does not implement a processed directional command to the applicable OSV control subsystem because:

a) An emergency situation (fire, etc.) results in a fault in the wiring between the SPU(s) and the applicable subsystems or a failure of the SPU(s).
b) The SPU malfunctions because it is old and has not received proper maintenance for optimal functioning.

Possible requirements for Scenario 43:

1. Redundant signal processing units should be separated such that an emergency situation does not cause all SPUs to fail at the same time.

2. Each SPU should be capable of signaling each control subsystem. For instance, SPU 1, SPU 2, and SPU 3 should all be able to signal the Stern Thruster, etc.

Scenario 43a: The electrical power supply to the SPU is interrupted as a command is being processed by the SPU and before the command is sent to the applicable control subsystem. When the power supply is restored, the command is not sent by the SPU to the applicable control subsystem.

Possible requirements for Scenario 43a:

1. Means must be in available to ensure that the correct signal is sent by the SPU to the applicable control subsystem. If a signal is not sent for any reason, feedback must be given to the SPU to resend the appropriate signal.
2. A disruption in the electrical power supply must not prevent the SPU from generating a signal for a directional command.
3. The SPU must be able to temporarily store commands and these commands must be available after a disruption in the power supply occurs so that the appropriate signal is generated.
4. The OSV Crew must receive feedback if the SPU receives and processes a command but does not send the appropriate signal to the appropriate control subsystem.

Unsafe Control Action- UCA44: SPU implements a directional command to the OSV control subsystems that is not commanded by the DP system or OSV Crew. [H-1, H-2]

Scenario 44: The SPU believes that a directional command has been provided by the DP system or OSV Crew because of a false signal that was generated by an anomalous event.

Possible requirements for Scenario 44:

1. Means must be in place to prevent the SPU from processing and implementing false signals that are not intentionally commanded by the DP system or OSV Crew.

Unsafe Control Action- UCA45: SPU takes too long to implement a processed directional command to the OSV control subsystems when the directional command is time sensitive. [H-1, H-2]

Scenario 45: System wear affects the processing capability and speed of the SPU without the SPU experiencing a failure that would result in a HDWR alarm, resulting in delays in the implementation directional commands to the OSV control subsystems.

Possible requirements for Scenario 45:

1. Each SPU must perform health checks and give applicable feedback to the OSV Crew if any system capability is degraded.
2. An alarm must be generated if signal processing and implementation takes longer than a predetermined amount of time.

Scenario 45a: Only commands issued at the Master Operator Workstation affect the operation of the OSV's control subsystems. Backup Workstations process all sensor and operator inputs, just like the Master, and continuously compute commands for the external devices. However, only the Master Workstation commands go through the Signal Processing Units (SPU) and are executed by the external devices. An event occurs where the Master Workstation transfers control of the OSV to the Backup Workstation, but the Backup Workstation experiences a delay in communication with the SPU and delays the execution of a directional command.

Possible requirements for Scenario 45a:

1. The DP system must give feedback to the OSV Crew if a seamless transfer from the Master to the Backup workstation is not possible.
2. There must not be any delay that occurs in sending control signals or SPU signal processing when the Backup Workstation becomes the active workstation controlling the DP system.

Unsafe Control Action- UCA46: SPU stops implementing a directional command to the OSV control subsystems before the maneuver is complete. [H-1, H-2]

Scenario 46: An event causes the SPU to fail mid maneuver. Because specific actuators are connected to specific SPUs, loss of a single SPU prevents the DP system from using all control subsystems controlled through that SPU. In this instance, the Thruster Allocation Logic (TAL) will attempt to make adjustments to use the remaining available thrusters to maneuver the OSV. If the TAL is unable to meet the required forces for the maneuver, an alarm is generated.

Possible requirements for Scenario 46:

1. Each SPU should be capable of controlling all control subsystems on the OSV so that if a single SPU fails, the backup SPU is truly redundant.
2. If an SPU fails and the TAL is unable to successfully reallocate commands to available control subsystems, the OSV must attempt to match the desired control input as closely as possible with the available resources.

Scenario 46a: The DP system believes that a maneuver is complete due to incorrect, conflicting, or missing sensor feedback and stops signaling the SPU. As a result, the SPU stops implementing a directional command when in reality the maneuver is not complete and directional command is stopped too early.

Possible requirements for Scenario 46a:

1. The SPU must be able to resolve conflicts between sensor data (DGPS, CyScan, etc.) and subsystem feedback (thruster feedback). If thruster feedback conflicts with position data, the SPU must still be able to complete the given maneuver being performed.
2. Thruster feedback sent to the SPU must not differ from actual thruster performance. Additional sensors should be added if necessary to ensure that thrusters perform as commanded by the SPU.

2.5. Summary of Case Study

This chapter discussed the STPA process as it was applied to analyzing an OSV DP system. The process began by defining the accidents and hazards that were used to guide the remainder of the analysis. Next, the system's control structure was modeled at varying hierarchical levels and the safety-related responsibilities and functional relationships of the components within the control

structure were established. The functional control structure at the technical system level was used to identify unsafe control actions, create causal scenarios, and generate safety constraints and potential safety requirements for the system.

Only a sample of the unsafe control actions, causal scenarios, and safety requirements were included in this chapter. However, the full list of these can be found in Appendices A through D. In total, STPA identified 46 unsafe control actions, 37 system-level safety constraints, and 171 recommended safety requirements for the system. To assess the scope of the recommended safety requirements that were generated, the 171 safety requirements were analyzed in detail to identify commonalities and to group similar requirements. Through this process, it was found that the safety requirements fell into four general categories that considered a wide range of factors. These categories include: feedback recommendations, design recommendations, procedures recommendations, and testing/training recommendations. Table 7 lists the factors that each category of recommendations covers.

Table 7: Categorized STPA Recommendations

Feedback Recommendations	Associated Causal Scenarios
DP System or other Malfunction	17, 21, 22, 23, 23a, 24a, 26, 27, 27a, 30, 36, 40, 41a, 43a, 45
Control Modes	1, 5, 5a, 10, 24, 25a, 34, 41
CyScan	7, 21a, 28, 29, 31
Alarms	11, 11a, 30a, 33
Master/Backup Station	9a, 12a, 39a, 45a
Parameter Setup	2, 14
Redundant Feedback Mechanisms	6, 11a
OSV Positioning	6, 13
Special Breakaways	17, 19
Joystick Response	25, 40
Environmental Conditions	3
OSV Separation Thresholds	13
Design Recommendations	**Associated Causal Scenarios**
Reliability/Redundancy	8a, 9a, 10a, 16a, 17, 23a, 27a, 39a, 41a
Miscellaneous	7a, 10a, 16, 18a, 21, 21a, 26
Signal Processing Units	18a, 43, 43a, 44, 45, 46, 46a
Control Modes	1, 5, 6a, 8a, 17, 20, 34
System Parameters	2, 4a, 12, 14, 15, 15a
Crew Operations	2, 6a, 9, 19, 22, 39
Activation of Target-Follow Mode	4, 17a, 20, 37a, 38

Master and Backup Consoles	1, 12a, 16a, 45a
CyScan Operations	29, 29a, 31, 32
Thruster Allocation Logic Operations	17a, 22, 46, 46a
Electrical Power	27, 43, 43a
Diagnostic Capability	27a, 37a, 38
Environment Detection Sensors	3, 39, 40
Safe Operating Envelope Violation	42
Unsafe User Inputs	37
Procedures Recommendations	**Associated Causal Scenarios**
Use of DP System	7a, 16, 18a, 23, 30, 36
DP System Setup Checklists	2, 2a, 4, 4a, 12
CyScan Operation	28, 29a, 32
Crew Roles	1, 35
Operations in Unsafe Sea State	3, 3a
Relinquishing Manual Control of OSV	5, 5a
Manual Control Settings	9, 35
Safety Considerations	18, 40a
Emergency Breakaway Response Times	18a
Training/Testing Recommendations	**Associated Causal Scenarios**
Breakaway Response Time Training	11, 42
OSV Breakaway Options	9
Master/Backup DP Console Training	12a
Optimum Manual Control Testing	9
Critical Fault Detection	11a
Component Reliability Determination	16a
Min. Lateral Separation Determination	18a
Adequacy of Alarms	30a
Breakaway Procedures	40a
Emergency Breakaway Response Times	42

Grouping similar safety requirements aids the follow-on process of responding to the analysis results. In a system that is already designed and fielded such as the OSV system analyzed in this case study, time, cost, and feasibility considerations will play a major role in the decision to implement the recommendations and thus such grouping can help the decision maker through the process.

Page intentionally left blank.

3. Results Comparison and Standard Compliance

Professor Nancy Leveson has made the following observation regarding safety and reliability engineering:

> The world of engineering has experienced a technological revolution in the last 40 years, while the basic engineering techniques applied in safety and reliability engineering, such as fault tree analysis (FTA) and failure modes and effects analysis (FMEA), have changed very little from their creation 50 years ago. [2]

Because traditional methods such as FTA and FMEA are unable to fully analyze systems that have become increasingly complex, STPA was created to handle today's complex, software intensive system.

3.1. Comparing the Problem Space

As the results of the STPA analysis on the OSV DP system highlight, STPA provides a framework to identify unsafe control actions and causal scenarios that can lead to hazardous system states that fall outside of the failure-centric problem space captured by FTA and FMEA. Figure 11 illustrates this fundamental difference between FTA and FMEA's focus compared to STPA's focus.

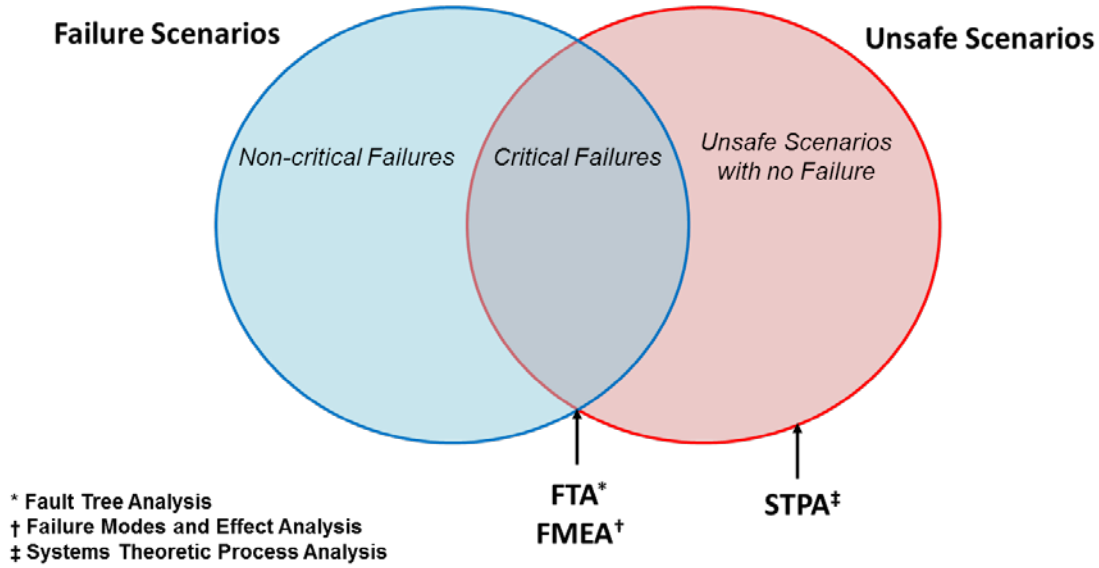


Figure 11: STPA Includes a Different Problem Space [12][1]

[1] Figure 11 is adapted from Ref. 12, Pg. 61 to show where FTA, FMEA, and STPA fit into the depicted problem spaces.

Since FTA and FMEA focus solely on failure scenarios, these methods cannot identify all scenarios (including non-failure scenarios) that can lead to an accident. For instance, while a widget failure may be a problem for a number of reasons, the widget failing will not necessarily lead to an accident. In other words, failure scenarios correlate to reliability problems and not necessarily safety problems (although as the diagram depicts, failure scenarios may also be unsafe). In short, reliability does not guarantee safety. Because FTA and FMEA focus solely on failure scenarios, there is a whole category of unsafe scenarios that will not be captured when using these methods to conduct a safety analysis.

This unsafe scenario problem space is where STPA is able to find safety concerns that FTA and FMEA does not. While failure scenarios are also identified, using STPA allows for the identification of hazardous system states that arise from unintended component interactions, inadequate design requirements, design flaws, human errors, and unsafe scenarios where no failures occur. Because of the different focus of STPA relative to FTA and FMEA, a one-to-one comparison of the methodologies is difficult. However, by discussing examples of STPA results that are not found when using FTA and FMEA, limitations of the traditional methods and advantages of STPA can be highlighted.

3.2. Fault Tree Analysis Comparison

A fault tree analysis of the OSV DP system has been conducted by an independent research team. Two separate fault trees were created for the OSV DP system. One assesses the probability of a collision or allision during DPS automated operations and is partially shown in Figure 12. The other assesses the probability of a collision or allision during DPS manual operations and is partially shown in Figure 13. Both figures have been adapted from the original fault trees in [13] for clarity and do not depict the lowest level failure events.

The fault tree for OSV Collision or Allision during Auto-Ops consists of three fault events: a hardware or software failure that misdirects the OSV's heading, the OSV turning towards a given object, and the DPO failing to avert the OSV collision. The hardware or software failure that misdirects the OSV can be caused by a hardware failure (CyScan Sensor Failure, DGPS Failure, Gyrocompass Failure, VRU Failure, Serial Data Distribution Box Failure, or Thruster/Rudder SPU Failure), a DPS Software failure, or an Electrical System Failure (Circuit

Breaker Failure, Wiring Failure, or Converter Failure). Whether or not the OSV turns towards an object given the hardware or software failure is assigned a 0.5 probability based on a 180 degree radial window. Whether or not the DPO fails to avert a collision given the previous two conditions is determined by whether the DPO operator and DPO watchmen both do not notice that the OSV is on a collision course and whether or not the DPO commits an error of omission.

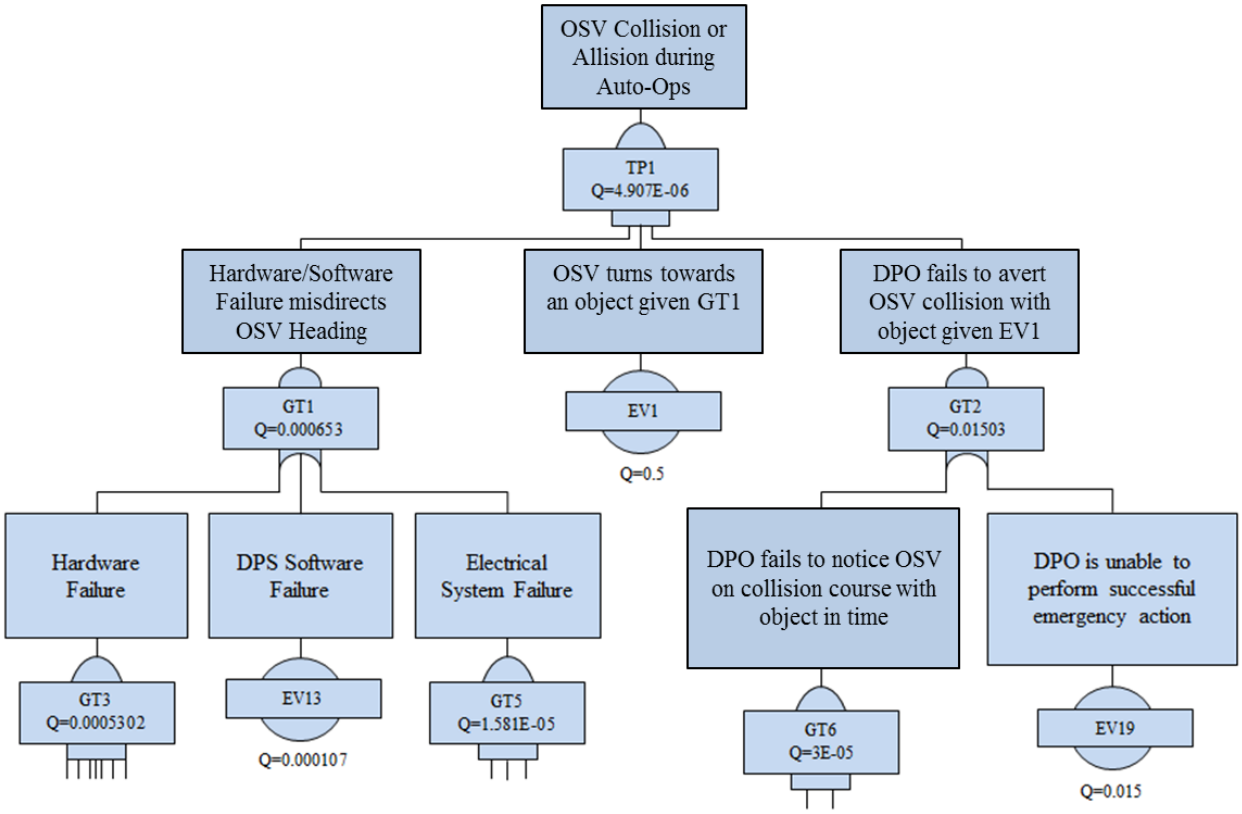


Figure 12: Fault Tree for OSV Collision or Allision during Auto-Ops [13]

The fault tree for OSV Collision or Allision during Manual-Ops is identical to the fault tree in Figure 12 with three exceptions. First, wind sensor failure is considered under the hardware failure event due to this sensor's input during manual operations. Second, the hardware and software event category is expanded to include personnel incorrectly maneuvering the OSV. Third, the probabilities of the DPO failing to prevent a collision or allision are slightly different due to the operator tasks and environment being different in auto versus manual operations.

