Systems Theoretic Accident Analysis of an Offshore Supply Vessel Collision

by

John Michael Mackovjak

B.S. Systems Engineering
United States Naval 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 TECHNOLOGY AND POLICY

AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
JUNE 2016

Signature of Author: _____

Institute for Data, Systems, and Society
06 May 2016

Certified by: _____

Nancy Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Accepted by: _____

Munther Dahleh
William A. Coolidge Professor, Electrical Engineering and Computer Science
Director, Institute for Data, Systems and Society
Acting Director, Technology and Policy Program

Page intentionally left blank.

Systems Theoretic Accident Analysis of an Offshore Supply Vessel Collision

by

John Michael Mackovjak

B.S. Systems Engineering
United States Naval 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 Technology and Policy

ABSTRACT

This thesis uses Dr. Leveson's Systems-Theoretic Accident Model and Process (STAMP) model of accident causation to analyze a collision in late July 2014 between two Offshore Supply Vessels equipped with software-intensive Dynamic Positioning Systems. The Causal Analysis based on STAMP (CAST) is compared with the Root Cause Analysis, a traditional chain of events based model, used by the original investigation team after the collision. Linear chain of event models like the Root Cause Analysis often look for a broken component or incorrect action within the proximal sequence of events leading to the accident. CAST examines a system's entire safety control structure to assess why the system constraints, control loops, and process models were either inadequate or flawed. This thesis aims at identifying how the safety control structure of the Offshore Supply Vessel operations could be improved by identifying the systemic factors and component interactions that contributed to the collision.

The primary objective of this thesis is to demonstrate the use of a systems theory-based accident analysis technique in analyzing a complex accident. The secondary objective of this thesis is to compare and contrast the outcomes of the Root Cause Analysis conducted by the Navy Programs organization, with the findings of the CAST analysis. Finally, this thesis examines STAMP's underlying new assumptions regarding the need for new safety analysis in the context of the findings from the CAST analysis of the collision.

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

Page intentionally left blank.

ACKNOWLEDGEMENTS

I would first like to thank my parents, David and Maria Mackovjak, as well as my brothers, David and James who have supported me throughout my experience at MIT. I would also like to extend my deepest gratitude to all my friends who have helped me along the way. In particular, I would like to thank Taylor Moore for providing unwavering encouragement. Your enduring generosity and support meant the world to me.

Frank Field, Ed Ballo, and Barb DeLaBarre in the Technology and Policy Program were perpetually cheerful advocates throughout my time at MIT. Thank you for your positive reinforcement and valuable input.

Thank you to Lincoln Laboratory and to all those individuals who supported my research through the Military Fellowship Program. I would like to sincerely thank John Kuconis, William Ross, Lauren White, Mike Boulet and Mark Donahue for your guidance, knowledge and significant assistance in this endeavor. Thank you to the entire Navy Programs organization who provided me with repeated feedback and technical expertise on the Offshore Supply Vessel operations.

Finally, I would like to express my gratitude to Dr. Nancy Leveson and the entire Systems Engineering Research Lab who introduced me to a new and invaluable way of thinking. You have given me the opportunity to reexamine my understanding of systems engineering and system safety in a more comprehensive and analytic manner. I will take this knowledge with me to the Navy fleet and beyond.

Page intentionally left blank.

Table of Contents

Table of Figures

Table of Tables

Page intentionally left blank.

1. Introduction

In late July 2014 two Offshore Supply Vessels (OSVs) conducting software-testing operations collided. This was the third accident in a span of three months involving OSV near misses and collisions. The subsequent investigation by the Navy Programs organization overseeing the OSV operations identified a number of problems using the Root Cause Analysis and Corrective Actions (RCA&CA) technique, a common event-based analysis technique. This thesis examines the collision using a system-based approach to examine the entire sociotechnical system design to identify unsafe component interactions, weaknesses in the existing safety control structure, and systemic factors that may have contributed to the accident. This method goes beyond component failures and instead focuses on component interactions and increased understanding of why each unsafe action occurred.

The motivation for system-based causation models is described in Chapter 2. It covers traditional event chain models and the problems with using event-based accident models. The systems-approach to safety is then summarized and the STAMP fundamental assumptions are detailed. The chapter ends with an overview of the entire Causality Model based on STAMP (CAST). The full CAST analysis is performed in Chapter 3, detailing the physical and hierarchal control structure details, system background, and the proximate events leading to the accident. The chapter examines control flaws and inadequacies in each level of the control structure and generates a set of recommendations given the analysis findings. Chapter 4 compares and contrasts the findings of the CAST analysis with the RCA&CA investigation originally conducted by the Navy Programs organization. Chapter 5 provides an examination of STAMP's underlying assumptions of the need for new safety analysis in the context of the findings from the CAST analysis of the collision. The thesis concludes with Chapter 6, detailing how the Navy Programs organization may move forward with this analysis technique.

The primary objective to this thesis is to demonstrate CAST's ability to analyze a complex accident including a comprehensive review of all levels of the system's control structure. The

secondary objective of this thesis is to compare and contrast the outcomes of the Root Cause Analysis conducted by the Navy Programs organization, with the findings of the CAST analysis.

2. Motivation for System-Based Causation Models

This section delves into the fundamental differences between two causation models: event chain models and system-based models. I provide a brief review of the limitations of event chain models, followed by an overview of the new method that strives to eliminate many of these shortcomings.

2.1. Event Chain Models

Investigation teams use accident causation models in order to make sense of accidents. The choice of which model to use shapes what accident details these teams look for, how they look for those details, and what the investigation team values as relevant facts. Root Cause Analyses present accidents as a linear chain of failure events. Each failure in the chain is viewed as the direct cause of the subsequent event in the chain. The Root Cause Analysis model leads the investigation team to identify corrective actions that would block one of the failure events in the chain of events, theoretically preventing the accident from coming to fruition.

The specific guidance for the RCA&CA used by the Navy Programs organization instructs the investigation team to look for both significant and minor problems. Significant problems are those that "resulted or could result in incidents, significant unplanned cost or rework, significant environmental hazard, equipment damage or malfunction, personnel injury, spread of contamination, or defeated safeguards." Minor problems are defined as "isolated deficiencies with minimal overall impact and no significant consequences." [**1**] Once the problems are identified, the investigation team uses the 5-Whys method to guide them in determining the root causes for the problem. The team asks a series of "whys" to generate deeper levels of understanding regarding the causes of the identified problems.

2.2. Problems with Event-Based Accident Analysis

One problem with event-based accident analysis is root cause seduction. Root cause seduction stems from the belief that there is an identifiable single, or sometimes multiple, root causes that

lead to an event. [**2**] A resulting façade of control can stem from the idea that if the root causes and contributory causes near the events are identified and eliminated, then future incidents will be prevented. This can create an incentive to find a root cause in the lower safety control structure where changes can be easily identified and eliminated, avoiding management or systemic causes that may be disruptive or costly to an organization. When multiple causes are identified, particular types are given more focus than others, normally based on how well they are understood. Root cause seduction often leads to low level physical design characteristics and low-level operator actions as the identified root cause.

Another problem with the traditional event chain model is the improper valuation and identification of problems associated with the loss. Focusing on an event, or surrounding contributory causes near the event that may trigger a loss, makes it difficult to identify the causal factors that may not be readily apparent in the event chain. The underpinning conditions for the event to occur may have been laid months or years before. Furthermore, possible problems identified in the investigation that do not directly fit within the event chain may be dismissed or ignored. The mere act of viewing an accident as a chain of events may limit comprehensive understanding of the loss.

Trust and dependence on immediately available solutions can become a convenient trap because short-term solutions are used to fix or add symbolic value to the problems identified. This trap can influence an investigator to fail to address systemic fundamental causes behind the accident. In contrast, as Leveson repeatedly emphasizes, "to effect high-leverage policies and changes that are able to prevent large classes of future losses, the weaknesses in the entire safety control structure related to the loss need to be identified and the control structure redesigned to be more effective." [**3**] A continual learning and improvement culture must stem from high-level leadership in management, and potentially requires organizational changes beyond the scope of event chain models of causality.

Traditional safety engineering and accident analysis techniques like Root Cause Analysis are stretched further by new changes in technology, society, and types of hazards that were not

apparent when the techniques were developed. Dr. Leveson provides several examples that are particularly relevant to the OSV collision [**3**]:

- **Changing nature of accidents:** Many methods of preventing accidents that previously worked on electromechanical components are now rendered ineffective in managing those that arise from the use of new digital systems.
- **Difficulty in selecting priorities and making tradeoffs**: Rising costs, budget limitations and increasingly competitive environments force many government agencies to factor productivity and cost into their short-term safety decisions.
- **Decreasing tolerance for single accidents:** In an increasingly interdependent global economy, every accident has a major impact in regards to financial and environmental losses. While it is important to learn from these accidents, more insistence is needed on preventing the occurrence in the first place.
- **Increasing complexity and coupling:** Increased complexity within today's systems makes it challenging for systems designers to account for all possible states as well as for operators to manage all possible situations and disturbances effectively.
- **More complex relationships between humans and automation:** The implementation of higher-level decision making with automation has led to the miscommunication between humans and machines becoming a progressively important factor in accidents.

Traditional causation models are limited by their underlying assumptions about safety. Event chain models assume it is possible to explain system behavior as a series of linear events over time. However, organizational factors, inadequate system controls, and indirect effects often play prominent roles in the loss and must be analyzed to fully understand the accident. Dr. Leveson rewrote the safety assumptions, as shown in Table 1, which were necessary to develop a new accident causation model founded in systems theory. [**3**]

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chain of events leading to the loss.	Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly.	Operator behavior is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability or reducing implementation errors will have little impact of safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behavior as a whole contributed to the loss and not on who or what to blame for it.

Table 1: Comparing Traditional Causation Model and STAMP Model Assumptions

These new assumptions allow the safety model to look beyond the traditionally narrow focus of physical component failures and operator errors. The whole concept of a root cause is reconsidered with an accident model that encourages a broader view of accident causality that leads the investigation beyond the immediate events preceding the loss.

2.3. Systems Approach to Safety

The traditional event chain model of causality fails to encompass many of the complexities needed to understand and manage today's engineered systems. Nevertheless, many of the event chain approach's limitations can be avoided by using a system-based approach. The most common past accident causation models assume that accidents are the result of component failure, whereas systems-based approaches strive to understand the interactions between system components. Systems achieve their emergent properties, like safety, through these component interactions. As an emergent property, safety can only be determined and evaluated accurately within the context of the whole. Component interactions may produce one outcome in a particular environment and an entirely different outcome within another. Therefore, safety depends on the enforcement of limitations on the behavior of the components in the system and must be constantly reevaluated based off of these changing interactions.

2.4. STAMP Overview

STAMP approaches accidents as complex dynamic processes, not just a chain of events that leads to a loss. By treating an accident as a control problem, rather than just a failure problem, system designers can help prevent accidents by creating constraints on enforceable component behavior and interactions, taking into account the nuances of the environment that surround the system. The STAMP model helps encompass a range of accident factors, including component failures, unsafe interactions among components, design errors, flawed requirements (particularly prevalent in software-related accidents), and complex human behavior. There are three main concepts that lay the foundation for STAMP: safety constraints, a hierarchical safety control structure, and process models.

2.4.1. Safety Constraints

Safety constraints are acceptable ways for a system or organization to achieve its mission goals. Properly enforced safety constraints prevent a system from entering a potentially unsafe state. These safety constraints are important in the STAMP model because the improper or lack of enforcement of constraints allow an unsafe set of conditions to occur leading to the accident. An example of a safety constraint relevant for a ship transiting though a channel could be: *the ship*

must not violate minimum separation distance from other surrounding vessels. While the violations of minimum separation distance may not directly cause a collision, the violation of the safety constraint allow a hazardous state to exist where an accident may occur.

2.4.2. Hierarchical Safety Control Structure

STAMP views systems as hierarchical structures where "each level imposes constraints on the activity of the level beneath it – that is, constraints or lack of constraints at a higher level allow or control lower level behavior." [**3**] A hierarchical safety control structure can range in complexity depending on the system. System theory allows for abstraction and concentration on different levels and parts of the system. This leads to better understanding of what controls are necessary to mitigate system hazards. Only the relevant subset of the overall safety control structure may be needed in examining these hazards. An example safety control structure for a ship transiting a channel is shown in Figure 1:

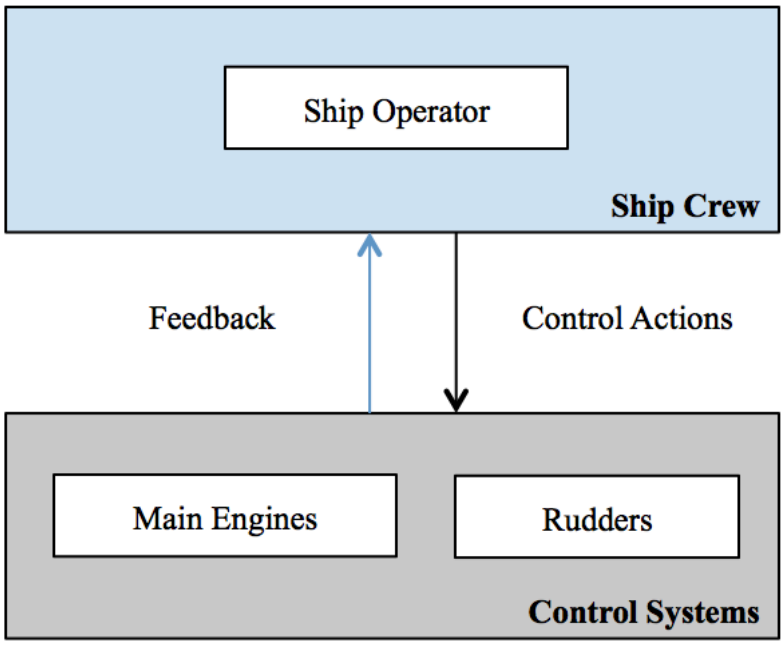

Figure 1: Example Safety Control Structure

The example safety control structure in Figure 1 is the model of the ship operator and the control systems controlling the ship movement. In this case, the control systems consist of the main engines and the rudders. Between the ship crew and control systems are the control processes that enforce safety constraints. The arrow from the ship operator to the control systems

represents control actions by the ship operator. The control actions are the ship operator's inputted commands to the main engines and rudders. The arrow from the control systems to the ship operator is the feedback channel. This channel provides feedback on how effectively the control commands and constraints are being satisfied. Possible feedback could be the engine state, the speed of the craft, or the rudder angle.

Accidents occur when safety constraints are violated by the lower-level components due to unsafe control imposed by the higher-levels. Unsafe control may result from missing constraints (unassigned responsibility for safety), unsafe control commands, safe commands that were not executed correctly at a lower level, or inadequately communicated or processed feedback about constraint enforcement. [**3**] Unsafe control may occur at each level of the hierarchical control structure, so control structures must be in place to enforce constraints at all levels. For example, a ship operator would be unable to enforce a safety constraint, like maintaining a minimum lateral separation from another vessel, if the ship operator was unaware of the constraint. A hazardous state could also occur if the ship operator did not believe it was his or her duty to enforce the separation constraint. Unsafe control may occur at each level of the hierarchical control structure, so control structures must be in place to enforce constraints at all levels.

The system control structure is particularly powerful due to its flexibility. As shown in Figure 2, the safety control structure can be expanded to better examine a system and determine the reason for any unsafe control actions.

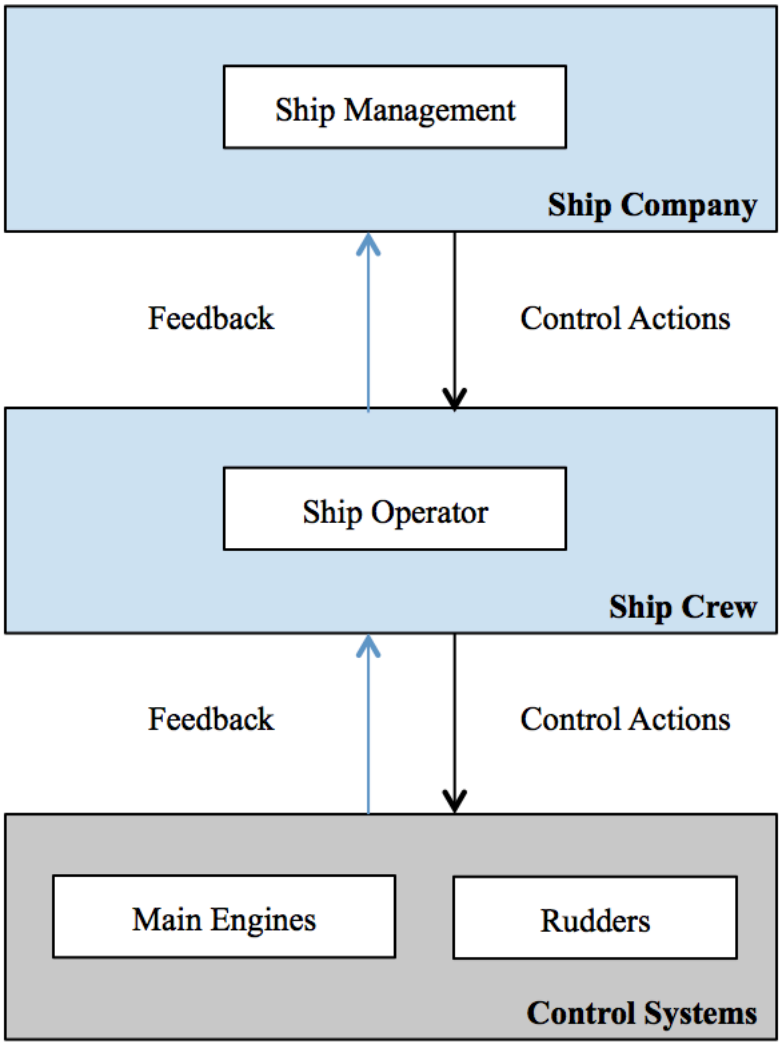

Figure 2: Expanded Example Safety Control Structure

As shown in the expanded example safety control structure, the ship operator both enforces and receives constraints. Ship management sends goals, policies, constraints, and control commands to the ship operator, and the operator sends back feedback to the ship company from operational experience. Without proper information through the control channel between ship management and the ship operator, it is impossible to impose safety constraints on the lower levels in the control structure to mitigate hazards. Without proper feedback from the ship operator to ship management, there is no way for the ship manager to know how effectively the imposed constraints are satisfied. It is important to note, hazards must first be identified at the system level, and then the safety constraints can be identified and processed from the top of the control structure down through the different control levels.

2.4.3. Process Models

All controllers in a system must contain a model of the process being controlled. The four conditions necessary to control a process within the hierarchical safety control structure are: the safety constraints enforced by each controller within the system, the downward control channels, the upward feedback channels, and the model of the process being controlled. The STAMP model asserts all controllers, whether they are automated controllers or human controllers, must understand the same type of information to effectively control a process: "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." [**3**] The process model provides the controller with an understanding of what inputs are needed to safely control the process given the available information about the controlled process. Accidents often occur when the process model of the controlled process does not match the actual process's current state. The mismatch of either the human's mental model or the automation's model of the controlled process leads to four types of hazardous control actions [**3**]:

1. Control actions are given that lead to a hazard.
2. Control actions required for safety are not provided.
3. Potentially correct control commands provided at the wrong time (too early or too late) lead to a hazard.
4. Control stopped too soon or applied too long leads to a hazard.

These four types of unsafe control actions apply to all levels of the hierarchical safety control structure. Understanding the safety constraints, control structure, and process models of controllers leading to the accident allows the system-based causal analysis to recommend changes that can make the system safer for future operations.

2.5. CAST Steps Overview

CAST contains nine steps, with the first three steps being the same ones used for all STAMP based techniques as outlined in Leveson's *Engineering a Safer World*. A goal of CAST is to avoid assigning blame on any single controller or causal factor, and instead to focus on why the accident occurred. Approaching accident analysis in this way aids an investigation team to

recommend changes that may eliminate causal and systemic factors, rather than simply fixating on eliminating symptoms. The nine steps of CAST are [**3**]:

1. Identify the system(s) and hazard(s) involved with the loss.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this. This structure may be completed in parallel with the later steps.
4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level. Identify the contribution of the following to the events: physical and operational controls, physical failures, unsafe interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure, determine how and ***why*** each successive higher level allowed or contributed to the unsafe control at the current level.
    a. For each system safety constraint, either the responsibility for enforcing it was never assigned to a component in the safety control structure or a component or components did not exercise adequate control to ensure their assigned responsibilities (safety constraints) were enforced in the components below them.
    b. Any human decisions or flawed control actions need to be understood in terms of (at least): the information available to the decision maker as well as any required information that was *not* available, the behavior-shaping mechanism (the context and influences on the decision-making process), the value structures underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.
7. Examine overall coordination and communication contributors to the loss.

8. Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9. Generate recommendations.

CAST is not designed to be a linear process. These steps provide a guideline for understanding the dynamic process that led a system to an accident.