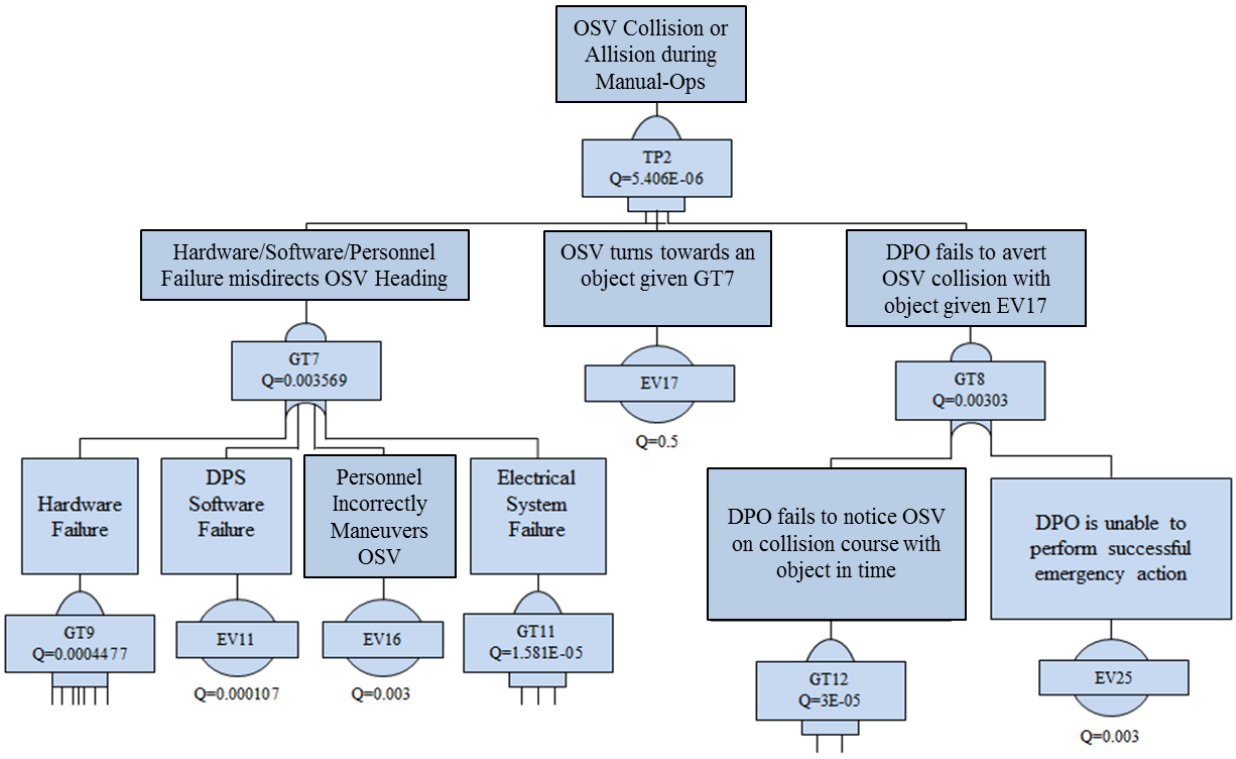


Figure 13: Fault Tree for OSV Collision or Allision during Manual-Ops [13]

The authors of the fault tree analysis state that "the focus of this analysis is to predict the probability of a collision due to failure of the Dynamic Positioning System (DPS)" [13]. While the fault tree may be useful in showing the probability of failure of hardware system components and the probability that a collision will occur due to a hardware component failure, there is little use for the fault tree when no failure occurs.

3.2.1. Non-Failure Example

One unsafe control action where no failure occurs that STPA identified is illustrated in the following causal scenario linked to UCA13:

Scenario 13: During operations, many user configurable parameters will not change; however, some user configurable parameters will require change as dynamic situations progress. As such, changes in user configurable parameters are mainly limited to DP system threshold (alarm) values. As the lateral separation distance between the OSV and the target vessel changes, the OSV Crew must change the DP system thresholds values as the relative positions of the two vessels changes. If the lateral separation between the OSV and the target vessel is changing often

and the OSV Crew is experiencing a high-workload, high stress environment, the OSV Crew may forget to change the DP system threshold values.

As illustrated by this example, the OSV Crew has the option to change DP system threshold values to adjust when feedback is provided during escort operations. While there is a procedural requirement that directs the OSV Crew to adjust DP system threshold values based on lateral separation distance, there is no system requirement that ensures the DP system thresholds are changed as the OSV decreases lateral separation with the target vessel (the DP system will not lose functionality if these parameters remain unchanged). While one could argue that not changing the DP system threshold values constitutes a failure of the OSV Crew, doing so would highly discredit the authority given to the OSV Crew to make decisions based on dynamic operations. With this unsafe scenario, by not updating DP system threshold values, negative consequences will only result if the DPO has to eventually prevent a collision.

According to the fault tree analysis and probability risk assessment, the probability that the DPO is unable to perform successful emergency action takes into account the baseline Human Error Probability and modifies this value to account for the operator's experience level and stress level [13]. This value makes little sense from a human factors standpoint, as the baseline Human Error Probability has very little meaning outside of laboratory testing. Regardless, with these factors accounted for, the analysis states that the probability that the DPO is unable to perform successful emergency action is 1.5E-2 [13]. However, given the potential for extremely small lateral separations between OSVs and target vessels during escort operations, if the DP system threshold values are not set to immediately alert the OSV Crew of a course deviation, the probability of the DPO successfully preventing a collision from happening could drastically decrease. This would correspond to a much higher probability than the "baseline Human Error Probability."

Given the fault tree method, the probability of the DPO failing to prevent a collision is identified, assessed in relation to the number of other failures that can occur, and the ultimate probability of a collision is either accepted, or measures are presented to increase the reliability of the system components. With STPA, in contrast, safety constraints that can be imposed on the system are

identified to prevent the unsafe system state from arising. For instance, given this unsafe control action, the DP system could automatically update threshold and alarm values given the lateral separation distance from the target vessel. By imposing this new requirement on the system, the risk of the OSV Crew not updating these parameter values and consequently not receiving vitally important feedback that is necessary to prevent a collision is no longer relevant (however this change to the system will now need to be analyzed to see if new safety concerns were introduced to the system).

3.2.2. Process Model Flaw Example

Another area where STPA identifies safety concerns that do not involve a failure is when a controller has a process model flaw. Each controller in a system has a model of the process that is being controlled. This process model is embedded in the mental model of human controllers and contains "the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state" [2]. When the controller's process model differs from the actual process that is occurring, the controller can be said to have a process model flaw. The following causal scenario associated with UCA3 illustrates how a flawed process model can lead to an unsafe control action:

Scenario 3: The ability of the DP system to properly maintain its position relative to the target vessel is highly dependent on the mission environment at the time of operation. Therefore, guidelines are in place to regulate when the DP system may be used during OSV operations. External variables that are considered include the current sea state, swell heights, visibility conditions, and wind speeds. The OSV Crew could activate DP system (auto) during an unsafe sea state due to a flawed process model regarding the sea state. Reasons that the OSV Crew may have a flawed process model could include:

a) The OSV Crew does not have accurate feedback regarding the current sea state classification.
b) The OSV Crew does not have accurate feedback regarding current swell heights.
c) The OSV Crew does not have accurate feedback regarding the current wind speeds.
d) The OSV Crew inaccurately classifies visibility conditions.
e) The OSV Crew misinterprets correct sensor data regarding these variables.
f) The environment changes abruptly during the transition to DP system (auto) operations.

In this example, the unsafe control action that needs to be prevented is the OSV Crew activating the dynamic positioning system in automatic target follow mode while the vessel is operating in an unsafe sea state. There are various reasons why this control action is considered unsafe. Most importantly, the dynamic positioning system is unable to operate properly when sea conditions are extremely unfavorable. For instance, in weather conditions that hinder visibility, the CyScan's ability to track the target vessel's reflectors could be diminished. When wind gusts are above a predetermined speed, the DP system is unable to adequately compensate for wind forces. When swell heights are too high, the OSV loses the ability to adequately remain on track in target follow mode. All of these environmental factors combined lead to a categorized sea state and the DP system should not be used because the DP system will likely function in a degraded and unsafe state.

The OSV Crew has little objective, quantitative feedback to aid in their decision to use the DP system for automatic operations given adverse weather conditions. Because of the lack of information available to the OSV Crew regarding weather conditions and how the weather conditions could possibly be degrading the functionality of the DP system during execution of target follow procedures, it is very realistic that the OSV Crew could have a flawed process model. This flawed process model regards the ability of the DP system to successfully perform automatic operations in adverse weather conditions until after a system error occurs and a collision is imminent and possibly unavoidable. Given this unsafe control action identified by the STPA process, there are possible requirements that can be implemented as safety constraints on the system to prevent this unsafe control action. Possible requirements that could be generated are shown below; however, it must be noted that this may not be a comprehensive list of requirements.

Possible requirements for Scenario 3:

1. The OSV Crew must be notified if the sea state is such that the conditions are unsafe for automatic OSV operations. If possible, sensor information should be integrated to output a sea state classification.

2. Sensors should give information to the OSV Crew regarding swell heights and wind speed. If swell heights or wind speeds are above the predetermined limit for automatic operations, the feedback should reflect this fact.
3. If possible, transitioning to automatic operations when wind speed, swell height, and sea state sensor data exceeds safe operating limits should not be possible.

These three requirements, if implemented, would effectively prevent the OSV Crew from using the DP system to operate in target follow mode during an unsafe sea state that could negatively affect the DP system's ability to navigate with respect to the target vessel in target follow mode. First, the OSV Crew must have relevant information regarding wind speeds and swell heights. This information alone will aid in determining whether or not it is safe to use the DP system in automatic mode. However, if it is possible to integrate the sensor information into a sea state classification that can be given to the OSV Crew as feedback, this function would mitigate the potential for judgment error from the OSV Crew and would provide a rigid metric around which guidance for DP system use could be built.

With these two system requirements implemented in the OSV and DP system, the OSV Crew would have information available to ensure that a flawed process model of DP system functionality during automatic operations does not arise due to adverse weather conditions. Yet, humans are prone to make errors, and even the most skilled operators are not immune to making mistakes. In addition, failures can occur that result in the necessary information not being relayed to the OSV Crew. Therefore, a third system requirement could be implemented to further constrain the system and add safety. By preventing the system from transitioning to automatic operations when wind speed, swell height, visibility conditions, and sea state exceed predetermined limits, the chance that the DP system is utilized for automatic operations during an unsafe sea state is effectively negated.

3.3. Failure Modes and Effect Analysis Comparison

By conducting an STPA hazard analysis on the OSV DP system, all of the failures captured by FTA and FMEA were identified as well as many other non-failure related safety concerns. Not only did STPA identify failure related safety concerns as well as FTA and FMEA, but it was also able to identify weaknesses in the FMEA that were not previously apparent.

After failure modes were identified, DP Proving Trials were conducted to analyze the effects that the identified failure modes had on the system. One of the many failure modes that were analyzed was a SPU Outstation Network Failure. To test the effect of this specific failure mode, each of the three SPUs was failed individually and independently. When SPU 1, SPU 2, and SPU 3 were failed, the result was that there was a loss of communication with the failed SPU and there was no loss of position or heading that occurred as a result of the SPU failure [14]. From the results of this FMEA, it is tempting to conclude that an individual SPU failure will have no negative effect on the ability of the DP system to perform its function; however, this conclusion is misleading.

3.3.1. Considering the Operational Environment

When the DP Proving Trials were initially designed to analyze each identified failure mode, the purpose was to certify the DP system as a Class-2 DP system (DPS-2). Because most DPS-2 systems are used in vastly different applications compared to escort operations, the typical use of DPS-2 systems influenced the test design. When each individual SPU was failed, the OSV was essentially stationary and maintaining station relative to a target location [14]. Because the OSV was stationary, when one SPU was failed, the remaining two SPUs were able to compensate for the failed SPU and maintain position and heading in the test environment. However, consider the following causal scenario identified through the STPA analysis of the DP system:

Scenario 46: An event causes the SPU to fail mid maneuver. Because specific actuators are connected to specific SPUs, loss of a single SPU prevents the DP system from using all control subsystems controlled through that SPU. In this instance, the Thruster Allocation Logic (TAL) will attempt to make adjustments to use the remaining available thrusters to maneuver the OSV. If the TAL is unable to meet the required forces for the maneuver, an alarm is generated.

This scenario identified by STPA differs from the FMEA test case with regard to the operational environment in which the SPU failure occurs. According to the DP Proving Trials, a single SPU failure will have no adverse effect on the ability of the DP system to maintain the OSV's position relative to the target vessel [14]. However, if a SPU were to fail mid-maneuver while the DP system is being used in target follow mode under conditions that would be present during escort operations, the effect would be drastically different. Because each individual SPU is connected

to specific control subsystems, the loss of a single SPU would result in multiple control subsystems being no longer available for use. For instance, the loss of SPU 1 would result in the DP system being unable to communicate or utilize the thruster, the main engine, and the rudder that is connected to that SPU. Therefore, the loss of a single SPU during operations where target follow mode is being utilized could result in the OSV being unable to maintain a proper positon relative to the target vessel and could ultimately contribute to the possibility of a collision occurring between the OSV and the target vessel.

In order to mitigate this safety concern, a possible new requirement that could be imposed on the system is to give each individual SPU the capability to communicate with all OSV control subsystems so that if an SPU fails, no control subsystem is lost as a result and the OSV is able to maintain proper position relative to the target vessel while still using the DP system in target follow mode. Whereas the idea of system redundancy as safety mitigation is reinforced through the DP Proving Trials and FMEA, this particular example shows how STPA is able to identify safety concerns that were previously unidentified and suggest requirements to make the system safer.

Only a few comparative examples have been discussed to highlight the advantages of STPA relative to FTA and FMEA. Regardless of these advantages, STPA, as with any hazard analysis techniques, must be compliant with MIL-STD-882E in order for it to be utilized on Department of Defense contracts that require this standard. The next section discusses STPA's compliance with MIL-STD-882.

3.4. MIL-STD-882 Compliance

The Department of the Navy, as with all military departments and defense agencies within the Department of Defense, uses MIL-STD-882E to "provide a standard, generic method for the identification, classification, and mitigation of hazards" [15]. Within this standard, eight elements of the system safety process, depicted in Figure 14, are identified and required (as a minimum) for an acceptable system safety effort for any Department of Defense system when no specific tasks are called out in the contract.

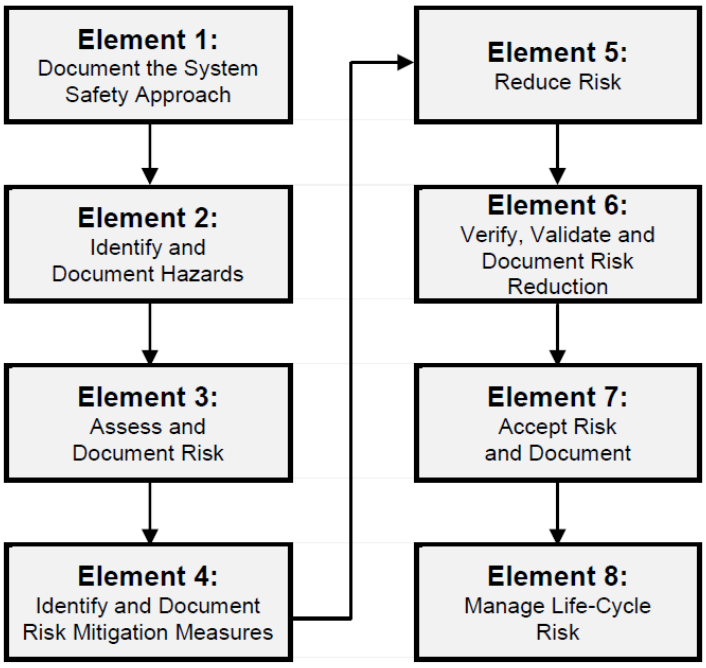


Figure 14: Eight Elements of the System Safety Process [15]

Within this framework, STPA can be used very successfully to directly or indirectly meet the requirements of all eight elements listed as part of the system safety process. One of the requirements for Element 1 in the System Safety Process is that the system safety approach must "describe the risk management effort and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure" [15]. As discussed in Chapter 2, one of the first steps in the STPA process is to assess the overall management structure and analyze how safety decisions are made and map throughout the organization. By considering the organizational influence on system operations, STPA is effectively able to meet this requirement.

To meet the requirements of Element 2 in the Systems Safety Process, MIL-STD-882E states that the following requirements must be satisfied:

> Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment…The hazard identification process shall consider the entire system life-cycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment. [15]

Simply stated, STPA meets these requirements. STPA provides a systematic analysis of the system and looks not only at hardware and system interfaces, but software as well (without assigning arbitrary and meaningless probabilities of failure to the software). Furthermore, by including the user throughout the STPA process and allowing the user to identify the relevant losses and hazards to be explored with the analysis, STPA considers the intended use, application, and operational environment of the system that is being analyzed, thus also meeting the intent of the requirements in element three. It is important to note; however, that the STPA process by design does not assign probabilities to the occurrence of unsafe control actions or causal scenarios that are identified. While the user may take the results from the STPA analysis and independently assign probabilities of occurrence and create a risk matrix from analysis results, doing so is intentionally not a formal part of the STPA process due to inadequacies with reliability-based approaches that have been previously discussed.

The fourth element in the Systems Safety Process states that the process must identify and document risk mitigation measures [15]. Using STPA, system requirements and constraints are generated for the overall management structure, after the identification of unsafe control actions, and after causal scenarios are generated that can lead to the occurrence of the identified unsafe control actions. MIL-STD-882E states that mitigation approaches can include “elimination of the hazard through design selection, reduction of risk through design alteration, incorporation of engineering features or devices, the provision of warning devices, and/or the incorporation of signage, procedures, training, and PPE” [15]. Looking at the list of requirements and constraints generated in response to the identified unsafe control actions and causal scenarios that were previously discussed, one can see that STPA provides requirements in each of these categories to help mitigate identified unsafe control actions that lead to hazards.

Elements five through eight of the System Safety Process fall outside of the formal STPA approach; however, because STPA is a hazard analysis technique that can be utilized at any point in a system’s developmental lifecycle, it can be used to indirectly support these elements. The results of the STPA analysis can be used to help design teams and program managers reduce system risk, document risk reduction measures that are taken in response to the analysis, and in doing so, manage the life-cycle risk of the system. While STPA is effective at meeting the

requirements of the generic system safety process, it can also be used to meet the requirements of specific tasks that may be called out in a contract. Consider Task 205: System Hazard Analysis. As stated in MIL-STD-882E, the purpose of Task 205 is to:

> Perform and document a System Hazard Analysis (SHA) to verify system compliance with requirements to eliminate hazards or reduce the associated risks; to identify previously unidentified hazards associated with the subsystem interfaces and faults; identify hazards associated with the integrated system design, including software and subsystem interfaces; and to recommend actions necessary to eliminate identified hazards or mitigate their associated risks…Areas to consider include performance, performance degradation, functional failures, timing errors, design errors or defects, and inadvertent functioning. While conducting this analysis, the human shall be considered a component within the system, receiving both inputs and initiating outputs. [15]

When reading the purpose and task description for Task 205, it is extremely clear that the STPA process can be used to complete the system hazard analysis as defined in MIL-STD-882E. STPA uses a method based in systems theory to identify losses relevant to the user, hazards that could lead to those losses, and unsafe control actions that could result in a hazard occurring. By assessing control actions in terms of not being provided, being provided, being applied in an incorrect order, or stopped too soon/applied too long, STPA addresses all of the areas that MIL-STD-882E identifies in the task description for the system hazard analysis. Furthermore, STPA is the only hazard analysis technique that is able to address all of the areas of concern called out in this task description, as traditional techniques are unable to meaningfully address all of the requirements due to the focus on failures.

Page intentionally left blank.

4. CAST Case Study

This chapter discusses how CAST was used to analyze an accident involving two OSVs during OSV testing. The case study illustrates how using the CAST framework for an accident analysis "provides the ability to examine the entire sociotechnical system design to identify weaknesses in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including systemic ones" [2] that contributed to the accident. Furthermore, this case study illustrates the similarities between STPA hazard analysis and CAST accident analysis and shows how once STPA is used to analyze an existing system design, the results can be used to inform subsequent CAST analyses. This link reduces the amount of work required to perform the accident analysis when both STPA and CAST are used to analyze the system.

4.1. Accident Scenario

The following accident scenario is derived from an incident that occurred during OSV/OSV testing. The full accident description is not available for public release; consequently, some of the accident details have been changed, omitted, or fictionalized for the purposes of this case study.

While conducting OSV testing for recertification of a specific vessel for target follow automatic operations, a minor collision occurred between two contractor-owned and operated OSVs. The two OSVs were operating at (x) ft. lateral separation with Vessel 1 operating in target follow mode and Vessel 2 operating in transit mode, simulating the target vessel. During the conduct of a test involving a starboard 45-degree turn, with a full target vessel rudder simulated, Vessel 1 (the outside vessel in the turn) began to lag behind Vessel 2, closing lateral separation to (y) ft., at which time Vessel 1's OSV master initiated a breakaway. During the breakaway Vessel 2's port quarter contacted Vessel 1's hull above the waterline. Figure 15 presents a visual depiction of this event.

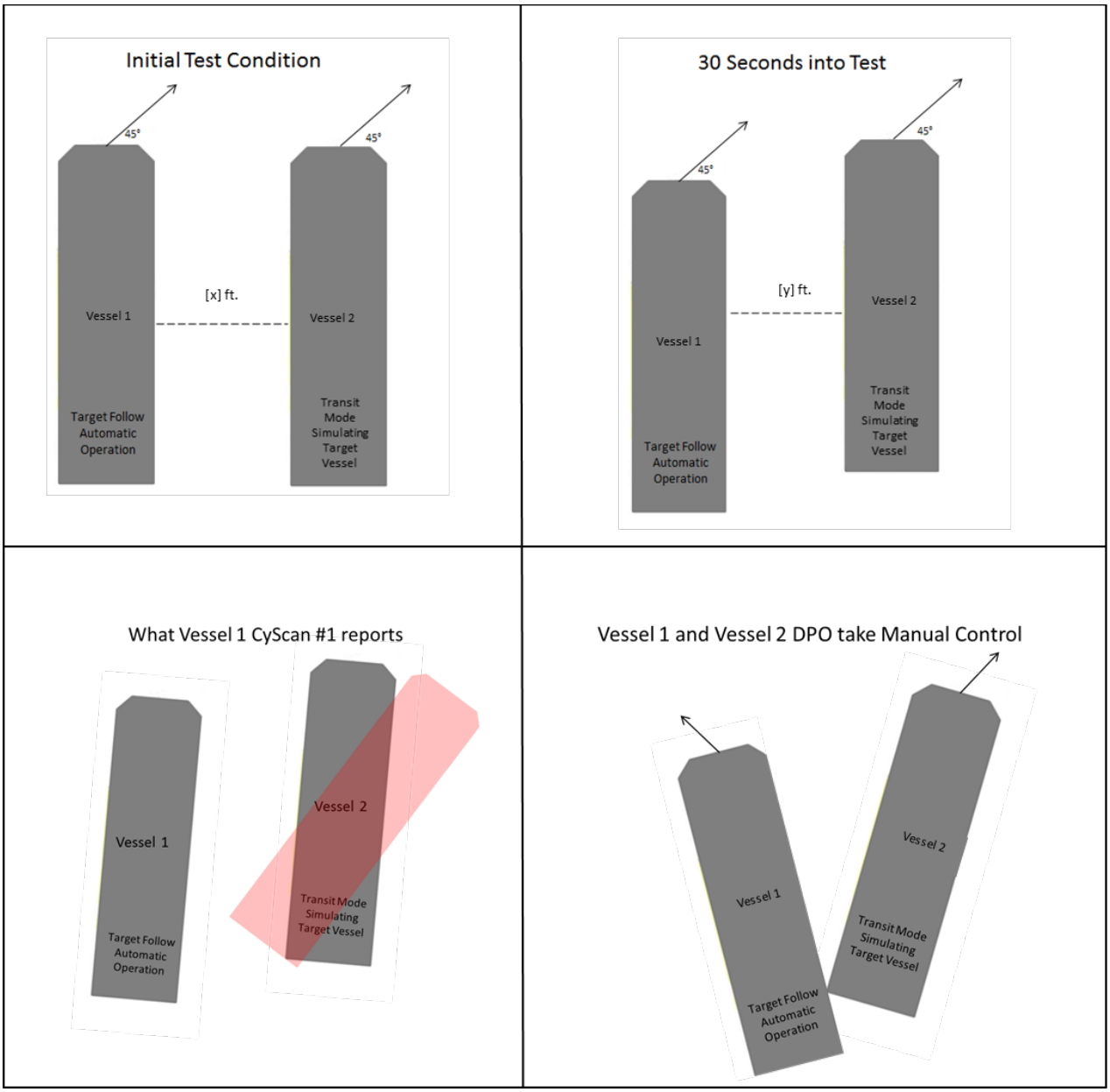


Figure 15: Visual Representation of Accident

4.2. Chain of Events

The following chain of events leading to the vessel collision was as follows:

21:46:59 – Vessel 2 begins starboard turn at (x) ft. lateral separation (45 degree turn, 40 degree/min, 12 knots)

21:47:27 – Vessel 1 falls back and DP system issues an alongship yellow alarm

21:47:30 – CyScan #1 on Vessel 1 reports that Vessel 2 has instantaneously rotated 37 degrees to starboard, the Noise Rejection Logic (NRL) filter removes CyScan #1's data from DP calculation due to it exceeding maximum allowable position delta

21:47:33 – Vessel 1's DP system issues a CyScan 1 NRL Data Rejection Alarm

21:47:36 – Vessel 1's NRL filter releases CyScan #1's data back into the DP system's calculation after the positional data falls within the filter's maximum allowable delta, the DP system commands the rudders/rotors/thrusters to turn the vessel starboard, CyScan #1 inconsistently flags its data as valid/invalid for next 30 seconds

21:47:38 – Vessel 1's DP system issues an alongship separation red alarm that indicates the DP system thinks Vessel 1's bow or stern is within (z) feet of Vessel 2, but this is attributable to the erroneous CyScan data

21:47:42 – Vessel 1 has maximum starboard rudder angles

21:47:49 – The DPO on Vessel 1 takes manual control of Vessel 1

21:47:50 – The DPO on Vessel 2 takes manual control of Vessel 2

21:47:55 – Vessel 1's rudder begins turning to port

21:47:58 – Vessel 1 rudder maximum to port

21:47:59 – Vessel 2's rudder begins turning to port

21:48:06 – Vessel 2 rudder maximum to port

21:48:14 – Vessel 2's rudder begins turning to starboard

21:48:17 – CyScan #2 data on Vessel 1 is marked as invalid by CyScan

21:48:24 – Vessel 2 rudder maximum to starboard (33 and 34 degrees)

21:48:32 – Vessel 2 rudder to zero

21:48:35 – Contact between vessels

4.3. Functional Control Structure

The functional control structure shown in Figure 16 depicts the functional relationship between components within the OSV systems that control the maneuvering of the OSVs during operations. As the CAST accident analysis develops, each component within this control structure and the interactions between each component is discussed in more detail. It is important to highlight the similarities between this control structure and the functional control structure used in the STPA analysis in Chapter 2, as the functional relationship between components within the OSV system are identical.

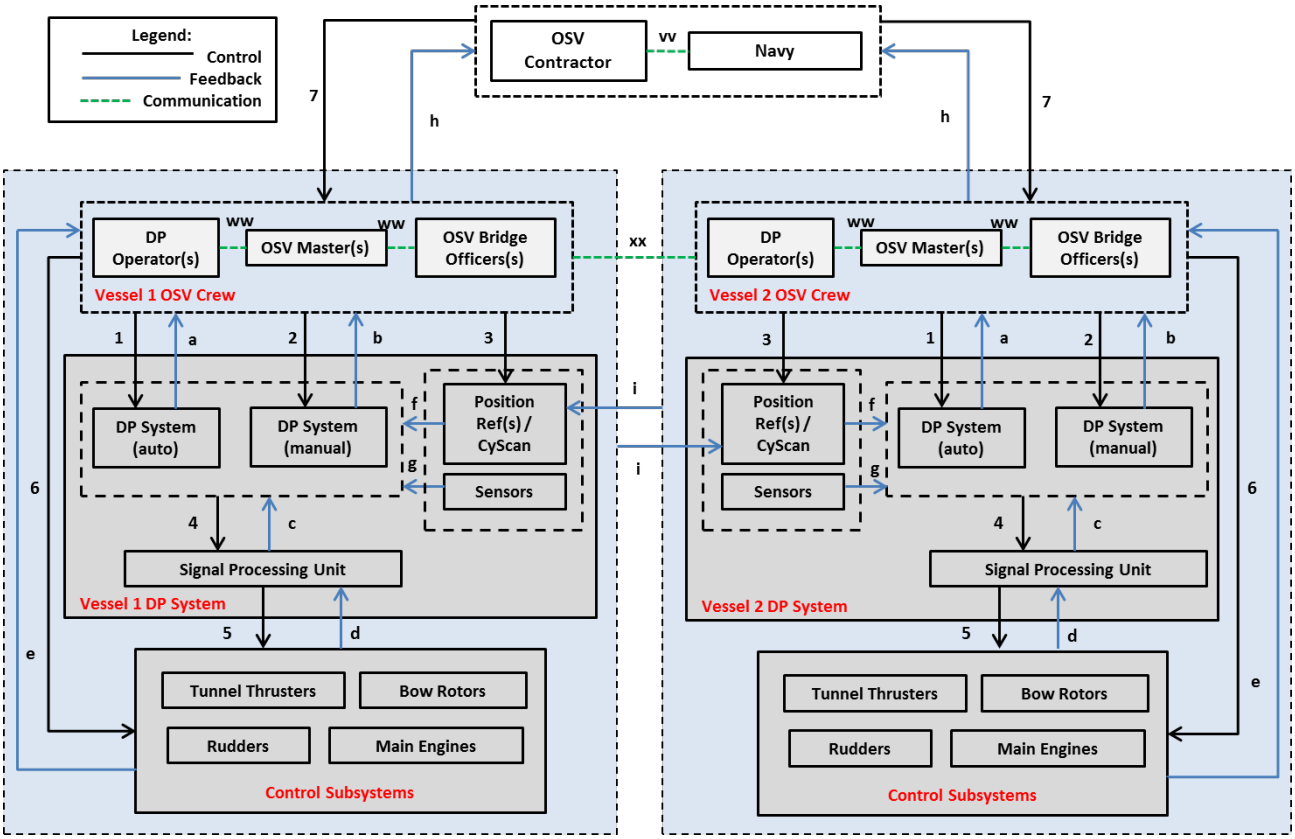


Figure 16: Safety control structure for OSV/OSV operations

The safety control structure in Figure 16 depicts three types of interactions between components: control actions, feedback, and communication. *Control actions* are defined as a component exerting functional control over another component, which is the controlled action. *Feedback* is defined as any type of information that one component sends to another component in response to a control action. *Communication* is defined as a two-way interaction between components that can result in either *control actions* or *feedback* being given. The following control actions, feedback, and communication are present within the OSV operations safety control structure.

4.3.1. Control Actions

1.) OSV Crew → DP system (auto)

- Activate/deactivate DP system (auto)
- Set user configurable parameters

2.) OSV Crew → DP system (manual)

- Activate/deactivate DP system (manual)
- Set user configurable parameters

- Provide directional commands

3.) OSV Crew → Position Ref(s)/CyScan/Sensors
   - Turn CyScan ON/OFF
   - Set sensor parameters

4.) DP system → Signal Processing Unit
   - Signal directional command

5.) Signal Processing Unit→ Control Subsystems
   - Implement directional command

6.) OSV Crew → Control Subsystems
   - Activate/deactivate full manual mode
   - Provide directional command

7.) Contractor/Navy→ Offshore Supply Vessel(s)
   - Vessel procedures, checklists, guidance, regulations, training etc.

4.3.2. Feedback

a) DP system (auto) → OSV Crew
   - Graphical display information
   - Subsystem status/information
   - Visual sensory feedback
   - Proprioceptive feedback
   - Auditory sensory feedback

b) DP system (manual) → OSV Crew
   - Graphical display information
   - Subsystem status/information
   - Visual sensory feedback
   - Proprioceptive feedback
   - Auditory sensory feedback

c) Signal Processing Unit → DP system
   - Actuator Feedback

d) Control Subsystems → Signal Processing
   - Raw data

e) Control Subsystems → OSV Crew
   - Visual sensory feedback
   - Proprioceptive feedback
   - Auditory sensory feedback

f) Position Ref(s)/CyScan → DP system
   - Raw data

g) Other DP system Related Sensors → DP system
   - Raw data

h) Offshore Supply Vessel → Organizational Authority
   - Situation reports, testing results, mission results, operational requests, etc.

i) Offshore Supply Vessel → Offshore Supply Vessel
   - Reflection confirmation, position information between CyScan sensor/reflectors

4.3.3. Communication

vv) Communication between OSV Contractor and Navy

ww) Communication between OSV Crewmembers

xx) Communication between OSV Crew #1 and OSV Crew #2

4.4. Hazard Definition and Safety Constraints

There is one hazard applicable to this accident that is controlled by the OSV operations control structure. The relevant hazard is *loss of minimum separation between vessels.* This hazard led to the vessel collision. The system-level safety constraints (derived from the relevant hazard) for the OSV system are:

1. Offshore Supply Vessels must not violate separation constraints during testing operation.
2. Automatic operation must not result in vessel(s) violating separation constraints.
3. Manual operation must not result in vessel(s) violating separation constraints.
4. Offshore Supply Vessels must not have an unplanned deviation in course during operations.
5. Methods must be in place to identify and correct any unplanned deviation in vessel course before minimum separation is violated.
6. Warnings must be in place to notify the vessel operators if course deviation occurs during automatic operation.

7. Measures must be available to avoid vessel collision should a failure in operation occur.

4.5. Physical Process Analysis

At this point in the CAST analysis, the physical process for the safety control structure is analyzed. The physical process of the safety control structure is analyzed in terms of safety requirements and constraints that were violated, the related emergency and safety equipment and controls, the failures and inadequate control that resulted, and the physical contextual factors that were relevant [2]. Figure 17 shows this analysis of the OSV's operations physical process.

Offshore Supply Vessel Operations Safety Controls

Safety Requirements and Constraints Violated:

- Offshore Supply Vessels must not have an unplanned deviation in course during operations
- Methods must be in place to identify and correct any unplanned deviation in vessel course before minimum separation is violated
- Offshore Supply Vessels must not violate separation constraints during testing operation

Emergency and Safety Equipment (Controls) - Partial List:

- Noise Rejection Logic (NRL) filter/alarm
- Bearing Invalid Alarm
- CyScan "Boolean Flags" used to indicate whether position and bearing data are valid
- Redundant position references
- Fully redundant dual control system
- OSV-OSV Automatic Operations Manual
- OSV-Target Vessel Manual Operations Manual
- Manual breakaway procedures

Failures and Inadequate Controls:

- Vessel 1's CyScan sent incorrect information to the DP system.
- Operating in automatic mode, Vessel 1's DP system ordered its control surfaces to respond to the incorrect CyScan input without adequate filtering.

Physical Contextual Factors:

- Potential for CyScan failure was discovered in March mishap; however testing continued before a solution was fully implemented.
- Accident occurred during testing for recertification of Vessel 1 for target follow automatic operations
- Accident occurred during one of the most stressing tests involved in the recertification process
- Vessel separation guidance had not been affirmatively finalized due to continued system testing

Figure 17: STAMP analysis at the OSV operation physical level

Looking at the physical level for the OSV operations control structure, it can be seen that many different measures were in place to help prevent an accident or mitigate the results of an accident if one were to occur. For instance, multiple NRL filters and alarms were implemented to filter faulty angular measurements from sources such as the gyro or the VRS; however, because discrete shifts were not expected for relative heading measurements, an NRL filter was not in place to screen this particular source of information. Regardless, other alarms were in place to notify the OSV crew should an issue arise, as did the Bearing Invalid Alarm when Vessel 1's DP system aggressively responded to the incorrect heading input. Once this alarm sounded, the DP Operator on both Vessel 1 and Vessel 2 responded independently and immediately (within 1 second of each other) and implemented manual breakaway procedures as outlined by the relevant operations manuals, checklist procedures, etc. However, due to the initial magnitude of the DP system incorrectly maneuvering the OSV, the actions taken by the DP Operators were inadequate to prevent the collision from occurring.