3. CAST Analysis

3.1. Accident Background

The United States Navy began contracting Offshore Supply Vessels (OSVs) in 2006 to serve as escort vessels for U.S. Navy Vessels transiting in and out of port. [**4**] The aptly labeled *target-follow operations* involve the OSVs following on either side of the U.S. Navy Vessel. OSVs were originally designed and constructed to serve in deep-water oil operations and other complex drilling projects, however, they were repurposed in 2009 to meet the Navy Program's specifications for escort mission. One main reason the U.S. Navy turned to OSVs was their integration of Class 2 Dynamic Positioning (DP) Systems, enabling the OSVs to use automated lateral separation control during target-follow operations. The Class 2 DP System facilitates the OSVs in precisely maintaining a constant lateral separation with the U.S. Navy Vessel through the variety of maneuvers necessary to transit in and out of port. When an OSV is in Target-Follow Mode, the DP System takes full control of the OSV actuators and completes the maneuvers with no human input.

Each OSV is equipped with the following principal features [**5**]:

- Automatic heading control
- Automatic position control
- Fully redundant control system
- Noise Rejection Logic (NRL) Filter
- Transit Mode (DP System assisted manual mode)

- Target-Follow Mode (DP System in full automatic mode)
- Triple redundant Reference Sensor Systems (RSS)

The Class 2 DP System contains two redundant DP System control computers and a sensor package to feed the vessel's position, heading, and attitude. The position reference sensors consist of DGPS, Hydro-Acoustic Systems, and Laser Radar. The Environmental Sensors consist of Wind Sensors, Gyrocompasses, Vertical Reference Sensors, and a Current Estimator. An example Class 2 DP System is shown in Figure 3 [**6**].

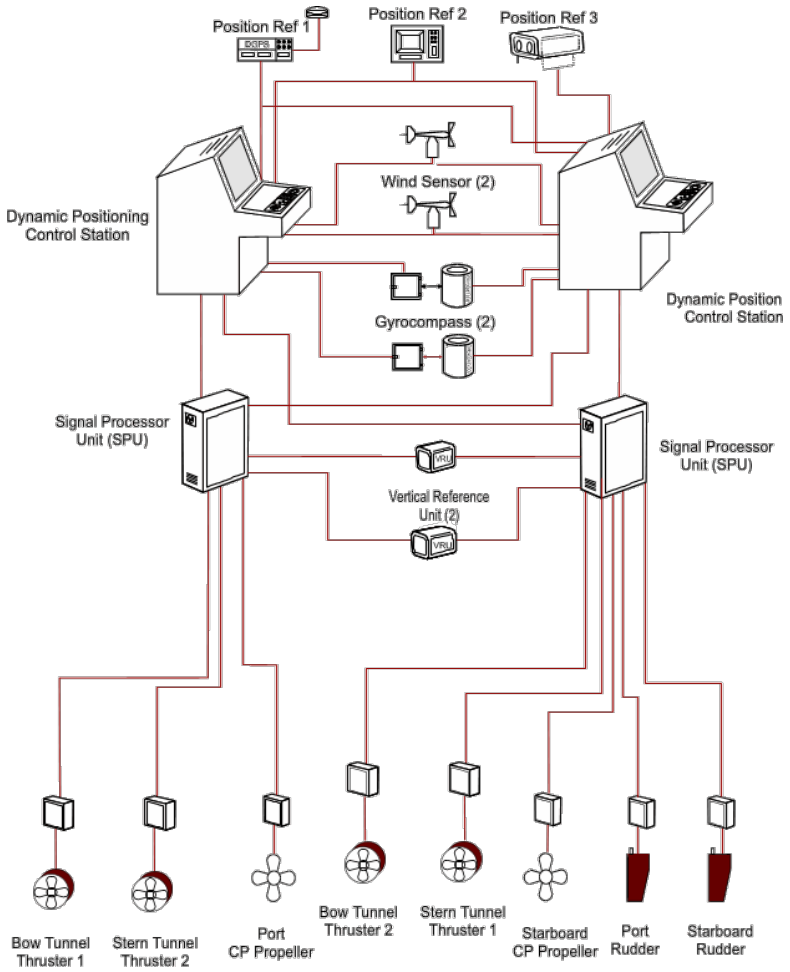

Figure 3: Example of a Class 2 Dynamic Positioning System

The DP System uses a Reference Sensor System (RSS) with a built-in redundancy to communicate accurate heading and position information to the DP System in order to calculate

the relative position of the OSV to the target vessel. The DP System inputs the RSS data and Environmental Sensor data to the DP Control Algorithm to output control commands to the OSV control subsystems. The control subsystems entail tunnel thrusters, rudders, bow rotors, and main engines. An overview of the system control loop controlling the OSV movement is shown in Figure 4:

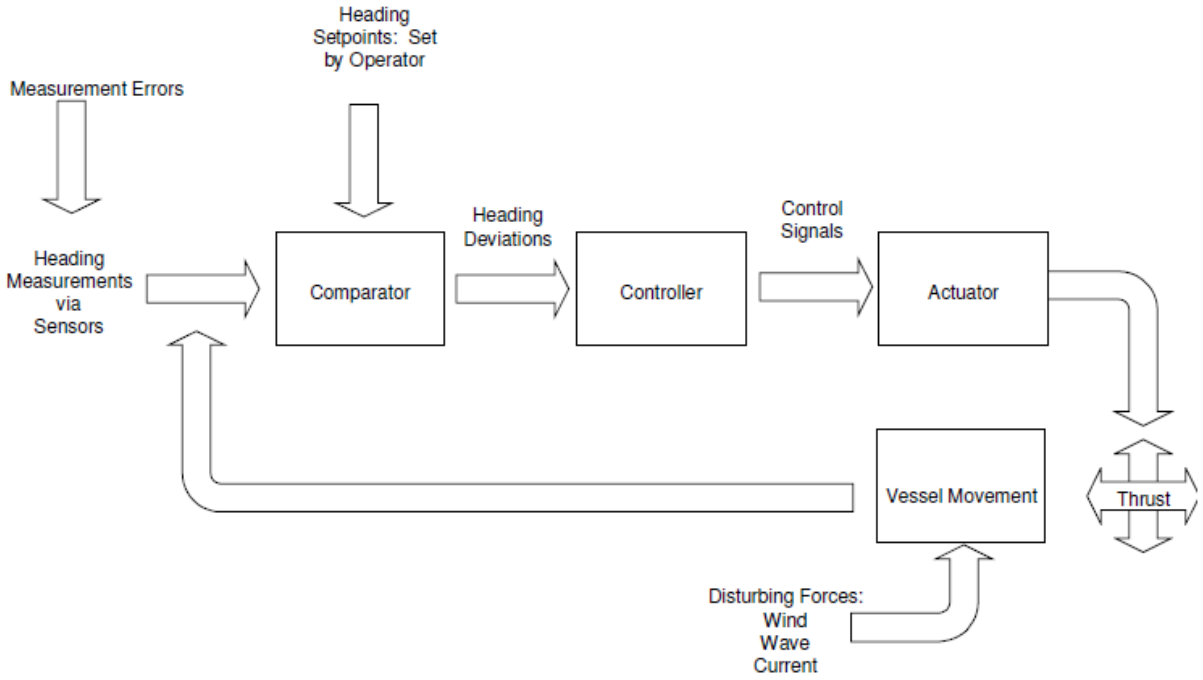

Figure 4: Offshore Supply Vessel Dynamic Positioning Control Loop [5]

In the event that all reference sensors fail while the DP System is in automatic Target-Follow Mode, the OSV switches to a supplementary automatic mode called Dead Reckoning Mode. The DP System switches, with no operator input, to Dead Reckoning Mode upon loss of all RSS data. Dead Reckoning Mode is designed to be a temporary backup mode that estimates the OSV's relative position and speed from the target vessel based on available wind sensor input, past position, past rates, and a Kalman vessel model. Dead Reckoning Mode enables the OSV to continue automatic operations rather than forcing the DP Operator to immediately switch to Full Manual Mode. However, Dead Reckoning Mode is an uncommon occurrence during normal operations. The DP System will remain in Dead Reckoning Mode until RSS data is recovered or the DP Operator switches to DP Manual Mode or Full Manual Mode.

3.1.1. OSV Tuning Operations

OSVs must conduct operations outside their normal duties as U.S. Navy escort vessels. In particular, OSVs conduct testing operations whenever there are software updates to the DP System. During software tuning and testing events, a Target OSV functionally takes the place of the U.S. Navy Vessel. The Target OSV acts as the stand-on vessel and simulates maneuvers the U.S. Navy Vessel would normally make. The other OSV used for testing and tuning operations is the Follow OSV. The Follow OSV operates alongside the Target OSV, and has the duty of maintaining a preset lateral distance from the Target OSV. In the event that the minimum lateral separation is lost, it is the responsibility of the Follow OSV, not the Target OSV, to regain the lateral separation.

The main purpose for test events is to collect a comprehensive set of software parameter test data. From these test data sets, the optimal parameters are determined and then the updated software is installed and used for normal OSV escort operations. During normal operations, the OSV Crew typically only encompasses the Dynamic Positioning Operator(s), OSV Master(s), and OSV Bridge Officer(s). However, during testing operations, there is also a Software Engineer, a System Analyst, and a Test Director in addition to the normal crew. The Test Director is in charge of all testing events, the Software Engineer is in charge of changing the DP System software parameters, and the System Analyst collects testing data. It should be noted, all Dynamic Positioning (DP) Operators are OSV Bridge Officers. The DP Operator is the individual who is in charge of entering control commands to the DP System and OSV manual controls. There are normally three to six OSV Bridge Officers per OSV, and the OSV Bridge Officer holding DP Operator position may switch with any other DP System-qualified OSV Bridge Officer.

The goal of the late July 2014 testing event was to test a range of parameters on a recently updated Noise Rejection Logic (NRL) Filter with the addition of heading measurements. Two previous OSV operating incidents, one near miss and one minor collision, occurred within five months of the late July 2014 accident and were the catalyst for the NRL Filter software update.

3.1.2. OSV Accident #1

On 26 March 2014 the Follow OSV, providing escort services for a U.S. Navy Vessel, violated minimum lateral separation. The Follow OSV's reference sensor picked up false reflections on a vessel opposite of the U.S. Navy Vessel and delivered the incorrect data to the DP System. This resulted in the DP System commanding the OSV rudders, rotors, and tunnel thrusters towards the U.S. Navy Vessel, resulting in a breakaway and a near miss event. At the time of the near miss, the Follow OSV DP System did not have a NRL Filter to prevent erroneous target heading data.

The Root Cause Analysis and Corrective Actions conducted after the accident identified thirteen specific problems, however the report indicated, "two significant problems directly led to the near miss incident and rise above the others with respect to importance/severity." Those problems were [**7**]:

- The reference sensor on the Follow OSV delivered incorrect data to the Dynamic Positioning System.
- There was no Noise Rejection Logic filter in the DP System to prevent the DP System from using erroneous target heading data provided by the reference sensor.