4.6. Controller Analysis

Although looking at the physical process is useful for understanding the events that contribute to an accident, it is inadequate to stop at the physical control level. The next step in the CAST analysis is to analyze each controller in the safety control structure in terms of each controller's safety-related responsibilities, unsafe decisions and control actions, and the context and process model flaws that influenced the events [2].

4.6.1. OSV Contractor and the Navy

At the time of this incident, the OSV contractor was responsible leasing Vessel 1 and Vessel 2 to the Navy. The Navy was responsible for creating and running testing procedures for the OSV Escort Operation System. Therefore, it is necessary that any detailed safety analysis includes a look at the OSV contractor and the Navy. Because of the bilateral relationship that exists between the OSV contractor and the Navy, as depicted in Figure 16, the two will be discussed together in terms of safety responsibilities. Figure 18 shows the analysis of the OSV contractor and Figure 19 shows the analysis of the Navy component.

OSV Contractor

Safety-Related Responsibilities:

- Ensure that vessels produced meet safety requirements and specifications outlined in contract.
- Provide guidance, checklists and procedures to vessel operators that influence safe operation of vessels.
- Communicate with Navy counterparts to promote safe operation and testing of OSV system.
- Ensure OSV personnel are qualified in accordance with current automatic operation qualification requirements.

Context:

- Previous issues regarding no Noise Rejection Logic (NRL) filter in DP system had not yet been corrected from 26 March incident.
- Initial design did not include NRL filter for relative heading measurements because it was believed that no instantaneous change in relative heading measurements could occur.
- Because the OSV program is in the test phase, certain information was either not known or not included in operation checklists, procedures, etc.

Unsafe Decisions and Control Actions:

- Contractor did not coordinate with the Navy to ensure Dynamic Positioning Officers had adequate target follow recency requirements.
- Contractor did not coordinate with the Navy to ensure adequate NRL filtering was used during automatic operations.

Process Model Flaws:

- Deciding that it was safe to continue testing procedures without the NRL filter fully corrected (December end date).

Figure 18: OSV Contractor Analysis

U.S Navy

Safety-Related Responsibilities:

- Provide creditable and affordable strategic solutions to the warfighter, such as Target Vessel escort operations.
- Provide adequate training to operators in support of escort operations.
- Create testing procedures for escort operations to evaluate various lateral separation distances.
- Communicate with contractor counterpart to promote safe operation and testing of OSV system.

Context:

- A rigorous and time-intensive test schedule over the past 8 years resulted in DPOs receiving less adequate in-situ training for target follow operations due to mission requirement pressures.
- Based on testing pressure and mission requirements, the Navy response to previous 26 March incident was insufficient.
- Vessel contract with contractor was nearing the end of its term. Ultimately all of the contractor vessels would be sold to the Navy.
- Minor collision occurred during one of the most stressful testing postures. The nature of the test program involves unknowns.

Unsafe Decisions and Control Actions:

- The Navy did not coordinate with contractor to ensure Dynamic Positioning Officers had adequate target follow recency requirements.
- The Navy did not ensure adequate NRL filtering was used during automatic operations.
- The Navy left out specific breakaway procedures and safety briefing requirements in its OSV-OSV test plans.

Process Model Flaws:

- Initial belief that no instantaneous change in relative heading measurements could occur (prior to 26 March accident).
- Deciding that it was safe to continue testing procedures without the NRL filter fully corrected (December end date).

Figure 19: Navy Analysis

Three months before this incident, a similar event occurred which involved the DP system and the lack of NRL filters. Yet, the decision was made that testing should continue with a greater lateral separation distance set. At any point, the OSV contractor or the Navy could have prevented the continuation of testing until the NRL filter was implemented; however, due to the intense scheduling demands of the operational program, the decision to press forward was made. Furthermore, the nature of the testing program is relevant. There are many unknowns that are inherent in the OSV operation that testing is meant to shed light on. Therefore, the mentality that arises due to this testing environment with respect to safety is different than during normal vessel operation: some risk is inherent and accepted while testing is meant to provide answers to these unknowns.

4.6.2. DP Operator, OSV Master, OSV Bridge Officer

Below the OSV contractor and the Navy in the functional control structure, the next controller to be analyzed is the OSV Crew of both Vessel 1 and Vessel 2. Within this OSV Crew, there are three different positions that are relevant: the Dynamic Positioning Operator(s), the OSV Master, and the Bridge Officer(s). An individual could be qualified for any combination of the three positions. At the most basic level, the Dynamic Positioning Officer is the person who is operating the DP system and controlling the vessel. The OSV Master is the commanding officer of the vessel, and the Bridge Officer acts in a supporting role to the OSV Master. Figure 20 and Figure 21 shows the analysis of the OSV Crew.

In this scenario, the OSV Crew members in each OSV are responsible for monitoring the DP system in automatic operation and taking manual control when necessary to ensure the safety of each OSV. After Vessel 1's DP system received erroneous data from the CyScan #1 and auto-responded by turning starboard towards Vessel 2, both DPOs on Vessel 1 and Vessel 2 responded appropriately by exercising manual takeover and breakaway. Although operating guidelines lacked specific OSV/OSV breakaway procedures, each DPO exercised their own judgment to attempt a safe breakaway. Although it is noted that the Vessel 2 DPO responded with excessive rudder use for the breakaway procedure which contributed to the minor collision between the two vessels, the time critical nature of the event and the available options for breakaway recovery points to the fact that each DPO responded to the best of their ability.

DP Operator, OSV Master, OSV Bridge Officer

Safety-Related Responsibilities:

- DP Operators are responsible for the actual maneuvering of the OSV in manual mode and the monitoring of the DP system during automatic mode.
- OSV Masters are responsible for training, understanding, and compliance with operations manual procedures.
- OSV Masters will ensure OSV Operations Manual Reference Documents and Checklists are current and approved prior to use.
- OSV Masters are responsible for completing all applicable reference documents and checklists for each Escort Operation.
- OSV Masters are responsible for retaining all checklist documents for 12 months (normal operation) and 36 months (incident occurred) for auditing purposes.
- OSV Masters are have ultimate responsibility and discretion in maneuvering their OSV for safe navigation and vessel operation.
- Bridge Officers are responsible for knowing and communicating information contained in applicable reference documents associated with test operation.
- Bridge Officers are responsible for documenting the accomplishment of checklists steps and providing secondary affirmation of checklist completion.
- Bridge Officers are responsible for communicating to the DP operator or OSV Master any time they feel that the DP system is not operating properly.
- Any human controller is responsible for initiating breakaway procedures if they feel that the safety of the vessel is in jeopardy.
- Any human controller is responsible for communicating the system state and their analysis of the DP system among each other.
- The human controllers in vessel 1 and vessel 2 are responsible for communication between the two vessels during testing procedures.

Figure 20: OSV Crew Analysis

DP Operator, OSV Master, OSV Bridge Officer (cont'd)

Context:

- Vessel 1 was operating in target follow automatic operation prior to the incident occurring.
- Vessel 2 was operating in transit mode simulating the target vessel.
- Vessel 1's CyScan error triggered multiple alarms and caused vessel 1 to turn aggressively towards vessel 2 in automatic mode.
- Both vessel 1 and vessel 2 DPO take manual control of respective vessels within one second of each other.
- DPO on vessel 2 used excessive rudder in turning starboard away from vessel 1 in attempt to avoid contact.
- Communication within and between vessels unavailable for this analysis.
- Manual takeover of vessel 1 and vessel 2 occurs within 13 and 14 seconds of erroneous heading being accepted by vessel 1 and within 22 and 23 seconds of the first alarm sounding on vessel 1.
- Operating procedures lacks specific OSV/OSV breakaway procedures and it is solely at the operators discretion to manually ensure vessel safety.

Unsafe Decisions and Control Actions:

- Due to extreme time constraints, DPO on vessel 1 and vessel 2 each exercise judgment in vessel breakaway without coordination.
- DPO on vessel 2 uses excessive rudder for breakaway procedure turning starboard causing port quarter to move in towards vessel 1.

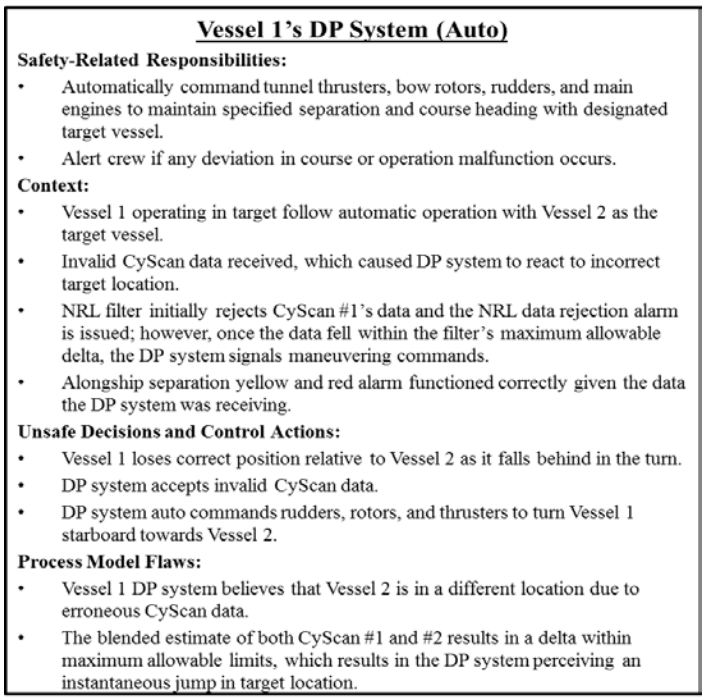
Process Model Flaws:

- Vessel 2 DPO process model regarding spatial location of both OSVs and the resulting effect of the breakaway procedure.

Figure 21: OSV Crew Analysis (continued)

4.6.3. Position References and CyScan

Figure 22 and Figure 23 shows the analysis on Vessel 1's DP system (auto) and Position Reference and CyScan sensors.



Vessel 1's DP System (Auto)

Safety-Related Responsibilities:

- Automatically command tunnel thrusters, bow rotors, rudders, and main engines to maintain specified separation and course heading with designated target vessel.
- Alert crew if any deviation in course or operation malfunction occurs.

Context:

- Vessel 1 operating in target follow automatic operation with Vessel 2 as the target vessel.
- Invalid CyScan data received, which caused DP system to react to incorrect target location.
- NRL filter initially rejects CyScan #1's data and the NRL data rejection alarm is issued; however, once the data fell within the filter's maximum allowable delta, the DP system signals maneuvering commands.
- Alongship separation yellow and red alarm functioned correctly given the data the DP system was receiving.

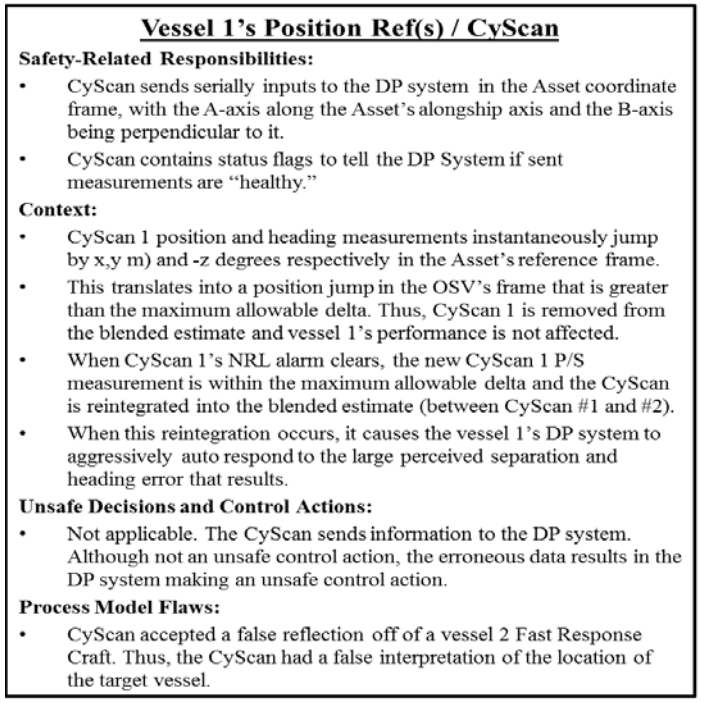
Unsafe Decisions and Control Actions:

- Vessel 1 loses correct position relative to Vessel 2 as it falls behind in the turn.
- DP system accepts invalid CyScan data.
- DP system auto commands rudders, rotors, and thrusters to turn Vessel 1 starboard towards Vessel 2.

Process Model Flaws:

- Vessel 1 DP system believes that Vessel 2 is in a different location due to erroneous CyScan data.
- The blended estimate of both CyScan #1 and #2 results in a delta within maximum allowable limits, which results in the DP system perceiving an instantaneous jump in target location.

Figure 22: Vessel 1 DP System (auto) Analysis



Vessel 1's Position Ref(s) / CyScan

Safety-Related Responsibilities:

- CyScan sends serially inputs to the DP system in the Asset coordinate frame, with the A-axis along the Asset's alongship axis and the B-axis being perpendicular to it.
- CyScan contains status flags to tell the DP System if sent measurements are "healthy."

Context:

- CyScan 1 position and heading measurements instantaneously jump by x,y m) and -z degrees respectively in the Asset's reference frame.
- This translates into a position jump in the OSV's frame that is greater than the maximum allowable delta. Thus, CyScan 1 is removed from the blended estimate and vessel 1's performance is not affected.
- When CyScan 1's NRL alarm clears, the new CyScan 1 P/S measurement is within the maximum allowable delta and the CyScan is reintegrated into the blended estimate (between CyScan #1 and #2).
- When this reintegration occurs, it causes the vessel 1's DP system to aggressively auto respond to the large perceived separation and heading error that results.

Unsafe Decisions and Control Actions:

- Not applicable. The CyScan sends information to the DP system. Although not an unsafe control action, the erroneous data results in the DP system making an unsafe control action.

Process Model Flaws:

- CyScan accepted a false reflection off of a vessel 2 Fast Response Craft. Thus, the CyScan had a false interpretation of the location of the target vessel.

Figure 23: Vessel 1 Position Reference and CyScan Analysis

The DP system combines measurements from online and healthy CyScan sensors to compute the position of the target vessel relative to the OSV. When Vessel 1 fell behind in the turn relative to Vessel 2, Vessel 1's CyScan #1 accepted a false reflection off of a Fast Response Craft on Vessel 2. This false reflection resulted in an instantaneous jump in CyScan #1's relative position and heading measurements that fell outside of the maximum allowable limit. As a result, CyScan #1's NRL alarm sounded and the data was rejected. However, once CyScan 1's position measurement fell below a specific threshold value, the NRL alarm was cleared automatically and the DP system blended both CyScan #1 and CyScan #2 data. This new blended data was accepted by Vessel 1's DP system (auto) and resulted in a perceived instantaneous jump in Vessel 2's location relative to Vessel 1. Therefore, Vessel 1's DP system (auto) responded by commanding the Vessel 1's rudders, rotors, and thrusters to aggressively turn starboard towards the Vessel 2. Each Vessel's DPO responded by taking manual control and attempting breakaway procedures, yet due to the relative location of the two vessels and the manual maneuvers that resulted, the minor collision between Vessel 1 and Vessel 2 occurred.

4.7. Safety Constraints/Requirements

With the relevant controllers analyzed, safety constraints and requirements can be generated to mitigate the unsafe control actions that were identified. Possible safety restraints/requirements could include:

1. Hazards identified in previous system assessments must be addressed and mitigated before testing resumes.
2. The DP system must not respond to any perceived instantaneous change in target vessel position.
3. Means must be available to identify and reject false inputs into the DP system.
4. Feedback must be given to the OSV Crew when false data inputs from the CyScan into the DP system occur.
5. The Navy and the OSV Contractor must provide DP Operators with measurable target follow recency requirements.
6. DP Operators must not operate an OSV unless target follow recency requirements are met.

7. The Navy and the OSV Contractor must coordinate and allocate responsibility for creating specific breakaway procedures and safety briefings for OSV operations.
8. The OSV Crew must receive training on specific breakaway procedures and when specific procedures are appropriate for different scenarios.
9. The OSV Crew must receive applicable safety briefings before OSV operations occur.
10. During OSV/OSV testing, the operators controlling the OSV must coordinate with one another (if time permits) when breakaway procedures begin.
11. The OSV Crew must receive feedback regarding the position and heading of both OSVs during OSV/OSV testing.
12. Measures must be in place to assess the future outcome of both OSV operators performing breakaway procedures simultaneously during OSV/OSV testing.
13. The OSV Crew must receive feedback independent from the DP system if the OSV is on a collision course with an external object or vessel.
14. If a situation requires both OSVs to implement breakaway procedures at the same time, a formal structure should be in place to guide how a dual breakaway differs from a singular breakaway (such as when an OSV breaks away from a target vessel).
15. CyScan sensors must be able to identify false reflections and must not use false reflections to send invalid signals to the DP system.

4.8. Comparing CAST to STPA

When comparing the CAST case study in this chapter to the STPA case study discussed in Chapter 2, the similarities between the two analyses are readily apparent. While STPA is a hazard analysis technique that is best utilized early in the concept development stage of a system's lifecycle (although it can be applied at any point in the system's developmental lifecycle), CAST is an accident analysis technique that is utilized after an accident has occurred to determine the causal factors that contributed to the accident. As such, the methods have two different focuses: hazard analysis and accident analysis. Yet, because both techniques are based on the systems theoretic accident model and processes (STAMP) framework, the underlying foundation of the two methods leads to many commonalities when using these methods for analysis.

4.8.1. Functional Control Structures

The functional control structure that was modeled in Chapter 2 for the STPA case study is equivalent to the functional control structure that is modeled in this chapter for the CAST case study. Looking at Figure 5 in Chapter 2, one can see that the functional control structure models the functional relationship of the components within the OSV system. For the STPA case study, the OSV system is being utilized for target follow escort operations, and as such, the OSV is interacting with a target vessel. This target vessel is not expanded in Figure 5 because the target vessel's control actions are not part of the hazard analysis. However, the CAST case study analyzes OSV/OSV testing, and in doing so, the target vessel that is depicted in Figure 5 is depicted as a second OSV for the CAST analysis in Figure 16. Comparing Figure 5 (the functional control structure for STPA) to Figure 16 (the functional control structure for CAST), one can see that if STPA is used for hazard analysis early on in a system's developmental lifecycle, the functional control structure is already created and available for use in the CAST accident analysis framework should the need for accident analysis arise. This is beneficial because it reduces the amount of work required to conduct the accident analysis, as the functional relationship between the system components has already been modeled as part of the STPA process.