3.1.3. OSV Accident #2

On 4 June 2014 the Follow OSV, conducting OSV/OSV test-follow operations for recertification, had a minor collision with the Target OSV. During a starboard turn, the Follow OSV reference sensor delivered an erroneous heading error to the DP System. The DP System subsequently ordered control surfaces, thrusters, and engine changes resulting in unplanned closure to the Target OSV. The Target OSV initiated an aggressive breakaway resulting in the stern of the Target OSV colliding with the Follow OSV.

The Root Cause Analysis and Corrective Actions conducted after the accident identified ten specific problems, however the report indicated, "two significant problems directly led to the near miss incident and rise above the others with respect to importance/severity." Those problems were [**8**]:

- The reference sensor on the Follow OSV delivered incorrect data to the Dynamic Positioning System.
- There was no Noise Rejection Logic filter in the DP System to prevent the DP System from using erroneous target heading data.

Similar to the previous 26 March 2014 accident, there was no NRL Filter in the DP System to prevent the use of erroneous target heading data. While there was a corrective action to modify the NRL Filter after the previous near miss that would include the target vessel heading, the modification had not been completed.

3.2. OSV / OSV Collision

In late July 2014 two OSVs collided while conducting a DP software tuning procedure. The OSV tuning operation was in place to determine the optimal software parameters required to employ a recently enhanced NRL Filter. The software update was implemented to mitigate target-heading errors related to the two previous OSV accidents.

The accident occurred during a target-follow turning maneuver between Target OSV and Follow OSV. Target OSV was in Hold Heading mode, acting as the stand-on vessel. Follow OSV was in automatic Target-Follow Mode with the DP System in control, and was supposed to automatically follow Target OSV at a preset lateral distance. The accident occurred during Test Event #18 and involved Target OSV initiating a port turn, with Target OSV as the inside vessel and Follow OSV as the outside vessel. While conducting the port turn, the Follow OSV's DP System automatically switched from Target-Follow Mode to Dead Reckoning Mode due to a rejection of all Reference Sensor System inputs from the NRL Filter software. The Follow OSV's DP Operator switched to Full Manual Mode and initiated the breakaway procedure. However, Follow OSV continued closure during the breakaway and Follow OSV's bow collided with Target OSV's starboard quarter below the waterline. A visual presentation of the accident is shown in Figure 5, where Alpha is the Target OSV and Echo is the Follow OSV.

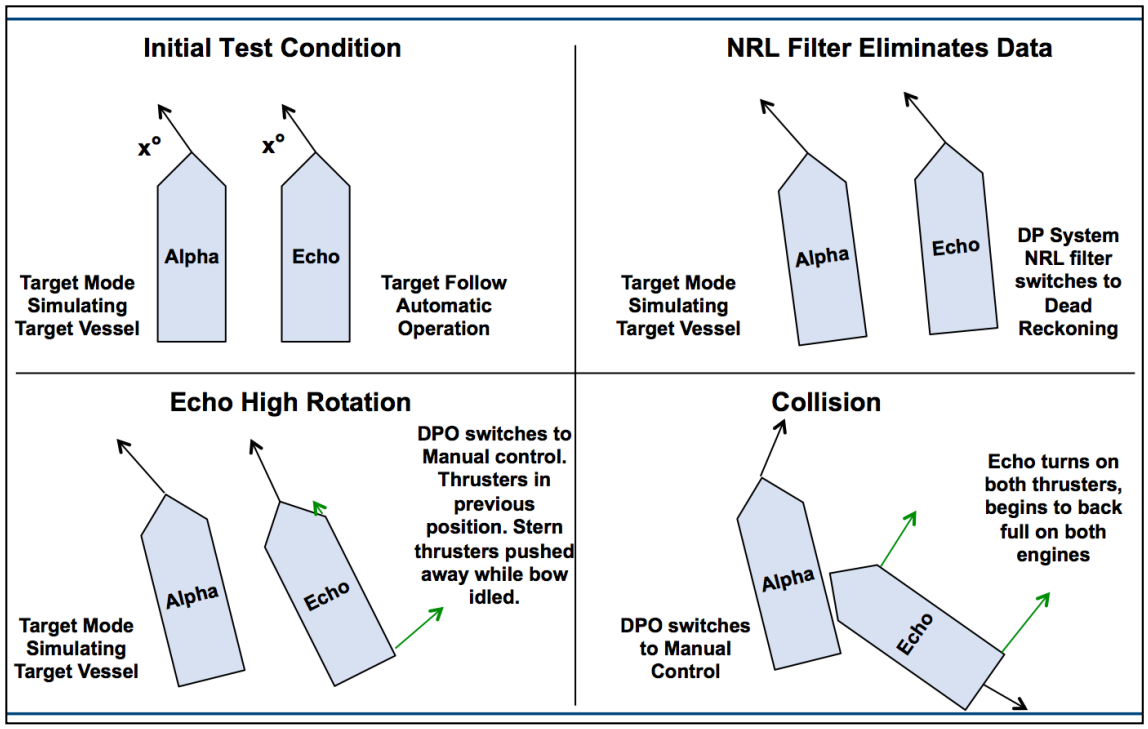

Figure 5: Visual representation of July 2014 OSV accident

Testing was immediately terminated and initial damage assessments took place. Follow OSV's damage assessment included a minor dent approximately two square feet on the bow and minor paint scratches. Target OSV's damage assessment included fendering near the point of impact pushed down by approximately two inches. Target OSV also had several fendering bolts misaligned. The United States Coast Guard (USCG) and the American Bureau of Shipping (ABS) cleared both vessels for all operations at sea after inspections in port. The DP System testing software installed for the tuning operation was replaced with the operational software that was currently being used in normal operations. The severity of this incident was assessed as "critical," and an immediate notification was sent to all stakeholder organizations.

A stakeholder team was formed after the accident to conduct a Root Cause Analysis and Corrective Action (RCA&CA) in order to identify and implement immediate corrective actions, as well as identify short and long term corrective actions. All future NRL Filter tuning operations were put on hold until immediate and short-term corrective actions were identified and completed.

3.2.1. Chain of Events

According to the RCA&CA report, data retrieved from the onboard Data Logger detailed the chain of events:

- **18:51:35** – Target OSV begins turn #18 of NRL Filter tuning procedure (port 45° turn, [x] feet lateral separation, 25 degrees/minute, 12-13 knots)
- **18:52:05** – Follow OSV Dynamic Positioning System's NRL Filter eliminates data from available Reference Sensor Systems and begins Dead Reckoning. Dead Reckoning slightly decreases port commands on control surfaces
- **18:52:14** – Follow OSV's Dynamic Positioning Officer switches into manual control, Follow OSV has high rotation to port, Follow OSV stern at 111 ft. lateral separation, Follow OSV Vessel bow at 116 ft. lateral separation
- **18:52:16** – Follow OSV's rudder at 2° to starboard, oscillates a little throughout incident, stays at less than 2.5°
- **18:52:18** – Follow OSV's aft thruster ramps up and then down for 7 seconds pushing away from Target OSV
- **18:52:24** – Actual loss of RSS #1 data
- **18:52:31** – Follow OSV forward and aft thrusters begin to push away from Target OSV
- **18:52:33** – Actual loss of RSS #2 data
- **18:52:36** – Actual loss of RSS #2 data
- **18:52:42** – Target OSV's Dynamic Positioning Officer switches into manual control, commands shift rudder to starboard
- **18:52:44** – Follow OSV's Main Engine feedback reaches 0, begins backing bell
- **18:52:46** – Contact between vessels
- **18:52:50** – Maximum rudder on the Target OSV of 30° starboard
- **18:53:07** – Follow OSV's Main Engine feedback reaches maximum backing bell

The events are further analyzed in Section 3.6 Proximate Events Leading to the Loss.

3.3. System Definitions and Hazards

3.3.1. System Definition

The first step in the CAST analysis is to identify the systems and hazards involved in the loss. The system being analyzed is the Offshore Supply Vessels (OSV) utilizing Class 2 Dynamic Positioning (DP) systems conducting tuning and testing operations.

3.3.2. System Hazard

As defined in Leveson's *Engineering a Safer World,* an accident is defined as "an undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on)." [**3**] For OSV tuning and testing operations there are three main types of accidents that must be prevented:

A-1. **Humans or equipment on OSV Vessels are injured or damaged.**

A-2. Humans or equipment on any surrounding craft are injured or damaged.

A-3. The scientific data corresponding to the mission goals is not collected or rendered unusable (i.e., deleted or corrupted) before it can be fully investigated.

For this CAST analysis, **A-1**: *Humans or equipment on OSV Vessels are injured or damaged,* will be the focus of the investigation. It should be noted that rather than scoping this accident as *humans or equipment on the Offshore Supply Vessels are injured or damaged*, one could frame the accident as *the scientific data corresponding to the mission goals is not collected or rendered unusable (i.e., deleted or corrupted) before it can be fully investigated.* By viewing the system goal as the collection of relevant test data, a different set of hazards would be defined to understand this loss. This analysis will focus on the former accident scope, and the data collection loss is covered within the analysis.

This accident occurred because hazardous conditions were permitted to exist. CAST defines a hazard as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)." [**3**] The two hazardous conditions states that existed and allowed the accident to occur were:

H-1. OSV Follow violates minimum separation standard with Target OSV.

H-2. OSV Operators lose control of Follow OSV Vessel.

3.4. System Safety Constraints and System Requirements

System safety constraints and requirements use controls to prevent system hazards from occurring. Physical design, processes, humans, automation, and/or social control can enforce these constraints. Properly enforcing the system safety constraints is key in preventing hazards and potential accidents from occurring.

3.4.1. System Safety Constraints

Table 2 outlines the high-level safety constraints that must be enforced to address each hazard:

	System Hazards	**System Requirements/Constraints**
H-1	OSV Follow violates minimum separation standard with OSV Target.	OSV Follow must not violate minimum separation standard with OSV Target.
H-2	OSV Crew loses control of OSV Vessel.	OSV Crew must not lose control of OSV Vessel. DP System must notify OSV operators when OSV is in hazardous state of control.

Table 2: System Hazards and System Requirements

3.5. Hierarchical Safety Control Structures

CAST uses hierarchical safety control structures to analyze how the system safety constraints and system requirements are imposed and enforced. The following sections abstract the system in three varying levels of control structures: Organizational Safety Control Structure, Functional Control Structure, and OSV/OSV Testing Safety Control Structure.

3.5.1. Organizational Safety Control Structure

It is important to examine and understand where the physical OSV system fits within the overall hierarchical control structure. Figure 6 shows the high level Organizational Safety Control Structure for OSV testing operations.