4.8.2. Controller Analysis

Using CAST, process model flaws that lead to unsafe control actions are identified for each relevant controller that was part of the accident. Similarly, throughout the STPA process, the safety-related responsibilities of the system controllers are documented and potential process model flaws that could lead to hazardous system states and unsafe control actions are identified. These STPA results can also be used to reduce the amount of work required to complete a CAST accident analysis. For instance, in the STPA case study, one UCA that was identified was the DP system giving an unsafe directional command to maneuver towards the target vessel during automatic operations (UCA18). One of the identified causal scenarios that could lead to this happening included the DP system having a flawed process model of the target vessels' location due to incorrect sensor information being accepted and used by the DP system (scenario 18a). Comparing this to the CAST Vessel 1 DP system (auto) analysis in Figure 22, the exact same unsafe control action and process model flaw is identified as a contributing factor to the accident.

Looking through the STPA case study, it can be seen that potential unsafe control actions and casual scenarios that are identified as part of the hazard analysis arise in the CAST accident analysis as unsafe control actions and process model flaws that did in fact contribute to the accident. While the CAST accident analysis cannot rely wholly on the STPA results, by framing the problem in terms of unsafe control and process model flaws during hazard analysis by using STPA, the follow on accident analysis using CAST will require less work in determining what went wrong should an accident occur.

Page intentionally left blank.

5. Conclusions

5.1. Summary of Work

This thesis demonstrated the effectiveness of using STPA for hazard analysis by applying STPA to an OSV DP system case study and comparing the results obtained through this process to independently conducted FTA and FMEA of the same system.

Chapter 2 presented how STPA was applied to the OSV DP system case study. In doing so, the accidents and hazards that were chosen to guide the STPA analysis were highlighted and the functional control structure that modeled the functional relationship between system components was presented. Chapter 2 showed how this functional control structure was used to identify unsafe control actions, system level safety constraints, causal scenarios, and potential safety recommendations for the OSV DP system. In total, STPA found 46 unsafe control actions, 37 system level safety constraints, and 171 potential safety recommendations for this case study.

Chapter 3 compared the results obtained through the use of STPA in Chapter 2 to independently conducted FTA and FMEA of the same system. The problem space where each method focuses is shown and the common identification of failures across methods is discussed. Furthermore, three representative examples were discussed in further detail to show areas where STPA is able to find additional results not identified through the use of traditional techniques. These examples highlight how STPA is able to identify unsafe scenarios where no failure occurs, unsafe scenarios that result from process model flaws, and how STPA more adequately considers the operational environment relative to the traditional hazard analysis techniques. It was concluded that STPA not only found all of the failures identified through traditional techniques, but also identified additional safety concerns not found through the use of FTA and FMEA. After comparing the STPA results to FTA and FMEA, MIL-STD-882E compliance is shown by dissecting the general elements of the system safety process as well as specific tasks that may be called out in system contracts.

Chapter 4 presented an accident analysis of an OSV/OSV collision using the CAST framework. This chapter walked through the CAST process and showed how CAST was used to generate

safety recommendations that considered not only system failures, but the systemic causal factors that contributed to the accident as well. Chapter 4 also discussed the similarities between STPA hazard analysis and CAST accident analysis and concluded that using STPA for hazard analysis significantly reduces that amount of work required to perform an accident analysis of the same system using the CAST framework.

5.2. Contributions

This thesis makes several contributions to both academic researchers and industry collaborators. The following are the primary contributions resulting from this thesis:

- **Case study results that may be used to improve dynamic positioning system safety.**

The case study in this thesis included an in-depth hazard analysis of an OSV DP system. As such, the functional control structure that was modeled is generic enough that it can be applied to dynamic positioning systems used in other applications. Furthermore, the full results of the STPA case study presented in Appendix A through D identify unsafe control actions, causal scenarios, and possible recommendations that may be applicable not only for the OSV DP system that is analyzed, but also similar DP systems used in additional applications. It is the hope of the author that the results obtained through the use of STPA on this case study can be used to make design changes and well as procedural changes that will increase the safety of OSV operations that utilize DP systems.

- **Technique comparison adds to the validity of STPA as a hazard analysis technique.**

By comparing the results of the STPA hazard analysis to independently conducted FTA and FMEA of the same system, it is the hope of the author that the results comparison strengthens the argument that STPA is a viable and robust option for hazard analysis relative to traditional techniques. By showing that STPA found all failures identified by traditional analysis techniques as well as more safety concerns not identified by traditional techniques, this thesis work adds to the existing literature that STPA as a hazard analysis technique is more successful at identifying safety concerns that traditional techniques such as FTA and FMEA. Furthermore, by showing how STPA is compliant with MIL-STD-882E, this thesis work further adds to the argument that STPA can be used as the primary hazard analysis technique to meet potential contractual requirements as well as to successfully design safety into the system.

- **Additional STPA example can be used to learn STPA process.**

As with any analysis technique, practice is necessary to increase the analyst's level of competence when using the technique. As such, the case study presented in this thesis adds to the existing number of STPA examples and provides an additional example which can be studied by other academics and professionals when learning how to use STPA. While the case study delves into details that are very specific to dynamic positioning systems, the level of analysis is such that it can be easily followed by those with little knowledge of DP systems.

5.3. Future Work

The research contained within this thesis may be used to perform additional analysis; the author suggests the following for future work:

- **Perform an STPA of the OSV DP system to analyze additional emergent properties.**

The STPA analysis in Chapter 2 focused on only one emergent property of the OSV's DP system: safety. What makes STPA such a powerful and useful analysis technique is the ability for the STPA process to guide the analysis of any of the system's emergent properties. Given that the framework is already set and the functional control structure of the system is already modeled, this STPA analysis that is focused on safety could be used as a starting point to analyze other emergent properties of the OSV DP system, such as security. By using the analysis contained within this thesis, an STPA-sec analysis would require much less work to complete than if being performed completely independently.

- **Collect workload metrics and compare to traditional hazard analysis techniques.**

The time taken to complete the STPA analysis in Chapter 2 was not rigorously measured or documented as part of this effort. In future comparative analyses where STPA is being compared to traditional analysis techniques, a rigorous collection and analysis of workload across techniques would add to the comparison that is being made. Subjectively, the author would argue that using STPA took much less time to complete than the traditional techniques that STPA was compared against; however, further research is needed to validate this claim.

Page intentionally left blank.

Bibliography

[1] D. F. Phillips, "Classic Single Point Failures of Redundant DP Systems," Dynamic Positioning Conference, October 13-14, 1998.

[2] N. Leveson, Engineering a Safer World: MIT Press, 2012.

[3] S. S. Ge, C. Y. Sang, and B. V. E. How, "Dynamic Positioning System for Marine Vessels," *The Impact of Control Technology*, T. Samad and A.M. Annaswamy (eds.), IEEE Control Systems Society, 2011, available at www.ieeecss.org.

[4] American Bureau of Shipping, "GUIDE FOR DYNAMIC POSITIONING SYSTEMS," American Bureau of Shipping Incorporated, July, 2014.

[5] L-3 Dynamic Positioning & Control Systems, "NMS6000 Class 2 Dynamic Positioning System," n.d. [Online]. Available: www.l-3mps.com/pdfs/NMS6000-CL2.pdf. [Accessed 26 March 2015].

[6] H. Verhoeven, H. Chen, and T. Moan, "Safety of Dynamic Positioning Operation on Mobile Offshore Drilling Units," Dynamic Positioning Conference, September 28-30, 2004.

[7] R. T. Anderson, Reliability Design Handbook, Reliability Analysis Center: ITT Research Institute, March, 1976.

[8] S. Pilot, "What is a Fault Tree Analysis: Use a General Conclusion to Determine Specific Causes of Systems Failure," Best of Back to Basics: March 2002, January, 2016.

[9] J. Marshall, "An Introduction to Fault Tree Analysis (FTA)," The University of Warwick, Peuss 2011/2012.

[10] National Aeronautics and Space Administration, Procedure for Failure Mode, Effects, and Criticality Analysis (FMECA), Office of Manned Space Flight: Apollo Program, August, 1966.

[11] D. H. Stamatis, Failure Mode and Effect Analysis: FMEA from Theory to Execution: ASQ Quality Press, 2003.

[12] N. Leveson, "A Comparison of STPA and the ARP 4761 Safety Assessment Process," MIT PSAS, October, 2014.

[13] A. Obaldo and J. Monat, "[OSV] Collision and Allision Hazard Fault Trees and Probabilistic Risk Assessment," Systems Planning and Analysis, December, 2014.

[14] Hornbeck Offshore Services, "HOS DP2 Proving Trials," Report # H11920, April 01, 2014.

[15] Department of Defense, MIL-STD-882E: Standard Practice for System Safety, U.S Department of Defense, May 11, 2012.

Appendix A: OSV Crew/DP System (auto)

This appendix presents the full list of unsafe control actions that were identified between the OSV Crew and the DP system (auto) as well as the full list of associated safety constraints and causal scenarios.

Table 8 lists all of the identified unsafe control actions that were identified between the OSV Crew and the DP system (auto).

Table 8: Full List of UCAs between OSV Crew and DP System (auto)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Activate DP System (auto)	UCA1: OSV Crew does not activate DP system (auto) when the OSV Crew believes that the DP system (auto) is controlling the OSV.[H-1, H-2]	UCA2: OSV Crew activates DP system (auto) with unsafe parameter set. [H-1, H-2]	UCA4: OSV Crew activates DP system (auto) before prescribed checklist procedures are complete. [H-1, H-2]	N/A
		UCA3: OSV Crew activates DP system (auto) during unsafe sea state. [H-1, H-2]	UCA5: OSV Crew waits to activate DP system (auto) x amount of time after actively relinquishing manual control of the vessel. [H-1, H-2]	
Deactivate DP System (auto)	UCA6: OSV Crew does not deactivate DP system (auto) and assume active manual control of the OSV when DP system (auto) results in unsafe maneuvering. [H-1, H-2]	UCA8: OSV Crew deactivates DP system (auto) without assuming active manual control of OSV. [H-1, H-2]	UCA10: OSV Crew deactivates DP system (auto) x amount of time before resuming active manual control. [H-1, H-2]	N/A

	UCA7: OSV Crew does not deactivate DP system (auto) when directed by the target vessel and the target vessel has initiated the removal of reflectors. [H-1, H-2]	UCA9: OSV Crew deactivates DP system (auto) when transferring to manual control will result in unsafe vessel maneuvering. [H-1, H-2]	UCA11: OSV Crew deactivates DP system (auto) x amount of time after the DP system experiences critical faults requiring immediate manual control. [H-1, H-2]	
Set DP system user configurable parameter	UCA12: OSV Crew does not set a required user configurable parameter when the default value is unsafe. [H-1, H-2]	UCA14: OSV Crew sets an invalid user configurable parameter when the default value is unsafe. [H-1, H-2]	N/A	N/A
	UCA13: OSV Crew does not update system parameter when changing situation requires a parameter to be updated. [H-1, H-2]	UCA15: OSV Crew changes a user configurable parameter to an unsafe value inside of specified lateral separation distance. [H-1, H-2]		

The full list of safety constraints/requirements associated with the identified unsafe control actions are as follows:

SC1: The control mode that is controlling the OSV must be depicted at all times. [UCA1]

SC2: The OSV Crew must not activate DP system (auto) with unsafe parameters set. [UCA2]

SC3: The OSV Crew must not activate DP system (auto) during an unsafe sea state. [UCA3]

SC4: The OSV Crew must not activate DP system (auto) before all prescribed checklist procedures have been completed. [UCA4]

SC5: The OSV Crew must not relinquish active control of the OSV until it is verified that automatic operations have been started. [UCA5]

SC6: The OSV Crew must deactivate DP system (auto) and take full manual control when DP system (auto) results in maneuvering that is unsafe for the given operation. [UCA6]
SC7: The OSV Crew must immediately deactivate DP system (auto) when commanded by the target vessel. [UCA7, UCA11]
SC8: The OSV Crew must never deactivate DP system (auto) without immediately assuming active manual control of the OSV. [UCA8, UCA10]
SC9: The OSV Crew must never transfer to full manual control of the OSV when doing so results in unsafe vessel maneuvering. [UCA9]
SC10: The OSV Crew must set all required user configurable parameters and verify that the parameter values are correct and promote safe maneuvering. [UCA12]
SC11: The OSV Crew must update all required user configurable parameters when the situation requires a parameter to be updated. [UCA13]
SC12: The OSV Crew must not set invalid user configurable parameter values. [UCA14]
SC13: The OSV Crew must not set unsafe user configurable parameter values inside of a predetermined lateral separation distance. [UCA15]

The causal scenarios and associated requirements for the full list of unsafe control actions are presented below.

Unsafe Control Action- UCA1: OSV Crew does not activate DP system (auto) when the OSV Crew believes that the DP system (auto) is controlling the OSV. [H-1, H-2]

Scenario 1: During OSV /Target Vessel escort operations, manual mode is the default mode for OSV control. To implement automatic mode where the DP system has control of the OSV, a number of steps are required to set up the automatic operation. Among the first items on the specific OSV / Target Vessel automatic operations checklist is the general set up page. Furthermore, once general setup is completed, subsequent checklist items are in place for the human operator to complete before transitioning to automatic operations. To begin target following automatic operations, the operator obtains permission to take station, maneuvers the OSV appropriately, checks sensors and other relevant parameters to verify correct operation, and

initializes target follow mode, which transfers control of the OSV to the DP system in automatic mode. Reasons that the OSV Crew might not activate the DP system (auto) could include:

a) Each OSV Crew member believes that another crew member is responsible for checklist items needed to implement DP system (auto). This could occur due to changing crew roles during mode transition.
b) Crew members sign off on checklist items that have not been completed. This could be a result of excessive workload, normalization of deviance, etc.
c) The OSV Crew follows the correct procedures but equipment failure results in the DP system (auto) not being implemented.
d) Depending on the maneuvering characteristics of the OSV, the human operator could incorrectly believe that target follow mode has been initialized when in actuality it has not begun.

Possible requirements for Scenario 1:

1. The active control mode must be depicted to the OSV Crew and noticeable to prevent mode confusion.
2. Information between the two DP consoles must be the same and must accurately portray the DP system state and the OSV operation.
3. The DP system must not change the mode without being commanded to do so by the OSV Crew. Any change in control mode must be audibly and visually annunciated to the OSV Crew.
4. Procedures must be in place that outlines the role of OSV crewmembers in controlling the OSV. If any member of the OSV Crew besides the current active controller changes the control mode for any reason, the change must be communicated among OSV crewmembers.
5. Any component failure that prevents mode changes must be identifiable and give feedback to the OSV Crew that the mode change has not occurred.

Unsafe Control Action- UCA2: OSV Crew activates DP system (auto) with unsafe parameter set. [H-1, H-2]

Scenario 2: The OSV Crew activates the DP system (auto) because the crew believes that the parameter values are safe (the OSV Crew has a flawed process model). Reasons for a flawed process model could include:

a) DP system set up is correct for a different operation, but incorrect for the current operation. This could cause the OSV crewmembers to mistakenly believe the parameter set is correct.
b) The OSV Crew does not notice that a parameter value is unsafe.
c) The OSV Crew changed the parameter value and did not realize that the change was incorrect.
d) The OSV Crew made an invalid parameter change and the DP system reverted to the default parameter value.
e) The OSV Crew performs a checklist item that is not implemented correctly by the DP system.

Possible requirements for Scenario 2:

1. DP system parameters must be verified and confirmed before activating DP system (auto) to ensure that input parameters promote safe vessel operation.
2. Means must be available to determine if parameter values in DP system setup are safe.
3. Default parameter values should be distinguishable from non-default values so that the OSV Crew knows when a parameter value is set to the default value.
4. The OSV Crew must receive feedback if an invalid parameter value is input during DP system setup.
5. Malfunctions with the DP system that result in an input not being implemented by the DP system must result in a noticeable alert to the OSV Crew.

Scenario 2a: The OSV Crew activates the DP system (auto) with an unsafe parameter set because crewmembers believe that another member has changed the parameter values (incorrect process model). Reasons for an incorrect process model could include:

a) A situation arises during DP system setup that requires the DP operator to change prior to activating the DP system (auto).
b) An OSV crewmember signs off on the setup checklist without verifying the checklist procedures.

Possible requirements for Scenario 2a:

1. If the DP Operator changes during checklist procedures, the set up procedures must be started again from the beginning.
2. If possible, OSV crewmembers must actively confirm checklist actions before signing off on the checklist item.

Unsafe Control Action- UCA3: OSV Crew activates DP system (auto) during unsafe sea state. [H-1, H-2]

Scenario 3: The ability of the DP system to properly maintain its position relative to the target vessel is highly dependent on the mission environment at the time of operation. Therefore, guidelines are in place to regulate when the DP system may be used during OSV operations. External variables that are considered include the current sea state, swell heights, visibility conditions, and wind speeds. The OSV Crew could activate DP system (auto) during an unsafe sea state due to a flawed process model regarding the sea state. Reasons that the OSV Crew may have a flawed process model could include:

a) The OSV Crew does not have accurate feedback regarding the current sea state classification.
b) The OSV Crew does not have accurate feedback regarding current swell heights.
c) The OSV Crew does not have accurate feedback regarding the current wind speeds.
d) The OSV Crew inaccurately classifies visibility conditions.
e) The OSV Crew misinterprets correct sensor data regarding these variables.
f) The environment changes abruptly during the transition to DP system (auto) operations.

Possible requirements for Scenario 3:

1. The OSV Crew must be notified if the sea state is such that the conditions are unsafe for automatic OSV operations. If possible, sensor information should be integrated to output a sea state classification.
2. Sensors should give information to the OSV Crew regarding swell heights and wind speed. If swell heights or wind speeds are above the predetermined limit for automatic operations, the feedback should reflect this fact.

3. If possible, transitioning to automatic operations when wind speed, swell height, and sea state sensor data exceeds safe operating limits should not be possible.
4. There must be quantifiable visibility requirements that if not met prohibit automatic operations.

Scenario 3a: The OSV Crew activates DP system (auto) because a command is given by the target vessel to perform escort services during an unsafe sea state.

Possible requirements for Scenario 3a:

1. The OSV Crew must have the authority to disregard target vessel commands to perform automatic operations if the sea state is at an unsafe level.
2. Automatic operations must not be allowed if environmental conditions are unsafe. While it should be within the OSV Crew's discretion to not perform automatic operations if they feel that safety is an issue, the OSV Crew must not be allowed to perform automatic operations at their discretion in an unsafe sea state.

Unsafe Control Action- UCA4: OSV Crew activates DP system (auto) before prescribed checklist procedures are complete. [H-1, H-2]

Scenario 4: A scenario exists where the OSV is behind schedule and is not ready to perform automatic operations when the target vessel is ready to begin operations. The OSV Crew activates DP system (auto) before prescribed checklist procedures are complete (or rushes through checklist procedures) in order to stay on schedule and perform required operations with the target vessel.

Possible requirements for Scenario 4:

1. The DP system must not be able to be activated unless all required set up procedures are accomplished.
2. Before the DP system is activated, the OSV Crew must have an opportunity to review all input setup parameters and verify that they are correct.

3. Independent verification should be used to ensure that all checklist procedures are completed prior to starting automatic OSV operations.

Scenario 4a: The OSV Crew believes that they have completed all required checklist procedures and activates the DP system, when in reality; some checklist procedures have been omitted (flawed process model). Reasons the OSV Crew could have a flawed process model include:

a) The OSV Crew receives incorrect feedback that makes them think a checklist item has been accomplished when it has not been.
b) A communication failure among OSV crewmembers occurs, leading OSV crewmembers to believe someone else has completed a checklist action item.

Possible requirements for Scenario 4a:

1. Positive feedback should be used when possible to confirm that DP system setup items have been accomplished.
2. Default parameter values should be distinguishable from non-default parameter values to prevent confusion among the OSV Crew.
3. Guidelines must be in place to regulate who actively performs setup action items and who verifies checklist procedures.

Unsafe Control Action- UCA5: OSV Crew waits to activate DP system (auto) x amount of time after actively relinquishing manual control of the vessel. [H-1, H-2]

Scenario 5: The OSV Crew activates DP system (auto) and it takes x amount of time for DP system (auto) to actively begin controlling the OSV. The OSV Crew does not realize this lag occurs and relinquishes active control of the OSV before the DP system begins controlling the OSV.

Possible requirements for Scenario 5:

1. The DP system must begin exerting control over the OSV within x amount of time after the OSV transfers control of the OSV to the DP system.

2. The OSV Crew must verify that the DP system is actively and accurately controlling the OSV when DP system (auto) is activated.
3. The OSV Crew must receive feedback that the DP system has taken control of the OSV when automatic operations begin.

Scenario 5a: The OSV Crew believes that they have activated the DP system for automatic operations when a malfunction or system fault causes the mode transfer to fail. The OSV Crew does not realize that the mode transfer did not occur for x amount of time.

Possible requirements for Scenario 5a:

1. The OSV Crew must never relinquish manual control of the OSV until it is verified that the DP system is actively controlling the OSV.
2. The OSV Crew must receive noticeable feedback if a mode transfer fails to prevent mode confusion.

Unsafe Control Action- UCA6: OSV Crew does not deactivate DP system (auto) and assume active manual control of the OSV when DP system (auto) results in unsafe maneuvering. [H-1, H-2]

Scenario 6: The OSV Crew does not recognize that the DP system (auto) is performing unsafe maneuvers. The OSV Crew could have this flawed process model of the DP system because:

a) The DP system is giving incorrect feedback to the OSV Crew regarding its functioning and/or maneuvering.
b) External cues are not available to the OSV Crew that allows them to assess the OSV's maneuvering characteristics.
c) The DP system is slowly deviating from desired maneuvering and the OSV Crew does not recognize the deviation in time to correct it.
d) DP system thresholds and/or alarm values have been set incorrectly so that unsafe maneuvering does not result in an alarm going off.

Possible requirements for Scenario 6:

1. The OSV Crew must receive feedback regarding how close the OSV is to the target vessel, an external structure, terrain, or another vessel regardless of the DP system threshold and alarm values that are set.
2. Feedback must be structured such that small deviations and movement trends are noticeable and easily accessible to the OSV Crew.
3. Maneuvering and position feedback must be present separate from the DP system so that incorrect or missing feedback from the DP system does not result in degradation of situational awareness.
4. The OSV Crew must be notified if OSV automatic operations results in maneuvering that is unsafe or different than the correct operation.

Scenario 6a: The OSV Crew is unable to activate full manual mode because of a DP system malfunction or other system failure that prevents the mode transfer.

Possible requirements for Scenario 6a:

1. The DP system must never prevent the OSV Crew from activing full manual control of the OSV.
2. Means must be available to recognize and fix DP system faults that could affect OSV maneuvering.

Unsafe Control Action- UCA7: OSV Crew does not deactivate DP system (auto) when directed by the target vessel and the target vessel has initiated the removal of reflectors. [H-1, H-2]

Scenario 7: Miscommunication between the target vessel and the OSV results in the target vessel crewmembers not telling the OSV Crew that they are initiating the removal of CyScan reflectors.

Possible requirements for Scenario 7:

1. The OSV Crew must always receive notification from the target vessel in advance of the target vessel initiating the removal of CyScan reflectors.

Scenario 7a: If the target vessel has initiated the removal of reflectors, false CyScan reflections could result in the DP system continuing to operate with invalid CyScan data if other communication between the OSV and target vessel has failed.

Possible requirements for Scenario 7a:

1. The OSV Crew must assume full manual control of the OSV if CyScan data is lost or invalid.
2. Measures must be in place to identify invalid or lost CyScan data.
3. Measures must be in place to prevent the CyScan from sending incorrect data to the DP system due to false reflections.

Unsafe Control Action- UCA8: OSV Crew deactivates DP system (auto) without assuming active manual control of OSV. [H-1, H-2]

Scenario 8: The OSV Crew deactivates the DP system (auto) without knowing that the DP system has been deactivated. The OSV Crew may have this incorrect process model because:

a) The feedback displays do not noticeably indicate when the control mode that is controlling the OSV changes.
b) There is no noticeable change that occurs when the DP system is deactivated.

Possible requirements for Scenario 8:

1. Any change in control mode must be noticeably annunciated to the OSV Crew.

Scenario 8a: The OSV Crew intentionally deactivates the DP system (auto), but they are unable to take active manual control of the OSV. The OSV Crew may be unable to take full manual control of the OSV because of:

a) A mechanical failure in the manual control system.
b) A failure in the process to change control modes.
c) Interference from the DP system.

Possible requirements for Scenario 8a:

1. No single mechanical failure should result in the inability to manually control the OSV.
2. The DP system must never interfere with manually controlling the OSV.
3. Resources must be in place to prevent the accidental activation of full manual control; however, the process put in place to take full manual control of the OSV must not hinder the OSV Crew from taking full manual control of the OSV.

Unsafe Control Action- UCA9: OSV Crew deactivates DP system (auto) when transferring to manual control will result in unsafe vessel maneuvering. [H-1, H-2]

Scenario 9: The OSV Crew deactivates the DP system (auto) when the full manual controls are set incorrectly. The DP system is setup to immediately transfer control between automatic and full manual modes; therefore, when transferring to full manual mode, the initial position of the manual controls is extremely important. Reasons the manual controls could be set incorrectly include:

a) The controls are setup correctly away from the target vessel per checklist procedures but are too aggressive for the operating envelope.
b) The controls are setup correctly away from the target vessel per checklist procedures but would result in the OSV maneuvering towards another hazard (terrain, external structure, another vessel).
c) The controls are set up incorrectly towards the target vessel because they were not adjusted after transferring to automatic operations.

Possible requirements for Scenario 9:

1. Testing must be done to determine safe manual control settings for different OSV locations in the operating envelope to ensure that in the event that a transfer to full manual mode occurs, the manual control settings are not too aggressive for the OSV.
2. Means must be available to determine if breaking away from the target vessel at any given time will result in the OSV risking collision with another source.

3. Full manual controls must never be set towards the target vessel while the DP system is operating. The default must be away from the target vessel in case the DP system stops functioning.
4. The OSV Crew must receive training on different defined breakaway procedures that utilize full manual breakaway and DP system manual breakaway so that there are various options available for breakaway depending on the situation.

Scenario 9a: The DP system (auto) is controlling the OSV towards the target vessel and the OSV Crew transfers to full manual. An error occurs that does not allow a seamless transfer between the DP system and full manual mode.

Possible requirements for Scenario 9a:

1. No failure should prevent a seamless transfer while changing control modes.
2. Methods must be in place to ensure that a seamless transfer to full manual mode is always possible.

Unsafe Control Action- UCA10: OSV Crew deactivates DP system (auto) x amount of time before resuming active manual control. [H-1, H-2]

Scenario 10: The OSV Crew deactivates DP system (auto) accidentally and does not realize that automatic control has been deactivated. Instead of transferring to full manual mode, the OSV is in DP system (manual) mode with no active control being exerted. The OSV Crew could have this flawed process model because:

a) A failure causes the DP system to incorrectly show what mode is controlling the OSV.
b) The OSV Crew does not notice feedback saying that the OSV is no longer in automatic mode.
c) The current OSV maneuvering is such that control inputs are minimal at the time of the DP system (auto) being deactivated, resulting in the OSV Crew not realizing that some active control is not being exerted.

Possible requirements for Scenario 10:

1. There must be multiple, independent sources of feedback depicting what control mode the OSV is operating with.
2. Any change in control mode must be noticeably annunciated to the OSV Crew.

Scenario 10a: The OSV Crew deactivates DP system (auto) and reverts to DP system (manual) or full manual control, but a system delay or software/hardware failure results in active manual control of the OSV being delayed.

Possible requirements for Scenario 10a:

1. The DP system must not have any lag time that noticeably affects OSV control.
2. No single hardware failure should prevent full manual control of the OSV from immediately occurring.

Unsafe Control Action- UCA11: OSV Crew deactivates DP system (auto) x amount of time after the DP system experiences critical faults requiring immediate manual control. [H-1, H-2]

Scenario 11: Multiple DP system alarms sound, but due to excessive workload and a demanding operational scenario, the OSV Crew is unable to immediately determine what the problem with the DP system is and thus delays in deactivating DP system (auto).

Possible requirements for Scenario 11:

1. Alarms must be prioritized and organized in such a manner that multiple alarms occurring at once do not become confusing.
2. Alarm feedback must contain enough information and being available in such a manner for the crew to understand immediately what the alarm signifies.
3. OSV Crews must receive training to minimize their reaction time during emergency situations and to aid in their understanding of system alarms.

Scenario 11a: The OSV Crew does not know that the DP system has experienced a critical fault that requires deactivation of the DP system (auto). The OSV Crew could have this flawed process model because:

a) The critical fault is not detected by the DP system.
b) The critical fault affects the feedback mechanism used to alert the OSV Crew.
c) The OSV Crew ignores the feedback that there is a critical fault because of frequent false alarms associated with the fault.

Possible requirements for Scenario 11a:

1. Testing must be done to determine what critical faults are present in the DP system. Sensors must be in place to detect these critical faults and give feedback to the OSV Crew that they have occurred.
2. Feedback mechanisms must not be affected by critical DP system faults. Redundant feedback should be used when the feedback mechanism cannot be protected against DP system faults.
3. False alarms must be avoided as much as possible while still ensuring that the alarm is useful. The OSV Crew must always respond appropriately to system critical fault alarms.

Unsafe Control Action- UCA12: OSV Crew does not set a required user configurable parameter when the default value is unsafe. [H-1, H-2]

Scenario 12: The OSV is preparing to conduct OSV / Target Vessel operations. Checklist procedures require the OSV Crew to set a number of configurable parameters to start automatic operations. If the previous OSV mission was an OSV / OSV test, the default parameter values will be incorrect and unsafe for OSV / Target Vessel operations. The OSV Crew members completing the checklist procedures may not notice this discrepancy and may not change a required user configurable parameter value that needs to be changed.

Possible requirements for Scenario 12:

1. The OSV Crew must actively verify the default configurable parameter value if no change is being made to the default parameter value.

2. When feasible, independent verification of user configurable parameters should occur to ensure that all user configurable parameters are set properly.
3. Default parameter values should be distinguishable from non-default parameter values.

Scenario 12a: The OSV Crew is required to set user configurable parameter values on the master and backup DP consoles prior to automatic operations. When the OSV Crew transfers the input data from the master to the backup console, the OSV Crew does not verify that all parameters transferred properly and the backup DP console has incorrect and unsafe parameters set.

Possible requirements for Scenario 12a:

1. All input parameters on the master and backup DP console must match after data is transferred during checklist procedures.
2. Currently, data transfer between consoles results in the Deviation Display Center parameter being reset to the default parameter value on the backup DP console. This discrepancy should be analyzed and fixed if required.
3. The master and backup DP system consoles should give feedback that the two systems contain identical information. If any information is different between the two consoles, the OSV Crew must be notified.
4. The OSV Crew should receive training on switching between the Master and Backup consoles to become proficient in the task.

Unsafe Control Action- UCA13: OSV Crew does not update a system parameter when a changing situation requires a system parameter to be updated. [H-1, H-2]

Scenario 13: During operations, many user configurable parameters will not change; however, some user configurable parameters will require change as dynamic situations progress. As such, changes in user configurable parameters are mainly limited to DP system threshold (alarm) values. As the lateral separation distance between the OSV and the target vessel changes, the OSV Crew must change the DP system thresholds values as the relative positions of the two vessels changes. If the lateral separation between the OSV and the target vessel is changing often and the OSV Crew is experiencing a

high-workload, high stress environment, the OSV Crew may forget to change the DP system threshold values.

Possible requirements for Scenario 13:

1. DP system threshold values must be compared to other available information to verify that the threshold value is appropriate for a given operation. If the threshold value is too close for a given operation, the OSV Crew should receive feedback and be required to change the threshold value.
2. The OSV Crew must receive feedback to actively verify the DP system threshold yellow/red alarm values if no change is made to the parameter value when lateral separation distances change by x feet.
3. The OSV Crew should receive trend analysis information regarding the OSV's position relative to the target vessel to help them better understand the future state of the OSV.

Unsafe Control Action- UCA14: OSV Crew sets an invalid user configurable parameter when the default value is unsafe. [H-1, H-2]

Scenario 14: The OSV Crew attempts to set an invalid user configurable parameter and checks the item off of the relevant checklist without realizing that the invalid parameter was not input into the system and the default parameter value remained. Reasons this could happen include:

a) The crewmember that inputs the invalid parameter value does not check to make sure the parameter value changes.
b) The default value is safe for other operations but not for the current operation, causing the crew member to recognize the familiar value and not notice the discrepancy.

Possible requirements for Scenario 14:

1. The DP system must not accept invalid parameter inputs. Any invalid parameter input must result in noticeable feedback to the OSV Crew.
2. The OSV Crew must be notified if an invalid user configurable parameter value is input. Furthermore, if an invalid user configurable parameter value is input, the OSV Crew must be notified that the default parameter value remains and the change was not made.

3. User configurable parameters must be displayed for review anytime a parameter change is made.

Unsafe Control Action- UCA15: OSV Crew changes a user configurable parameter to an unsafe value inside of specified lateral separation distance. [H-1, H-2]

Scenario 15: Many user configurable parameters are set prior to operations beginning and do not change for the remainder of the operation (such as target length, etc.). The OSV Crew could accidentally change one of these user configurable parameter values while trying to make a different change that is needed. The crewmember may not realize that they are changing the wrong parameter value.

Possible requirements for Scenario 15:

1. Input screens used to change configurable parameter values must clearly display what parameter value is being changed.
2. User configurable parameter values that do not change once operations begin should not be able to be changed while the DP system is operating.

Scenario 15a: The OSV Crew intentionally changes the parameter to a new value, but the value that is input is unsafe. The OSV Crew inputs an unsafe parameter value because of confusion due to different units of measurement. The OSV Crew could put in the correct value for the incorrect unit of measurement for a given user configurable parameter.

Possible requirements for Scenario 15a:

1. User configurable parameter values must display the associated unit of measurement.
2. The DP system must reject input user configurable parameter values that are outside of a predetermined range while automatic operations are occurring.

Appendix B: DP System/Signal Processing Unit

This appendix presents the full list of unsafe control actions that were identified between the DP system and the Signal Processing Unit as well as the full list of associated safety constraints and causal scenarios.

Table 9 lists all of the identified unsafe control actions that were identified between the DP system and the Signal Processing Unit.

Table 9: Full List of UCAs between DP System and Signal Processing Unit

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Provide directional command (DP Auto)	UCA16: DP system (auto) does not provide a directional command during automatic operations when a maneuver is required. [H-1, H-2]	UCA18: DP system (auto) gives an unsafe directional command to maneuver towards the target vessel, terrain, an external structure, or another vessel during automatic operations. [H-1, H-2]	UCA20: DP system (auto) gives a directional command to the OSV after manual control has been established. [H-1, H-2]	UCA22: DP system (auto) stops providing a directional command to the OSV before the desired maneuver is accomplished. [H-1]
	UCA17: DP system (auto) does not provide a directional command to all required OSV control subsystems for a given maneuver. [H-1, H-2]	UCA19: DP system (auto) gives a directional command that uses the wrong control subsystems for a given maneuver. [H-1, H-2]	UCA21: DP system (auto) gives a maneuvering command to the OSV x seconds too late to perform the maneuver successfully. [H-1, H-2]	UCA23: DP system (auto) continues providing a directional command to the OSV too long, resulting in an overshoot of the desired maneuver. [H-1]

Provide directional command (DP Manual)	UCA24: DP system (manual) does not signal the SPU when the OSV Crew gives a directional command to the control subsystems. [H-1, H-2]	UCA25: DP system (manual) signals the SPU with a control command differently than the OSV Crew intends. [H-1, H-2]	UCA26: DP system (manual) signals the SPU x time after the OSV Crew gives a command to the control subsystems. [H-1, H-2]	UCA27: DP system (manual) stops signaling the SPU before the control command is implemented. [H-1, H-2]

The full list of safety constraints/requirements associated with the identified unsafe control actions are as follows:

SC14: DP system (auto) must immediately provide all required directional commands to all relevant control subsystems needed for safe OSV maneuvering while in automatic operations. [UCA16, UCA17, UCA21]

SC15: DP system (auto) must not give a directional command to the OSV that would result in the OSV colliding with the target vessel, terrain, and external structure, or another vessel. [UCA18]

SC16: DP system (auto) must not give directional commands to the wrong combination of OSV control subsystems for a given maneuver. [UCA19]

SC17: DP system (auto) must not give a directional command to OSV control subsystems after manual control of the OSV has been established. [UCA20]

SC18: DP system (auto) must give directional commands to OSV control subsystems for the correct amount of time in order for the OSV to correctly perform the desired maneuver. [UCA22, UCA23]

SC19: The DP system (manual) must immediately signal directional commands given by the OSV Crew to the SPU. [UCA24, UCA26]

SC20: The DP system (manual) must never signal the SPU to make a directional command if the command is not provided by the OSV Crew. [UCA25]

SC21: The DP system (manual) must continue signaling the SPU to control the OSV control subsystems until the command is successfully implemented. [UCA27]

The causal scenarios and associated requirements for the full list of unsafe control actions are presented below.