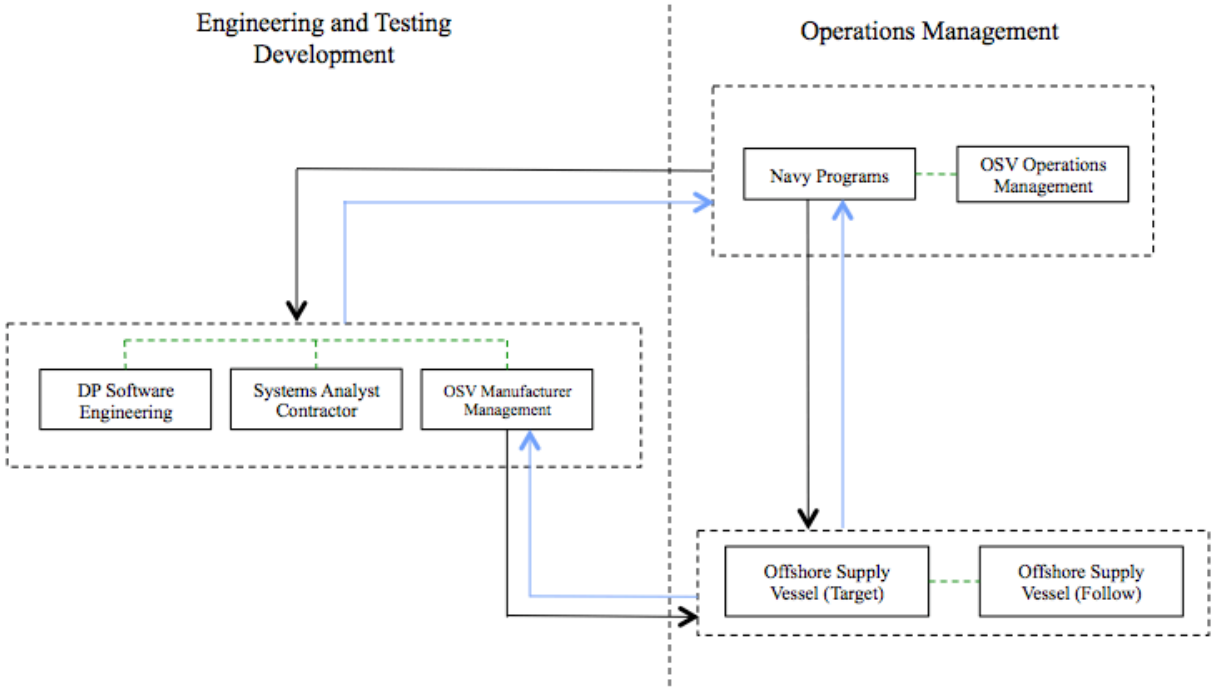

Figure 6: OSV Testing Organizational Safety Control Structure

The system is separated between the Engineering and Testing Development controllers and the Operations Management controllers. The Engineering Testing and Development controllers consist of DP Software Engineering, System Analyst Contractors, and OSV Manufacturer Management. The system goal of the Engineering Testing and Development controllers, with respect to tuning and testing operations, is to develop safe systems and provide the Operations Management controllers with operating requirements, test plans, and testing procedures necessary to conduct safe operations.

- ***DP Software Engineering***: This organization is responsible for providing the physical and software components for the DP Systems utilized by the OSVs for automatic target follow operations. DP Software Engineering is contracted to work with the OSV

Manufacturing Management to integrate the automation and control systems, as well as work with the Operations Management controllers to provide the specific NRL Filter parameter test sequences used in the testing and tuning operations.

- ***Systems Analyst Contractors***: This organization is responsible for providing systems design and engineering, logistics support, and systems program planning to the Engineering Testing and Development controllers. For this operation, the Systems Analyst Contractors hold a direct contract with Navy Programs. The Systems Analyst Contractors were founded primarily to support Navy Programs, with the mission of providing timely and objective assessments of technical, operational, and policy issues involved with OSV operations.
- ***OSV Manufacturer Management***: This organization holds a contract with Navy Programs to produce the OSV and provide the trained and certified crew to operate the vessels. The OSV Manufacturer Management have the primary responsibility to ensure their crew is trained on the DP Systems, are up to date on their U.S. Coast Guard certification and health certification, and understand the operating procedures and guidelines of the OSVs for this specific operation. The OSV Manufacturer Management also handles all OSV repairs and has an independent incident report system. The Safe Operations Manual is the overall guidance provided to the OSV Crew on how to conduct general operations. This guidance is independent from the Operations Management documentation that is for specific test events.

The Operations Management controllers consist of Navy Programs and OSV Operations Management. The system goal of the Operations Management controllers is to ensure all operating requirements, test plans, and test procedures are safe and ready for use in operations.

- ***Navy Programs***: This organization has overall responsibility for the safety of all OSVs in all operations. Navy Programs coordinates with OSV Operations Management to approve and provide the test documentation used by the OSV Crew during testing operations. Navy Programs hold contracts with Systems Analyst Contractors and OSV Manufacturing Management to provide all the necessary analysis, equipment, and

manpower necessary to conduct safe OSV operations. Navy Programs is also responsible for conducting and coordinating accident analysis of any incidents involving OSV operations.

- ***OSV Operations Management:*** This organization coordinates with Navy Programs to provide guidance, checklists and procedures to the OSVs for testing operations. OSV Operations Management ensures the fulfillment of contractual obligations with Navy Programs, in part, by overseeing all testing specific guidance the OSV Crew uses in software update operations.

Figure 7 illustrates the hierarchical structure of documentation prepared by Engineering and Testing Development, approved by Operations Management, and directed to OSVs for testing operations. The red (small-dashed) arrows indicate which document each controller on the left prepared. The blue (large-dashed) arrows indicate which document each controller on the right approved for use. The green (solid) arrows point to which documentation each document references. For example, the Target OSV – Follow OSV Test Plan was prepared by the Contracted Systems Analyst and was approved by Navy Programs and OSV Operations Management. The test plan references the Target-Follow Software Tuning and Testing Procedures.

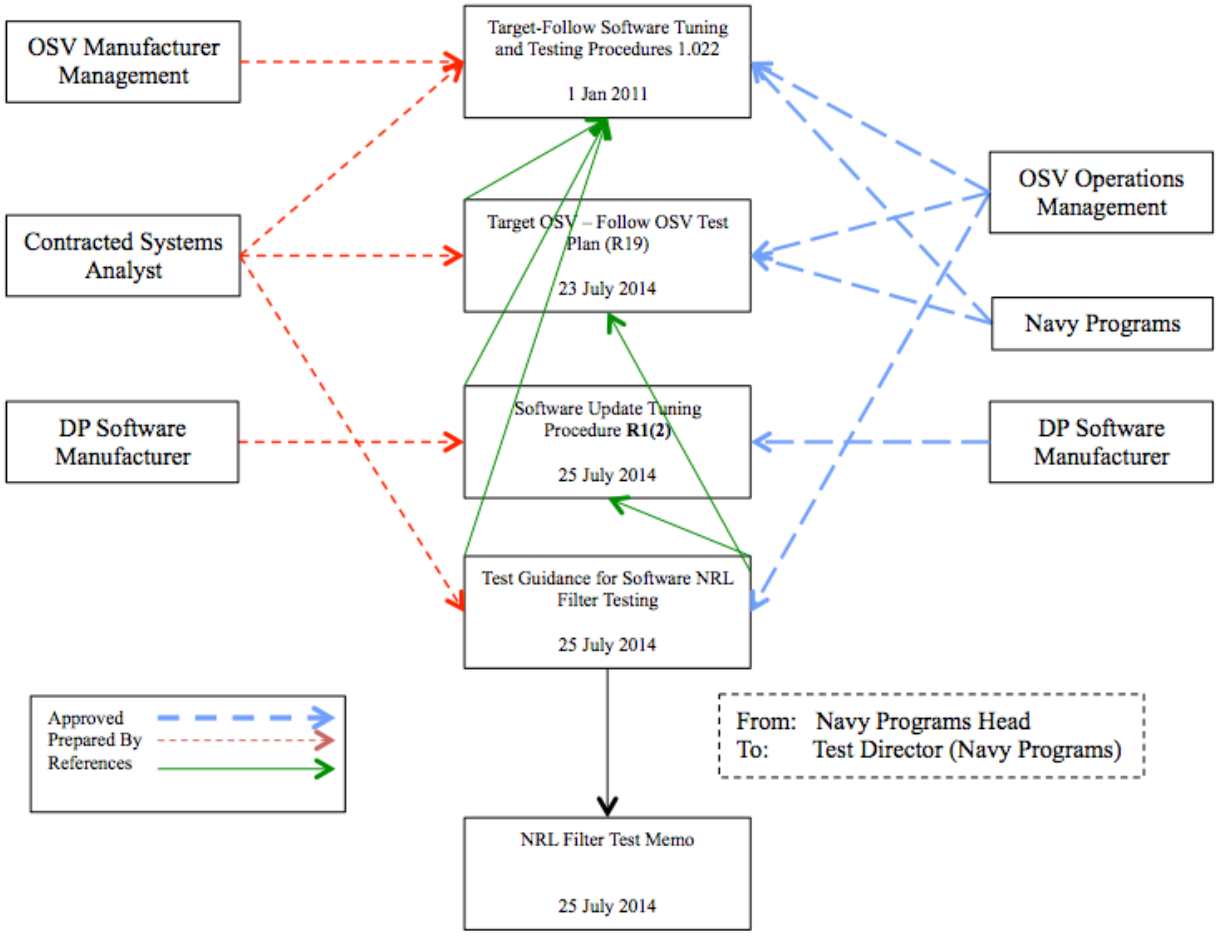

Figure 7: Traceable Documentation for OSV Test Operations

The following test documents were approved by Navy Programs and sent to the OSV crew prior to the late July 2014 test event:

- *Target – Follow Software Tuning and Testing Procedures 1.022:* The OSV Manufacturer and Contracted Systems Analyst prepare these testing procedures, and Navy Programs and OSV Operations Management approve them. These procedures were approved in January 2011. The testing procedures provide information and instructions for conducting any operations that involve an OSV that simulates a U.S. Navy Vessel for software tuning purposes. Responsibilities for the Test Director, OSV Crew, and OSV Technical Team are listed here. The testing procedures are nested within the main OSV Operations Manual Rev4, which is an array of instructions meant to govern all OSV operations.

- *Target OSV – Follow OSV Test Plan (Revision 19):* The Contracted Systems Analyst prepared this test plan, and OSV Operations Management and Navy Programs approved it. The test plan was approved on 23 July 2014. The test plan provides information and instructions for conducting OSV testing with the purpose of assessing the ability of the system with the updated software package. This Target OSV – Follow OSV Test Plan assigns responsibility and provides instructions for the Test Director, OSV Follow Master, OSV Target Master. It also includes the breakaway criteria and was recently updated to include specific revisions from the 3 June 2014 accident. This is an overarching procedure that is used for all Target OSV – Follow OSV test assessments, so it provides only example testing matrixes rather than specific tuning procedures.
- *Software Update Tuning Procedures (Revision 1 / 2):* The DP Software Manufacture prepared and approved these tuning. It was approved as Revision 1 on 14 July 2014; however, the Test Guidance for Software NRL Filter Testing referenced it as Revision 2 for Software Filter Testing with an approval date of 25 July 2014. The tuning procedures give the specific test matrix and calibration parameters for the proposed test sequence. The test matrix is shown in Table 3.
- *Test Guidance for Software NRL Filter Testing:* The Contracted System Analyst prepared the test guidance and the OSV Operations Management approved it. The test guidance was approved on 25 July 2014. The test guidance assigns specific individuals to perform the duties as Test Director, System Analyst, and Software Engineer. The specific names, dates, and procedures for the testing event are provided. It also assigns specific safety related responsibilities to the OSV Crew for the late July 2014 test event.
- *NRL Filter Test Memo:* The NRL Filter Test Memo is the final test document and it is sent from the Navy Programs Head to the Test Director assigned to the late July 2014 test event. The Test Memo encloses all other documentation and officially approves them for use during the test event.

3.5.2. Functional Control Structure

The Functional Control Structure in Figure 8 illustrates the relationship between the DP Operator and the DP System.

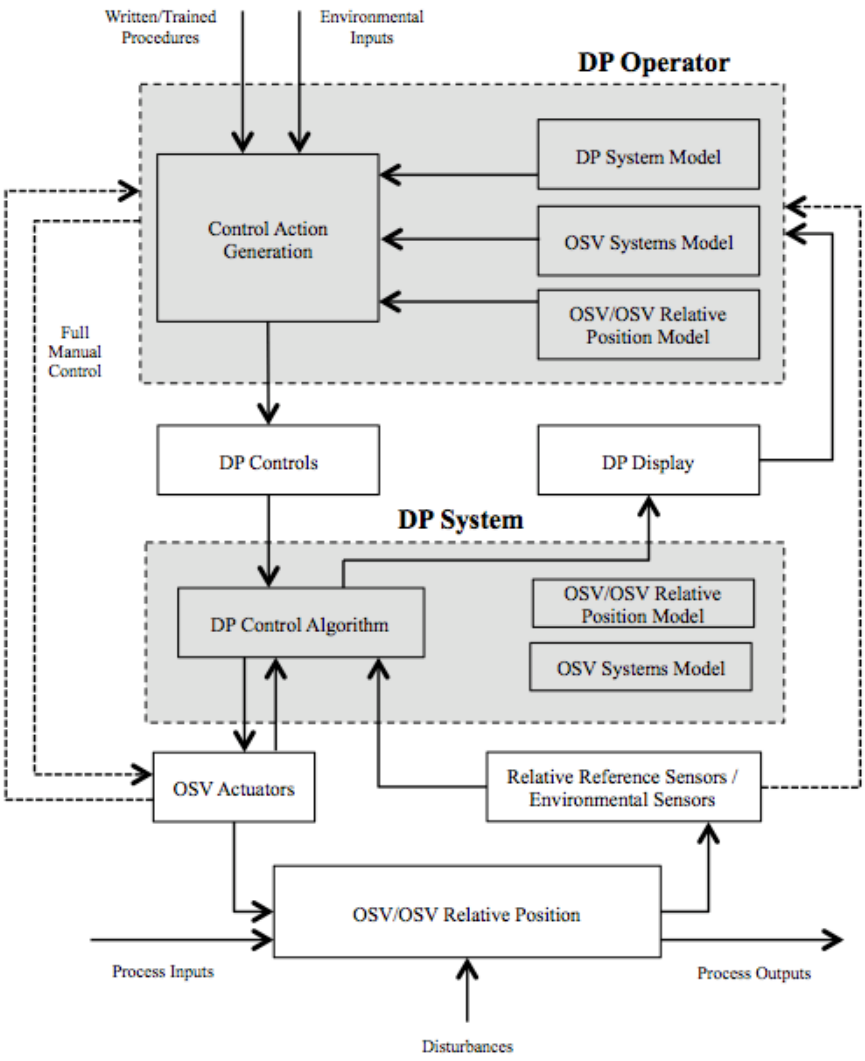

Figure 8: Functional Control Diagram between DP Operator, DP System, and OSV/OSV Relative Position

An important control structure to understand within the OSV System is between human controllers and automated controllers. This relationship is important because, as Dr. Leveson highlights, "we cannot 'design' human controllers, but we can design the environment or context in which they operate, and we can design the procedures they use, the control loops in which they operate, the processes they control, and training they receive." [**3**] This is particularly relevant in accident investigation, because these interactions are often where unsafe control and feedback may shape the context in which human operators made decisions. Both controllers in the system, the DP Operator and the DP System, contain process models of the systems being controlled.

3.5.2.1. OSV/OSV Relative Position

The controlled process in Figure 8 is the relative position between the Follow OSV and Target OSV. The OSV Actuators, any secondary process inputs, and external disturbances control the relative position between the Follow OSV and Target OSV. The OSV Actuators consist of the tunnel thrusters, bow rotors, rudders, and main engines.

3.5.2.2. DP System

The DP System contains a DP Control Algorithm responsible for processing inputs and feedback and updating the DP System process models. It uses these process models and other inputs to produce control outputs to the OSV Actuators. The DP System has three main inputs: DP Controls inputs sent from the DP Operators, sensor feedback from the Reference Sensor Systems and Environmental Sensors, and feedback from the OSV Actuators. Feedback is critical for the DP System to know if the control actions to the OSV Actuators were received, for detecting any errors or failures in the system, and for updating the DP System process models in how the system is responding. The OSV/OSV Relative Position Model and OSV Systems Model are what the DP System believes the current state of the system is. The DP System uses the NRL Filter to check for any out of range or unexpected inputs from the Reference Sensor Systems against the OSV/OSV Relative Position Model. Any out of range data is rejected.

3.5.2.3. DP Operator

The DP Operator has a model of the OSV/OSV Relative Position, the OSV Systems, and a model of the DP System that informs the operator's control action generation. The DP Operator's control action generation is similar to the DP System's Control Algorithm, except the DP Operator has a DP System Model in addition to the OSV/OSV Relative Position Model and OSV System Model. Initial training, instructed procedures, and experimentation mainly affect the DP Operator's control action generation for the controlled process over time. The DP Operator also has environmental inputs and display information from the DP System to update the process models and inform control action generation.

The Functional Control Structure also shows direct feedback to the DP Operator from the OSV Actuators, Reference Sensor Systems, and Environmental Sensors. This feedback (noted by the dotted arrows) is pertinent when the DP Operator controls the system via Full Manual Control.

The Functional Control Structure is discussed in more detail, as it pertains to the late July 2014 accident, in the DP System Analysis Section 3.8.2.

3.5.3. Safety Control Structure

The safety control structure shown in Figure 9 depicts the detailed component interactions within the OSV system during testing and tuning operations.

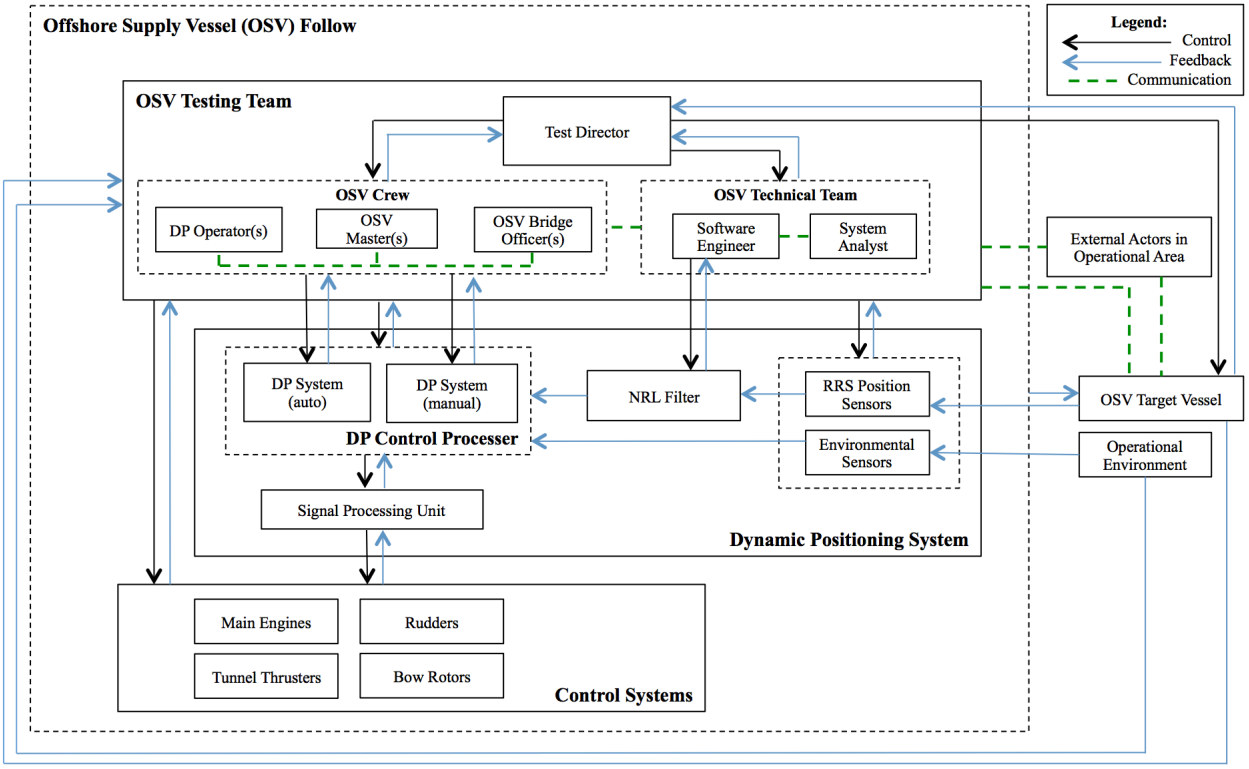

Figure 9: Detailed OSV/OSV Testing Safety Control Structure

The three types of interactions between components are control actions, feedback, and communication. These interactions are detailed below:

Control Actions:

1. Test Director ➔ OSV Crew
    a. Direct sequence of test plan events
    b. Ensure OSV Crew is qualified for test
    c. Ensure OSV Crew understands test objectives
2. Test Director ➔ OSV Technical Team

a. Assign test team duties
b. Ensure OSV Technical Team understands test objectives