Unsafe Control Action- UCA16: DP system (auto) does not provide a directional command during automatic operations when a maneuver is required. [H-1, H-2]

Scenario 16: DP system (auto) is controlling the OSV in target follow mode. The DP system (auto) may not provide a directional command to the OSV when a maneuver is required because it thinks the OSV is in the correct position in relation to the target vessel (flawed process model). This flawed process model could be caused by:

a) Incorrect sensor information being used by the DP system.
b) Relevant sensors not providing needed information to the DP system.
c) An error with the signal processing unit processing received sensor data.

Possible requirements for Scenario 16:

1. The DP system must be able to identify incorrect sensor data. Incorrect sensor data must not prevent the DP system from providing maneuvering commands when needed for a given maneuver.
2. The DP system should not be used if there are no independent backup sensors available to provide needed information should the main sensors fail.

Scenario 16a: DP system (auto) is controlling the OSV in target follow mode. The DP system (auto) may provide a directional command to the OSV; however, a component failure could prevent the directional command from being implemented.

Possible requirements for Scenario 16a:

1. Testing must be done to determine appropriate reliability for system components involved in DP vessel maneuvering.
2. If a component failure occurs, the independent backup must be utilized immediately. If a maneuver was in progress when the component failure occurs, the transition to the backup component must not significantly affect the maneuver that is in progress.

3. Independent components must not allow a single incident to cause both components to fail.

Unsafe Control Action- UCA17: DP system (auto) does not provide a directional command to all required OSV control subsystems for a given maneuver. [H-1, H-2]

Scenario 17: The DP system utilizes Thruster Allocation Logic (TAL) and uses the SPUs to send actuator commands to individual thrusters to meet the surge, away, and yaw axes components of the original command. If a thruster or multiple thrusters fail, an actuator reconfiguration is required to change the TAL so that maneuvering commands are broken into the correct commands for each remaining available thruster. If an actuator reconfiguration is not conducted when one is needed, all required OSV control subsystems may not be utilized for a given maneuver.

Possible requirements for Scenario 17:

1. Feedback must be given to the OSV Crew if a breakaway is required to perform an actuator reconfiguration.
2. The DP system must not send maneuvering commands to control subsystems that are no longer functioning properly.
3. The OSV Crew must be alerted if the DP system is attempting to send maneuvering commands to a control subsystem that is no longer functioning correctly.
4. The DP system must be able to adjust its TAL to immediately respond to component failures.

Scenario 17a: The DP system cannot utilize all required OSV control subsystems because the OSV Crew has indicated that needed thrusters, etc. are not in auto mode.

Possible requirements for Scenario 17a:

1. All healthy control subsystems must be put into auto before target follow mode can begin.

2. Changing a control subsystem from auto to off or manual during target follow operations must result in an appropriate change to the Thruster Allocation Logic.
3. Changing a control subsystem from auto to off or manual must require additional confirmation from the OSV Crew before the change occurs.

Unsafe Control Action- UCA18: DP system (auto) gives an unsafe directional command to maneuver towards the target vessel, terrain, an external structure, or another vessel during automatic operations. [H-1.1-H1.3, H-2]

Scenario 18: The DP system is properly controlling the OSV in target follow mode. The target vessel maneuvers in a manner that causes the OSV to respond correctly; however, the OSV response results in the OSV unsafely maneuvering towards and external structure, terrain, or another vessel.

Possible requirements for Scenario 18:

1. Guidelines must be in place that outlines operating procedures for the OSV Crew when the safety of the target vessel could jeopardize the safety of the OSV (i.e. colliding with an external structure versus colliding with the target vessel).
2. Procedures must be in place to minimize situations where external structures, other vessels, and/or terrain pose a threat to the escorting OSVs.

Scenario 18a: DP system (auto) is controlling the OSV in target follow mode. The DP system (auto) may provide an unsafe directional command to the OSV because it thinks the OSV is in a different position in relation to the target vessel than it actually is (flawed process model). This flawed process model could be caused by:

a) Incorrect sensor information being used by the DP system.
b) Relevant sensors not providing needed information to the DP system.
c) An error with the signal processing unit processing received sensor data.

Possible requirements for Scenario 18a:

1. Testing must be conducted to determine what the minimum separation distance between the target vessel and OSV should be during escort operations. The OSV Crew must have enough time to respond to an unsafe maneuver command given by the DP system to avoid contact with the target vessel, another vessel, terrain, or external structure.
2. If an error occurs with the SPU, the backup SPU must be able to transition into use without affecting the OSV maneuvering.
3. The DP system must be able to identify incorrect sensor data. Incorrect sensor data must not prevent the DP system from providing maneuvering commands when needed for a given maneuver.
4. The DP system should not be used if there are no independent backup sensors available to provide needed information should the main sensors fail.

Unsafe Control Action- UCA19: DP system (auto) gives a directional command that uses the wrong control subsystems for a given maneuver. [H-1, H-2]

Scenario 19: The DP system (auto) uses Thruster Allocation Logic (TAL) and sends a directional command to the SPU. In response, the SPU commands each individual thruster to meet the surge, away, and yaw axes components of the original command. If the TAL is wrong, the DP system could signal the wrong control subsystems from a given maneuver.

Possible requirements for Scenario 19:

1. Means must be available to test the TAL to make sure that it is correct and performs as the software programmer intends.
2. Feedback must be given to the OSV Crew to notify them if a software code change is needed for proper DP system functioning. If a software code change is needed, the DP system must not be used until the code change occurs.

Unsafe Control Action- UCA20: DP system (auto) gives a directional command to the OSV after manual control has been established. [H-1, H-2]

Scenario 20: The DP system (auto) has an incorrect process model and believes that a DP system directional command needs to be sent when the DP system is not activated. This incorrect process model could result because:

a) An anomalous signal triggers the DP system when the vessel is under manual control.
b) Faulty communication between the DP system and other OSV subsystems (missing feedback).

Possible requirements for Scenario 20:

1. DP system control inputs must never override manual control inputs. If the OSV is in manual mode, the DP system must not be able to control the OSV subsystems.
2. The DP system must have guards to prevent activation unless intentionally activated by the OSV Crew.
3. When the OSV is operating under full manual control, there must be measures in place that prevent the DP system from sending signals to the OSV control subsystems.

Unsafe Control Action- UCA21: DP system (auto) gives a maneuvering command to the OSV x seconds too late to perform the maneuver successfully. [H-1, H-2]

Scenario 21: The DP system is operating in target follow mode and gives a maneuvering command to the OSV x seconds too late to perform a given maneuver successfully because the DP system experiences a system lag that results in a maneuvering command being delayed.

Possible requirements for Scenario 21:

1. The DP system must not experience any system lag that would prevent a maneuvering command from being implemented on time to successfully perform a maneuver.
2. The OSV Crew must receive quantifiable feedback if the DP system is experiencing any amount of system lag that could affect the DP system's performance.

Scenario 21a: The OSV begins trailing behind the target vessel in target follow mode, but the DP system does not recognize that the OSV is not in the correct position relative to the target

vessel and thus gives a maneuvering command x seconds too late to correct its position relative to the target vessel. The DP system could have a flawed process model because:

a) The CyScan sensors give invalid data to the DP system causing the DP system to think that the OSV is in the correct location relative to the target vessel when it is not.
b) The CyScan sensors give valid data to the DP system that the OSV is in the incorrect location relative to the target vessel; however, the DP system processes this information incorrectly.

Possible requirements for Scenario 21a:

1. Invalid CyScan data must not result in the DP system giving a required maneuvering command too late to perform a maneuver successfully.
2. The DP system must alert the OSV Crew if an error occurs with CyScan data processing.

Unsafe Control Action- UCA22: DP system (auto) stops providing a directional command to the OSV before the desired maneuver is accomplished. [H-1]

Scenario 22: The DP system (auto) believes that the desired maneuver has been accomplished when it has not been accomplished (flawed process model) and thus stops providing directional commands when a directional command is needed. This could be the result of:

a) Thrusters giving invalid feedback to the DP system (such as more propulsion being provided than what is actually being provided).
b) Sensors giving invalid feedback, such as incorrect location of the OSV relative to the target vessel.
c) The SPU processing information incorrectly and sending the wrong feedback to the DP system CPU.

Possible requirements for Scenario 22:

1. Means must be available to verify sensor feedback even if redundant sensors are giving the same incorrect feedback.
2. The OSV Crew must receive noticeable feedback if the DP system stops a maneuver before it is fully accomplished.

3. The DP system must account for all possible additional forces in its control algorithm to ensure that maneuvering is not stopped too soon.

Unsafe Control Action- UCA23: DP system (auto) continues providing a directional command to the OSV too long, resulting in an overshoot of the desired maneuver. [H-1]

Scenario 23: The OSV is performing target follow operations and the DP system has an incorrect process model regarding the location of the OSV with respect to the target vessel when the target vessel is performing a maneuver. The DP system could have an incorrect process model because:

a) Sensors provide incorrect feedback to the DP system.
b) CyScan sensors provide incorrect data to the DP system.
c) Other sensors provide incorrect data to the DP system, resulting in the DP system not counteracting the correct amount of external forces on the OSV.

Possible requirements for Scenario 23:

1. Feedback must be given to the OSV Crew if the OSV deviates from normal target follow maneuvering.
2. Issues with any sensor that could cause the DP system to give incorrect maneuvering commands must be detectable and alert the OSV Crew. If any sensor experiences an issue where the effect on the DP system is unknown, the DP system must not be used.

Scenario 23a: The amount of thrust provided by each individual thruster is incorrect and unable to maintain proper maneuvering in relation to the target vessel. For instance, the thrusters moving the OSV towards the target vessel may provide too much thrust and the thrusters providing counterthrust may not provide enough counterthrust or may fail, resulting in the OSV overshooting its desired maneuver.

Possible requirements for Scenario 23a:

1. Feedback must be in place to alert the OSV Crew if actual thrust values deviate significantly from expected values.

2. The DP system must be able to adjust its Thruster Allocation Logic to immediately respond to component failures.

Unsafe Control Action- UCA24: DP system (manual) does not signal the SPU when the OSV Crew gives a directional command to the control subsystems. [H-1, H-2]

Scenario 24: The DP system allows the OSV Crew to use a joystick and various control knobs to control different aspects of the OSV while the DP system controls other parts of the OSV when in various DP system (manual) modes. Therefore, depending on the DP system (manual) control mode selected by the OSV Crew, the OSV Crew could get mode confusion and be unaware that a control input is not applicable for the given mode that is selected, resulting in the DP system not signaling the SPU when the OSV Crew gives a directional command.

Possible requirements for Scenario 24:

1. The specific control mode currently selected to control the OSV must be readily displayed to the OSV Crew.
2. Feedback must be given to the OSV Crew stating which control mechanisms require manual input and what each control mechanism is controlling given the selected control mode.
3. If a control mechanism is inactive for a given control mode, noticeable feedback should be given to the OSV Crew if the OSV Crew provides an input to the inactive control mechanism.

Scenario 24a: The DP system stops working but does not alert the OSV Crew that it is not working. In certain situations, the only way to realize that the DP system has stopped functioning properly is to notice that the DP system display has no movement and the time clock is not updating. If the OSV Crew does not notice this malfunction immediately, they will not realize that the DP system is not signaling the SPU in response to a command given prior to the malfunction.

Possible requirements for Scenario 24a:

1. Sensors must be added to alert the OSV Crew if the DP system has stopped and the DP console screen is frozen.

Unsafe Control Action- UCA25: DP system (manual) signals the SPU with a control command differently than the OSV Crew intends. [H-1, H-2]

Scenario 25: The OSV Crew has the option to choose different response curves for the joystick used to control OSV control subsystems in various DP system (manual) modes. For some joystick curves, small deflections in the joystick will result in a large force on the OSV. For other joystick curves, using the same amount of joystick deflection will result in a smaller force on the OSV. If the OSV Crew believes that the joystick is set to use a certain response curve when it is not, a control input could be very unsafe.

Possible requirements for Scenario 25:

1. The joystick response curve must be depicted to the OSV Crew on all DP Console screens, not just on the Heading & Position drop-down menus.
2. Multiple sources of feedback must be present for the OSV Crew to ensure that it is known which response curve the joystick is using.

Scenario 25a: The OSV Crew is confused about the specific control mode that is active at a given time, resulting in a control input that the OSV Crew believes will control a specific subsystem actually controlling a different, unintended subsystem.

Possible requirements for Scenario 25a:

1. The control mode that is active must have associated feedback regarding which control mechanisms control which OSV subsystem in that specific control mode.

Unsafe Control Action- UCA26: DP system (manual) signals the SPU x time after the OSV Crew gives a command to the control subsystems. [H-1, H-2]

Scenario 26: The OSV Crew provides a directional command through the DP system; however, system wear results in the signal being sent from the DP Console to the SPU being delayed.

Possible requirements for Scenario 26:

1. The DP system must not experience any system lag that would prevent a maneuvering command from being implemented on time to successfully perform a maneuver.
2. The OSV Crew must receive quantifiable feedback if the DP system is experiencing any amount of system lag that could affect the DP system's performance.

Unsafe Control Action- UCA27: DP system (manual) stops signaling the SPU before the control command is implemented. [H-1, H-2]

Scenario 27: The DP system is signaling the SPU to implement a control command when the connection between the DP system and the SPU is lost and/or disrupted, resulting in the control command not being fully implemented. This could happen because:

a) The specific wiring between the DP console and the SPU that is responsible for the given command becomes loose at either terminal.
b) The power supply to the DP system and SPU fails.

Possible requirements for Scenario 27:

1. Feedback must be given to the OSV Crew if any wires become loose and disrupt the communication between any components of the DP system.
2. The OSV Crew should have enough information to quickly determine what communication fault has occurred, where the issue originated, and how to fix the problem.
3. If the main power supply fails and the backup power supply turns on, the transition must not affect control commands that were occurring when the power supply was disrupted.

Scenario 27a: The DP system believes that the control command has been fully implemented and stops continuously signaling the SPU, when in reality the control commands have not been fully carried out by the OSV. The DP system could have a flawed process model because:

a) Sensors feeding information into the SPU are giving conflicting and/or incorrect data.
b) Sensors fail and stop sending information needed information to the SPU that is relevant to carrying out control commands.

Possible requirements for Scenario 27a:

1. Redundant sensors should be fully independent to ensure that one sensor failing has no influence on the other sensor(s) functioning.
2. Conflicting data sent to the SPU must result in feedback being given to the OSV Crew with enough information to diagnose and correct the problem.
3. The DP system should have a diagnostic “test” capability that allows the OSV Crew to request and receive additional diagnostic information regarding the DP system during operations.

Appendix C: OSV Crew/Position Refs and CyScan

This appendix presents the full list of unsafe control actions that were identified between the OSV Crew and the Position References/CyScan as well as the full list of associated safety constraints and causal scenarios.

Table 10 lists all of the identified unsafe control actions that were identified between the OSV Crew and the Position References/CyScan

Table 10: Full List of UCAs between the OSV Crew and Position Refs/CyScan

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Turn CyScan ON	N/A	UCA28: OSV Crew turns on CyScan for use during automatic operations with incorrect CyScan parameters set. [H-1, H-2]	N/A	N/A
		UCA29: OSV Crew turns on CyScan without disconnecting power and restarting CyScan software after it has been in suspend mode for too long. [H-1, H-2]		
Turn CyScan OFF	UCA30: OSV Crew does not turn CyScan OFF and assume manual control when the CyScan malfunctions. [H-1, H-2]	UCA31: OSV Crew turns CyScan off during automatic operations while target follow mode is active. [H-1, H-2]	UCA32: OSV Crew turns CyScan off before switching to manual control of the OSV. [H-1, H-2]	N/A

The full list of safety constraints/requirements associated with the identified unsafe control actions are as follows:

SC22: CyScan parameter values must be verified and confirmed before OSV automatic operations begin. [UCA28]

SC23: CyScan sensors should be disconnected from power and restarted after being in suspend mode for a predetermined amount of time. [UCA29]

SC24: The OSV Crew must always turn CyScan sensors off and assume full manual control of the OSV when a CyScan malfunction occurs. [UCA30]

SC25: Automatic operations must never continue if CyScan sensors are turned off. [UCA31]

SC26: The OSV Crew must immediately assume full manual control of the OSV when CyScan sensors are turned off. [UCA32]

The causal scenarios and associated requirements for the full list of unsafe control actions are presented below.

Unsafe Control Action- UCA28: OSV Crew turns on CyScan for use during automatic operations with incorrect CyScan parameters set. [H-1, H-2]

Scenario 28: The OSV Crew believes that the sensor target longitudinal offsets, tilt, and/or azimuth angle for the CyScan sensor is set correctly when in reality one or all of these parameters are incorrect. The OSV Crew's flawed process model could be the result of:

a) The OSV Crew setting an incorrect parameter value and not realizing that a mistake was made.
b) Target reflectors being set incorrectly by the target vessel crew.
c) CyScan's tilt angle is not optimal for obtaining proper reflections.

Possible requirements for Scenario 28:

1. Target reflectors must be set in the exact same location on the target vessel for all escort missions.
2. Procedures must be in place to ensure the CyScan's tilt angle is optimal during operations.

3. Feedback must be given to the OSV Crew if the CyScan's tilt angle is not optimal during operations.

Unsafe Control Action- UCA29: OSV Crew turns on CyScan without disconnecting power and restarting CyScan software after it has been in suspend mode for too long. [H-1, H-2]

Scenario 29: CyScan sensors have been in suspend mode for an extended period of time. The OSV Crew is unaware of any system irregularities due to the extended suspend mode and begins automatic operations with unsafe CyScan sensors.

Possible requirements for Scenario 29:

1. CyScan systems must record how long suspend mode periods last and this information must be readily available to the OSV Crew.
2. If CyScan sensors have been in suspend mode longer than a predetermined amount of time, the OSV Crew must receive feedback to disconnect power and restart the CyScan software before beginning automatic operations.
3. The CyScan system should require software restart and disconnect from the power supply after an extended period of suspend mode.

Scenario 29a: The DP operator does not restart the CyScan software and disconnect/reconnect the CyScan to/from its power supply because the DP operator believes that the task was performed by another member of the OSV Crew.

Possible requirements for Scenario 29a:

1. Checklist procedures must be in place that outline when and how often CyScan systems should be disconnected from its power supply and its software restarted.
2. CyScan systems must record how long suspend mode periods last and this information must be readily available to the OSV Crew.

Unsafe Control Action- UCA30: OSV Crew does not turn CyScan OFF and assume manual control when the CyScan malfunctions. [H-1, H-2]

Scenario 30: The CyScan sends invalid and faulty data to the DP system. The DP system does not recognize that the data is faulty and thus does not alert the OSV Crew that the CyScan has malfunctioned. This could result from one CyScan reflection being intentionally eliminated from the data input (due to weak signal, failure, etc.) and the remaining two CyScan reflections sending faulty data to the DP system. With only two reflections available, divergence will not be detected and the OSV Crew would not remove the CyScan from the DP system inputs.

Possible requirements for Scenario 30:

3. Automatic operations must not occur when CyScan redundancy is diminished.
4. The OSV Crew must have noticeable feedback any time that a sensor cannot use median testing to detect divergence.

Scenario 30a: The DP system detects a CyScan malfunction but does not provide an adequate alert the OSV Crew that a CyScan malfunction has occurred.

Possible requirements for Scenario 30a:

3. Further testing must be conducted to assess current DP system alarms. Testing should determine if any new alarms need to be added or if current alarms do not provide adequate information for the OSV Crew to adequately understand and respond to the alarm.
4. System critical alarms should be distinguished from non-critical alarms.

Unsafe Control Action- UCA31: OSV Crew turns CyScan off during automatic operations while target follow mode is active. [H-1, H-2]

Scenario 31: The OSV Crew is experiencing an extremely high workload during a stressful maneuver and accidentally turns the CyScan sensors off during operations while a maneuver is taking place.

Possible requirements for Scenario 31:

1. It must not be possible to turn all CyScan sensors off while target follow mode is active and the DP system is using CyScan inputs to control the OSV.
2. Any time CyScan sensors are turned off, the OSV Crew must receive an immediate and noticeable feedback that the sensors are off.
3. Turning CyScan sensors off must be multi-step and have guards in place to prevent accidentally turning off the CyScan.

Unsafe Control Action- UCA32: OSV Crew turns CyScan off before switching to manual control of the OSV. [H-1, H-2]

Scenario 32: A situation occurs that requires the OSV Crew to end automatic operations and switch to full manual control of the OSV. The OSV Crew inadvertently turns off the CyScan sensor before switching the OSV to full manual control.

Possible requirements for Scenario 32:

1. CyScan sensors must never be turned off before switching to manual control of the OSV.
2. It must not be possible to turn all CyScan sensors off while target follow mode is active and the DP system is using CyScan inputs to control the OSV.

Appendix D: OSV Crew/DP System (manual)

This appendix presents the full list of unsafe control actions that were identified between the OSV Crew and the DP system (manual) as well as the full list of associated safety constraints and causal scenarios.

Table 11 lists all of the identified unsafe control actions that were identified between the OSV Crew and the DP system (manual).

Table 11: Full List of UCAs between OSV Crew and the DP System (manual)

Control Action	Not providing causes hazard	Providing causes hazard	Incorrect timing/order	Stopped too soon/applied too long
Activate DP System (manual)	UCA33: OSV Crew does not activate DP system (manual) and actively assert manual control of the OSV when manual control is required. [H-1, H-2]	UCA34: OSV Crew activates DP system (manual) when the OSV Crew believes that DP system (auto) has active control of the OSV. [H-1, H-2]	UCA35: OSV Crew activates DP system (manual) x amount of time before beginning to exert active control of the OSV. [H-1, H-2]	N/A
Deactivate DP System (manual)	UCA36: OSV Crew does not deactivate DP system (manual) when full manual control of the OSV is needed. [H-1, H-2]	UCA37: OSV Crew deactivates DP system (manual) and activates target follow mode when activating target follow mode is unsafe. [H-1, H-2]	UCA38: OSV Crew deactivates DP system (manual) and activates target follow mode before performing required prestart procedures. [H-1, H-2]	N/A
Provide directional command	UCA39: OSV Crew does not provide a DP (manual) directional command when a directional command is required to avoid	UCA40: OSV Crew provides a DP (manual) directional command that could result in contact with the target vessel, terrain, an	UCA42: OSV Crew provides a DP (manual) directional command x seconds too late when a directional command is	N/A

	contact with the target vessel, terrain, an external structure, or another vessel. [H-1.1-H-1.3]	external structure, or another vessel. [H-1.1-H-1.3]	needed. [H-1]	
		UCA41: OSV Crew provides a DP (manual) directional command to an incorrect combination of control subsystems for a given maneuver. [H-1, H-2]		

The full list of safety constraints/requirements associated with the identified unsafe control actions are as follows:

SC27: The OSV Crew must activate DP system (manual) and actively assert manual control of the relevant OSV Control subsystems when DP system (manual) control is required. [UCA33]

SC28: The OSV Crew must never activate DP system (manual) without immediately providing the required control inputs associated with DP system (manual) control. [UCA34, UCA35]

SC29: The OSV Crew must always deactivate DP system (manual) and provide full manual control when full manual control of the OSV is required. [UCA36]

SC30: The OSV Crew must never relinquish control of the OSV in DP system (manual) until another mode of control has been established. [UCA37, UCA38]

SC31: The OSV Crew must always provide required directional commands in DP system (manual) when the directional command is needed to avoid contact with the target vessel, terrain, an external structure, or another vessel. [UCA39]

SC32: The OSV Crew must never provide directional commands to the OSV in DP system (manual) that would result in the OSV colliding with the target vessel, terrain, an external structure, or another vessel. [UCA40]

SC33: The OSV Crew must never provide a directional command to an incorrect combination of OSV control subsystems in DP system (manual). [UCA41]

SC34: Directional commands to the OSV in DP system (manual) must be given at the right time and for the correct amount of time for a given maneuver to be successfully accomplished. [UCA42]

The causal scenarios and associated requirements for the full list of unsafe control actions are presented below.

Unsafe Control Action- UCA33: OSV Crew does not activate DP system (manual) and actively assert manual control of the OSV when manual control is required. [H-1, H-2]

Scenario 33: The DP system is controlling the OSV in automatic mode when a malfunction occurs or the DP system is still able to operate but loses redundancy and is thus less safe. The current situation is such that full manual mode may be unsafe; therefore, use of the DP system is still required, but in manual control mode through the DP system. The OSV Crew may not know to activate DP system (manual) because:

a) The loss of functionality in automatic mode in unannounced and the OSV Crew does not know that automatic mode has lost functionality.
b) The DP system announces that a malfunction has occurred, but the OSV Crew does not take the alert seriously and change control modes.
c) The DP system announces that a malfunction has occurred, but the OSV Crew takes an incorrect action to resolve the problem.

Possible requirements for Scenario 33:

1. False alarms must be minimized while still keeping an adequate threshold for detection of DP system issues.
2. Alarms that require changing control modes must include this information in the feedback that is given to the OSV Crew when the alarm is activated.

Unsafe Control Action- UCA34: OSV Crew activates DP system (manual) when the OSV Crew believes that DP system (auto) has active control of the OSV. [H-1, H-2]

Scenario 34: The OSV Crew accidentally activates DP system (manual) but has an incorrect process model and believes that the DP system is controlling the OSV in automatic mode because:

a) Feedback (such as CyScan points, etc.) is displayed in the same manner regardless of the control mode that is active.
b) The OSV is not changing course so there is no external feedback to alert the crew that the control mode has changed.

Possible requirements for Scenario 34:

1. Measures must be in place to prevent the accidental changing of control modes.
2. Any time a control mode changes, there must be noticeable feedback to prevent the OSV Crew from getting mode confusion.
3. There must be multiple, independent sources of feedback, including a prominent display on all DP console screens, that depict which control mode is currently active and controlling the OSV.

Unsafe Control Action- UCA35: OSV Crew activates DP system (manual) x amount of time before beginning to exert active control of the OSV. [H-1, H-2]

Scenario 35: The OSV Crew activates DP system (manual) immediately prior to an emergency event that requires the OSV Crew's attention. In this high stress, high workload environment, the DPO delays in providing active manual control for x amount of time because they are task saturated.

Possible requirements for Scenario 35:

1. Controls should be set prior to activating DP system (manual) modes so that control is exerted immediately when the mode becomes active.
2. The first priority of the DPO must always be to control the OSV. Other members of the OSV Crew must provide assistance to the DPO in high workload situations to ensure that active control of the OSV is not delayed.

Unsafe Control Action- UCA36: OSV Crew does not deactivate DP system (manual) when full manual control of the OSV is needed. [H-1, H-2]

Scenario 36: Sensors that provide information for the DP system have multiple, independent, backup sensors to provide redundancy in case of a single failure. The DP system can still operate without the redundant backups; however, the DP system is less safe when doing so. The OSV Crew decides to continue DP system use when redundancy is lost. The OSV Crew could make this decision because:

a) The OSV Crew does not know that a given sensor no longer has redundant backups.
b) The OSV Crew decides that using the DP system without added redundancy is appropriate.

Possible requirements for Scenario 36:

1. The OSV Crew must always suspend DP system use if any component of the DP system loses redundancy where a single failure could result in the system failing.
2. Any time a sensor or system component fails, the OSV Crew must receive adequate feedback that a failure has occurred.

Unsafe Control Action- UCA37: OSV Crew deactivates DP system (manual) and activates target follow mode when activating target follow mode is unsafe. [H-1, H-2]

Scenario 37: The OSV is within x feet of the target vessel in DP system (manual) mode. Target follow mode is set to change the OSV's position relative to the target vessel too much given how close the OSV is to the target vessel. Initializing target follow mode in such a scenario could result in an excessively aggressive OSV maneuver to meet the target follow requirement.

Possible requirements for Scenario 37:

1. If the OSV is within a predetermined lateral separation distance from the target vessel, the DP system must not accept inputs to change the OSV's position relative to the target in greater than x increments.
2. If the OSV is within a predetermined lateral separation distance from the target vessel, target follow mode should not activate if excessive or previously determined unsafe

inputs are provided to the DP system. The DP system should request that the OSV Crew change the unsafe inputs to within a predetermined range before DP system (manual) mode can be deactivated.

Scenario 37a: The OSV Crew activates target follow mode when the DP system (auto) is experiencing a system failure or has limited capabilities. The OSV Crew does not know that the automatic mode had degraded and deactivates DP system (manual) to initialize target follow mode.

Possible requirements for Scenario 37a:

1. The OSV Crew must be able to test the DP system for functionality and capability prior to initializing target follow mode and deactivating the DP system (manual) mode.
2. Target follow mode should be prohibited from being activated if a system health test finds any issues with the DP system that could affect target follow mode.

Unsafe Control Action- UCA38: OSV Crew deactivates DP system (manual) and activates target follow mode before performing required prestart procedures. [H-1, H-2]

Scenario 38: The OSV Crew must match target course and speed as close as possible prior to initiating target follow mode. Furthermore, the OSV Crew must ensure that both CyScan 1 and CyScan 2 are enabled and functioning correctly on the follow sensor page prior to initializing target follow mode. The OSV Crew may forget to perform these steps or perform them incorrectly, making the deactivation of the DP system (manual) unsafe.

Possible requirements for Scenario 38:

1. The DP system must remain in manual and not initialize target follow mode if both CyScan 1 and CyScan 2 are not enabled and functioning correctly.
2. The OSV must match the target vessel course and speed within a predetermined range in order for target follow mode to be initialized.
3. There should be a readiness indicator for target follow mode to notify the OSV Crew that all required action items have been completed prior to changing the control mode.

Unsafe Control Action- UCA39: OSV Crew does not provide a DP (manual) directional command when a directional command is required to avoid contact with the target vessel, terrain, an external structure, or another vessel. [H-1.1-H-1.3]

Scenario 39: The OSV Crew does not know that a directional command is required to avoid contact with the target vessel, terrain, an external structure, or another vessel. The OSV Crew could have this flawed process model because:

a) Invalid or faulty feedback is given to the OSV Crew regarding the OSV's position relative to its surroundings.
b) The OSV Crew misinterprets available feedback that correctly indicates a directional command is needed.
c) The OSV Crew is unable to detect terrain or another vessel to know that a directional command is required to avoid contact.

Possible requirements for Scenario 39:

1. The OSV must have enough sensors to adequately detect the target vessel, terrain, external structures, and other vessels in the mission environment.
2. Independent means must be available to determine if maneuvering is required to avoid a OSV collision.

Scenario 39a: The OSV Crew gives a directional command to the OSV through the DP console; however, a hardware failure or software error results in the directional command not being provided.

Possible requirements for Scenario 39a:

1. DP system components must have a predetermined reliability to help minimize hardware failures.
2. The DP system must immediately revert to the Backup console in the event that the Master console fails. If this occurs, the OSV Crew must immediately be notified that the transition between consoles has occurred.

3. No single failure should prevent the OSV Crew from being able to provide control inputs to the OSV through the DP system.

Unsafe Control Action- UCA40: OSV Crew provides a DP (manual) directional command that could result in contact with the target vessel, terrain, an external structure, or another vessel. [H-1.1-H-1.3]

Scenario 40: The OSV Crew has a flawed process model of the operating environment and does not know that the directional command provided will result in contact with the target vessel, terrain, an external structure, or another vessel. The OSV Crew could have this flawed process model because:

a) The OSV does not have adequate water depth sensors to provide depth information to the OSV Crew.
b) CyScan information is faulty, resulting in range information to the target vessel being incorrect.
c) DGPS information is faulty, resulting in invalid feedback being given to the OSV Crew.
d) OSV sensors malfunction and/or fail, resulting in the OSV Crew not having available information that is needed for OSV operations.
e) The OSV Crew does not realize that the joystick is desensitized and that the joystick response curve is set differently than the default/anticipated joystick response curve.

Possible requirements for Scenario 40:

1. The OSV must have water depth sensors to give water depth information to the OSV Crew during operations.
2. The OSV Crew must be notified anytime a sensor malfunctions or fails to prevent confusion among the OSV Crew regarding feedback that is received.
3. Multiple sources of feedback must be present for the OSV Crew to ensure that it is known when and how much the joystick is desensitized.

Scenario 40a: The OSV is escorting the target vessel through a tight operating space, such as through a bridge crossing. A malfunction or failure forces the OSV Crew to break away from the

target vessel, but doing so results in the OSV risking contact with another vessel, terrain, or an external structure (such as a bridge).

Possible requirements for Scenario 40a:

1. Guidelines must be in place for extenuating circumstances such as what action the OSV Crew should take when ensuring the safety of the target vessel places the OSV at risk of collision with another source.
2. Breakaway procedures should be reviewed to ensure that adequate breakaway procedures exist for all operating contingencies.

Unsafe Control Action- UCA41: OSV Crew provides a DP (manual) directional command to an incorrect combination of control subsystems for a given maneuver. [H-1, H-2]

Scenario 41: The OSV Crew is operating the OSV under DP system (manual) control. There are various modes that constitute DP system (manual) control, such as transit mode, pilot mode, etc. Each mode is slightly different and uses the controls slightly differently to control the OSV. The OSV Crew could give a correct directional command for a certain manual control mode; however, the same input could provide a directional command to an incorrect combination of OSV subsystems in a different control mode.

Possible requirements for Scenario 41:

1. Feedback must be given to the OSV Crew depicting what each control mechanism is controlling given the selected control mode.
2. The control mode that is active must be readily depicted and easily located on the DP Console at all times.

Scenario 41a: The OSV Crew gives a valid control input through the DP system; however, the Thruster Allocation Logic (TAL) does not recognize that a thruster has failed and thus signals an incorrect combination of OSV control subsystems in response to the OSV Crew's directional command.

Possible requirements for Scenario 41a:

1. The DP system must be able to adjust its TAL to immediately respond to component failures.
2. The OSV Crew must be alerted if the DP system is attempting to send maneuvering commands to a control subsystem that is no longer functioning correctly.
3. If the TAL is unable to utilize available control subsystems to perform a given control input, it must be able to notify the OSV Crew and indicate that full manual control is needed.

Unsafe Control Action- UCA42: OSV Crew provides a DP (manual) directional command x seconds too late when a directional command is needed. [H-1]

Scenario 42: The OSV maneuvers too close to the target vessel for a given operation and the OSV Crew is required to perform breakaway procedures to increase the lateral separation between the target vessel and the OSV. Given the close distance between the OSV and the target vessel during escort operations, the OSV Crew may not have enough time to comprehend alarms and available information and react appropriately to prevent a collision.

Possible requirements for Scenario 42:

1. When using the DP system for control, if the OSV crosses into the predetermined safe operating envelope of the target vessel, the DP system should automatically initiate thrusters to maneuver the OSV away from the target vessel until full manual mode is activated.
2. Testing must be conducted to determine how long the OSV Crew has to react during breakaway procedures at different lateral separation distances.
3. OSV Crews must receive training to minimize their reaction time during emergency situations and to aid in their understanding of system alarms.

This material is based upon work supported by the Department of the Air Force under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Air Force.