3. Test Director ➔ OSV Target Vessel
    a. Coordinate events and ensure safe initial conditions
4. OSV Crew ➔ DP System (auto)
    a. Activate/deactivate DP System (auto)
    b. Set user configurable parameters
5. OSV Crew ➔ DP System (manual)
    a. Activate/deactivate DP System (manual)
    b. Set user configurable parameters
    c. Provide directional commands
6. OSV Testing Team ➔ DP Control Processer
    a. Setup Data Logger
    b. Start/Stop Recording Data
7. Software Engineer ➔ NRL Filter
    a. Set NRL Filter parameters
8. OSV Crew ➔ RSS Position and Environmental Sensors
    a. Turn sensors ON/OFF
    b. Set sensor parameters
9. DP System ➔ Signal Processing Unit
    a. Signal directional command
10. Signal Processing Unit ➔ Control Systems
    a. Implement directional command
11. OSV Crew ➔ Control Systems
    a. Activate/deactivate full manual mode
    b. Switch between Fore/Aft Control Panel
    c. Thruster directional command
    d. Rudder control input
    e. Main Engine control input
    f. Rotor control input

Feedback:

1. OSV Crew ➔ Test Director

    a. Automatic operations qualification requirement checks
    b. Report any unsafe (environmental/system) conditions
2. OSV Technical Team ➔ Test Director
    a. Modifications to tuning procedure
3. OSV Target Vessel ➔ Test Director
    a. Initial Target OSV system state conditions
    b. Visual feedback on OSV/OSV relative distance
4. DP System (auto) ➔ OSV Crew
    a. Graphical display information
    b. Subsystem status/information
    c. Visual sensory feedback
    d. Proprioceptive feedback
    e. Auditory sensory feedback
    f. Dead Reckoning Mode Alarm
5. DP System (manual) ➔ OSV Crew
    a. Graphical display information
    b. Subsystem status/information
    c. Visual sensory feedback
    d. Proprioceptive feedback
    e. Auditory sensory feedback
6. DP Control Processor ➔ OSV Testing Team
    a. Logged vessel feedback data
    b. Logged DP System data
7. NRL Filter ➔ Software Engineer
    a. Graphical display information
    b. Subsystem status/information
8. Signal Processing Unit ➔ DP System
    a. Actuator feedback data
9. Control Systems ➔ Signal Processing
    a. Raw actuator positional data
    b. Actuator status
10. Control Systems ➔ OSV Crew
    a. Visual sensory feedback

    b. Proprioceptive feedback
    c. Auditory sensory feedback
11. NRL Filter ➔ DP Control Processor
    a. Heading and position data
    b. “Good” or “Bad” signal for RSS data
12. RSS Position Sensors ➔ NRL Filter
    a. Raw target reference frame data
13. Environmental Sensors ➔ DP Control Processor
    a. Wind speed/direction data
    b. Geographical directional data
    c. OSV roll, pitch, heave data
    d. Water current data
14. OSV Target Vessel ➔ RSS Position Sensors
    a. Reflection confirmation
    b. Position information between RSS Position Sensors and reflectors
15. OSV Target Vessel ➔ OSV Testing Team
    a. Visual feedback on OSV/OSV relative distance
16. OSV Follow Vessel ➔ OSV Target Vessel
    a. Reflection confirmation
    b. Position information between RSS Position Sensors and reflectors
17. Operational Environment ➔ Environmental Sensors
    a. Raw environmental data
18. Operational Environment ➔ OSV Testing Team
    a. Visual sensory feedback
    b. Auditory sensory feedback

Communication

1. Communication between OSV Crew and OSV Technical Team
2. Communication between DP Operator(s), OSV Master(s), and OSV Bridge Officer(s)
3. Communication between Software Engineer and System Analyst
4. Communication between OSV Testing Team and External Actors in Operational Area
5. Communication between OSV Testing Team and OSV Target Vessel
6. Communication between OSV Target Vessel and External Actors in Operational Area

3.6. Proximate Events Leading to Loss

3.6.1. Accident Test Matrix

The accident occurred during Test Event #18 of the tuning event timeline. The NRL Filter parameters are altered in a series of tests as the OSVs repeat preset maneuvers in order to collect this set of test data. In order to build a comprehensive set of test data, NRL parameters were tested at values that were less than the expected optimal values. This test was designed to confirm the bounds of the NRL Filter parameters and indicate which values were too restrictive. This test began at a higher lateral separation to invoke a greater measurement of noise from the sensors and to begin testing at a safer distance.

The test event matrix used in July 2014 is depicted in Table 3:

Test Matrix	Test Number	Maneuver	NRL Parameters	Lateral Separation	Speed	Turn
A	1	A1	aa	High	12-13kts	Starboard
	2	A2	aa	High	12-13kts	Port
	3	A1	bb	High	12-13kts	Starboard
	4	A2	bb	High	12-13kts	Port
	5	A1	cc	High	12-13kts	Starboard
	6	A2	cc	High	12-13kts	Port
	…	…	…	…	…	…
B	17	B1	aa	Low	12-13kts	Port
	18	B2	aa	Low	12-13kts	Starboard
	19	B1	bb	Low	12-13kts	Port
	20	B2	bb	Low	12-13kts	Starboard
	21	B1	cc	Low	12-13kts	Port
	22	B2	cc	Low	12-13kts	Starboard
	…	…	…	…	…	…

Table 3: Test Matrix Alpha and Bravo used in July 2014

As shown in the test sequence in Table 3, there were two different test matrixes, A and B. Test Matrix A consists of Tests #1 through #16 and Test Matrix B consists of Tests #17 through #32. The vessel speed was constant for all tests and each set of parameters was evaluated using a

starboard and port turn. Test #1 and Test #2 have the same software parameters, except Test #1 is a starboard turn and Test #2 is a port turn. Test Matrix A and B are identical except Matrix A was conducted first at a high lateral separation, whereas Matrix B was conducted second at a low lateral separation.

3.6.2. Events Leading to Collision

The OSV crews spent over four hours running parameter changes on the NRL Filter for Test Matrix A at the higher lateral separation distance prior to Test #18. All except the two tests with the most restrictive NRL parameters passed in Test Matrix A. During Test #1 the DP System entered Dead Reckoning Mode and the DP Operator conducted a breakaway. As a result of the breakaway, the OSV Testing Team decided to skip Test #2. Test #2 would have been the same as Test #1 except the vessels would have executed a port turn rather than a starboard turn. After finishing Test Matrix A, the crew reduced lateral separation and began Test Matrix B.

The first two tests in Test Matrix B were the same ones that failed in Test Matrix A. During Test #17 the Follow OSV entered Dead Reckoning for one second and then immediately recovered. The OSV Crew completed the turn. The OSV Crew then decided to continue to Test #18. The system analyst gave a verbal warning to the DP Operator that the vessel may enter Dead Reckoning again. It should be noted that Test #18 is the same as Test #2, but at a closer lateral separation. Thus, the parameters and direction of turn for Test #18 was never conducted at the safer high lateral separation distance of the skipped Test #2.

Midway through Test #18 the DP System entered Dead Reckoning Mode, the DP Officer broke away and a minor collision occurred after a series of events detailed in the Chain of Events Section 3.2.1.

3.7. Physical Failures

The RCA&CA investigation found that no physical components failed on the OSV and all systems performed in accordance with their designed parameters leading to the accident. The discussion on how the physical design of the OSV affected the DP Operator's performance is covered in the OSV Level Controller Analysis Section 3.8.

3.8. OSV Level Controller Analysis

3.8.1. NRL Filter Analysis

Safety-Related Responsibilities

- Compare new RSS measurements to the last good RSS measurements.
- Reject RSS data measurements if differences between last good and new measurements are greater than set parameter threshold.
- Send RSS data measurements to DP Control Processor if differences between last good and new measurements are lower than set parameter threshold.
- Send signal to DP System if all three RSSs signals are rejected.
- Send signal to DP System if RSS signals are recovered.

Context

- Two previous accidents occurred in part due to unwanted RSS measurement noise being sent to DP System. The NRL Filter was updated to include heading measurements in order to avoid unwanted measurement noise. Previously, the NRL Filter would only reject data when there was a rapid shift in position, and not shifts in heading.
- NRL was tested at parameter values less than expected operational optimums to ensure a full set of data collection.

Unsafe Decisions and Control Actions

- Not applicable. NRL Filter only sends feedback from RSS position sensors to DP Control Algorithm based on parameter settings. While not an unsafe control action, the NRL Filter rejected appropriate raw sensor data from the Target OSV resulting in Dead Reckoning Mode.

Process Model Flaws

- NRL Filter believed Target OSV data was environmental noise, and consequently rejected all incoming Reference Sensor System data. This lack of RSS data led the DP System to have a flawed process model (thinking the sensors had failed when they had not) and resulted in the DP System moving into Dead Reckoning Mode.

The System Analyst Contractor created the following functional control diagram to detail the feedback between the RSS position sensors, NRL Filter, and DP Control Processor:

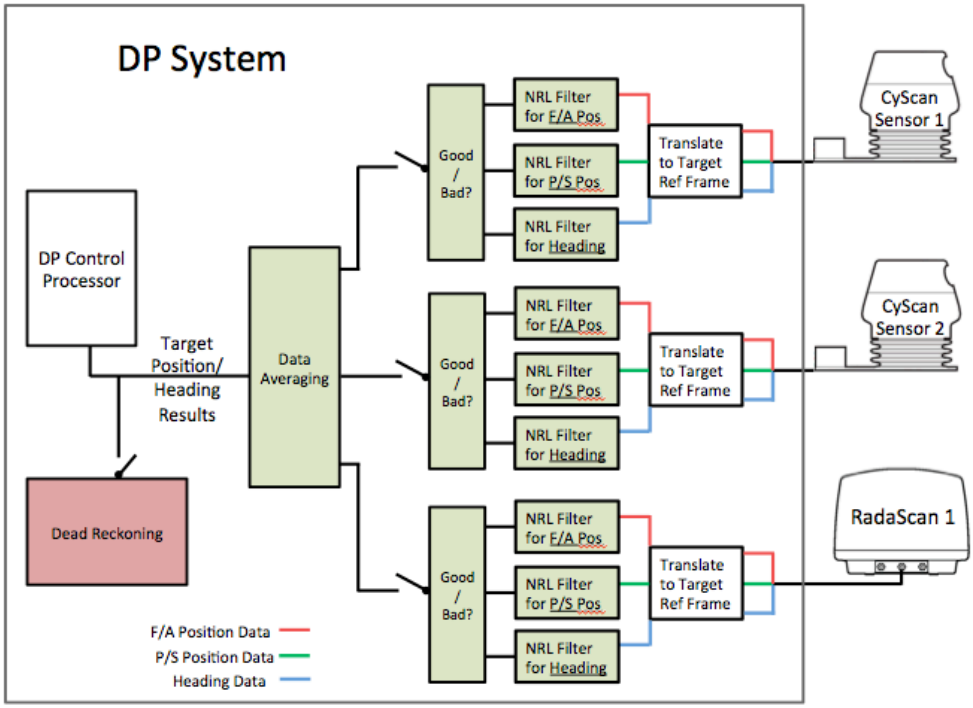

Figure 10: Functional Control Diagram detailing feedback between RSS sensors, NRL Filters, and DP System

The NRL Filter analyzes the raw RSS data and determines if any signals are outside the parameter thresholds, indicating unwanted environmental noise. The DP System averages the data sent from the NRL Filters and sends the resulting Target Position/Heading Results to the DP Control Processor. If any of the NRL Filters for each sensor determine the data has exceeded the parameter threshold set by the Software Engineer, a "Bad" signal is sent to the "Data Averaging" processor. If all three RSS sensors send a "Bad" signal, Dead Reckoning Mode is entered. Upon any of the NRL Filters sending back a "Good" signal, Dead Reckoning Mode is exited and the DP System automatic Target-Follow mode retakes control.

Appendix A further details the NRL Filter rejection and the four events leading up to the DP Operator switching to Manual: DP System operating with no NRL Rejection, DP System in Dead Reckoning Mode with all RSS sensors rejected, DP System recovering from Dead Reckoning Mode after one RSS sensor recovers, and DP System in Dead Reckoning Mode with all RSS sensors rejected.

The NRL Filter did not fail in this accident. It acted in accordance with the parameters listed in the testing plan.

3.8.2. DP System Analysis

Safety-Related Responsibilities:

- Automatically send control commands to tunnel thrusters, bow rotors, rudders, and main engines to maintain lateral separation from Target OSV as commanded by DP Operator.
- Automatically enter Dead Reckoning Mode and send control commands based on available Target OSV position and heading if all RSS sensor data are "Bad."
- Display OSV Actuator current status and commanded status.
- Display Reference Sensor System and Environmental Sensor data.
- Alert OSV Crew when any deviations in course or operations occur.
- Alert OSV Crew of any abnormalities or malfunctioning of OSV Actuators, Reference Sensor Systems, or Environmental Sensors.

Context:

- OSVs were originally designed for Offshore Oil Drilling. The default thruster control station for drilling operations is in the Aft Control station and was never redesigned for target-follow operations.
- Forward Control station's manual controls are preset to a breakaway configuration. Aft Control station's manual controls are not preset. No human controller is required to observe the Aft Control station.
- Prior to testing, the DP System was simulated with NRL Filters and found to not be at serious risk of entering Dead Reckoning Mode.

Unsafe Decisions and Control Actions:

- DP System did not give relevant feedback to OSV Crew about Dead Reckoning Mode.
- DP System automatically defaults Full Manual Control of thrusters to Aft Control station instead of the Forward Control station, which is where the OSV Crew operates the vessel.
- Kalman filter reset estimated relative OSV velocity to zero upon entering Dead Reckoning Mode. This inhibited the DP System from recovering from Dead Reckoning Mode.
- Data logger does not log DP Operator input commands, only feedback data from vessel movement.

Process Model Flaws:

- DP System believes position data from RSS sensors is invalid and should not be used to control OSV.

- DP System upon entering Dead Reckoning Mode believes there is zero relative motion between Follow OSV and Target OSV.

Unsafe Interaction between DP System and NRL Filter

An unsafe interaction between the DP System and the NRL Filter prevented the DP System from recovering from Dead Reckoning Mode on its own during Test #18. The DP System in Dead Reckoning Mode works, in part, by using a Kalman Filter algorithm to estimate where the Target OSV and Follow OSV will be in the future given past sensor data. The recorded data from the vessels showed that a previously identified software issue in which the Kalman Filter resets the relative velocity rate to zero during Dead Reckoning occurred during this testing event. The Kalman Filter resetting the relative velocity rate between Target OSV and Follow OSV means the DP System believed the target vessel and following vessel continued moving and rotating at the same speed when Dead Reckoning Mode was entered. The DP System's model of the OSV/OSV relative velocity did not match the actual system state. DP Software Engineering gave the following example to illustrate the Kalman Filter processing issue [**9**]:

> "For example, say the target vessel is initially rotating at 25°/min to port and the follower is rotating at 30°/min to port. Assuming the follower is on the starboard side, the estimated relative motion rate as seen by the follower is 5°/min to port. If the follower vessel then enters Dead Reckoning, the relative motion rate is reset to zero and the follower then believes that the target is rotating at 30°/min. If the follower then climbed to 40°/min, then it would believe the target vessel also climbed to 40°/min as well where in reality it could still be at 25°/min."

This Kalman Filter issue had further unintended consequences with regards to the NRL processing. The NRL Filter works by comparing new sensor measurements to the last good sensor measurement to see if the difference between the two is greater than a preset threshold. DP Software Engineering noted [**9**]:

> "To account for the expected differential, the past measurement is propagated using the estimated relative velocity. Consequently, resetting the relative velocity to zero during Dead Reckoning eliminates the propagation of the past measurements in the NRL processing."

Resetting the relative velocity between the OSVs whenever there is relative motion between the Target OSV and Follow OSV made it extremely difficult for the DP System to recover from a NRL rejection while in Dead Reckoning Mode. Due to the nature of turning maneuvers, relative motion between the OSVs is expected. There was approximately a 10 meter change unaccounted for in relative position between the time Dead Reckoning Mode began and Manual Mode was entered due to the Kalman filter resetting the relative velocity rate to zero.

The reason behind this known issue not being fixed prior to testing is covered in Section 3.10 Engineering and Testing Development Controller Analysis.

The following **recommendations** address the unsafe interaction:

- Kalman Filter must freeze relative velocity instead of resetting relative velocity to zero upon DP System entering Dead Reckoning Mode.

3.8.3. OSV Crew Analysis: DP Operator(s), Bridge Officer(s)

Safety-Related Responsibilities:

- DP Operators are responsible for the safe maneuvering of the OSV using both the DP System and Full Manual Control.
- DP Operators are responsible for maintaining minimum lateral separation standards with Target OSV.
- DP Operators are responsible for understanding and performing breakaway procedures any time they feel the safety of either vessel is in jeopardy.
- DP Operators are responsible for understanding and performing breakaway procedures when conditions dictate mandatory breakaway as defined in operation procedures.
- DP Operators are responsible for conducting practice breakaways prior to testing events requiring close lateral separation with the Target OSV vessel.
- DP Operators are responsible for reporting any unsafe conditions (environmental or systems) to the Test Director.
- DP Operators are responsible for granting permission to the System Analyst or Software Engineer before any changes are made to DP System software code, parameters, gains, or actuators.
- DP Operators are responsible for canceling and clearing all DP System Alarms.

- Bridge Officers are responsible for communicating with the DP Operator and OSV Master when they feel the vessel is in jeopardy or a breakaway should be conducted.
- DP Operators and Bridge Officers are responsible for operating the OSV in accordance with OSV Manufacturer Management procedures, Rules of the Road, and the Safe Operations Manual.
- DP Operators and Bridge Officers are responsible for understanding the Target-Follow Software Tuning Procedures, Test Plan, and Test Sequence.
- DP Operators and Bridge Officers must participate in a pre-test safety brief conducted by the OSV Manufacturer Management representative and the Test Director.
- DP Operators and Bridge Officers are responsible for completing all pre-underway checklists. Where applicable, initial checklist must be independently verified by a second Bridge Officer.
- DP Operators and Bridge Officers are responsible for filling out exercise data sheets post-operation.
- DP Operators and Bridge Officers are responsible for setting radios within the pilothouse to channels to monitor applicable traffic.
- DP Operators and Bridge Officer are responsible for requesting permission to come alongside from the Target OSV Bridge Officers.
- DP Operators and Bridge Officers are responsible for updating the Target OSV Bridge Officers about their vessel's capabilities and material condition.
- DP Operators and Bridge Officers are responsible for communicating with the Target OSV before any maneuver and if a breakaway ever occurs.

Context:

- Test Director, System Analyst, and OSV Master were not on the bridge during Test #18.
- DP System entered and recovered from Dead Reckoning Mode on Test #17, the previous test event to Test #18.
- The Software Engineer warned the DP Operator that the DP System might enter DR Mode again for Test #18.
- Instituting a breakaway during a test event requires approximately 15-20 minutes to realign the OSVs and reinstate testing.
- The RCA&CA from the previous accident, on 4 June 2014, determined the DP Operator in the Target OSV used excessive rudder during an emergency breakaway, causing the two OSVs to collide.

- DP System frequently alarmed throughout the four hours of testing leading to the accident, requiring constant manual acknowledgement/canceling of alarms from the OSV Crew.

Unsafe Decisions and Control Actions:

- DP Operator did not breakaway upon loss of all Reference Sensor Systems.
- DP Operator did not initially press the button to switch thruster control from the aft control station to the forward control station.
- DP Operator did not use available rudder to steer OSV.
- Bridge Officer began clearing DP System Alarms leading up to Test #18.

Process Model Flaws:

- DP Operator believed it was acceptable for the DP System to stay in Dead Reckoning Mode for a certain amount of time before breaking away.
- DP Operator believed the DP System would recover from Dead Reckoning Mode like previous Test Events.
- DP Operator believed he pressed the button to switch the thruster control from the aft control station to the forward control station.
- DP Operator believed he was in control of the OSV Thrusters for 17 seconds, when in fact, the aft control station was in control of the OSV Thrusters.
- Bridge Officer believed it was okay to help manage the DP System Alarms.

The system analysis must consider how humans operate within the context of the physical system. It is important to understand what information was and was not available to the DP Operator, what behavior-shaping mechanisms were present, what environmental inputs were affecting the operator decisions, and what process model flaws existed and why. Table 4 shows the relative time scale between the initiation of Test Event #18 and the minor collision.

Event	Relative Time (s)	Event Description
18.A	00:00	Test Event #18 Initiated
18.B	00:28	Dead Reckoning Mode Entered 1st Time
18.C	00:30	Dead Reckoning Mode Entered 2nd Time
18.D	00:39	Full Manual Mode Entered
18.E	00:56	Both Tunnel Thrusters Manually Directionally Configured
18.F	01:05	Both Tunnel Thrusters Manually 100% Configured
18.G	01:11	Minor Collision

Table 4: Event timeline organized with relative timescale

As shown in Table 4, the DP System entered Dead Reckoning Mode twice, and it was not until 9 seconds after the DP System entered Dead Reckoning Mode the for the second time that the DP Operator shifted to Full Manual Mode. Figure 11 is the Functional Control Structure with the available feedback channels to the DP Operator highlighted between Event 18.A and 18.C.

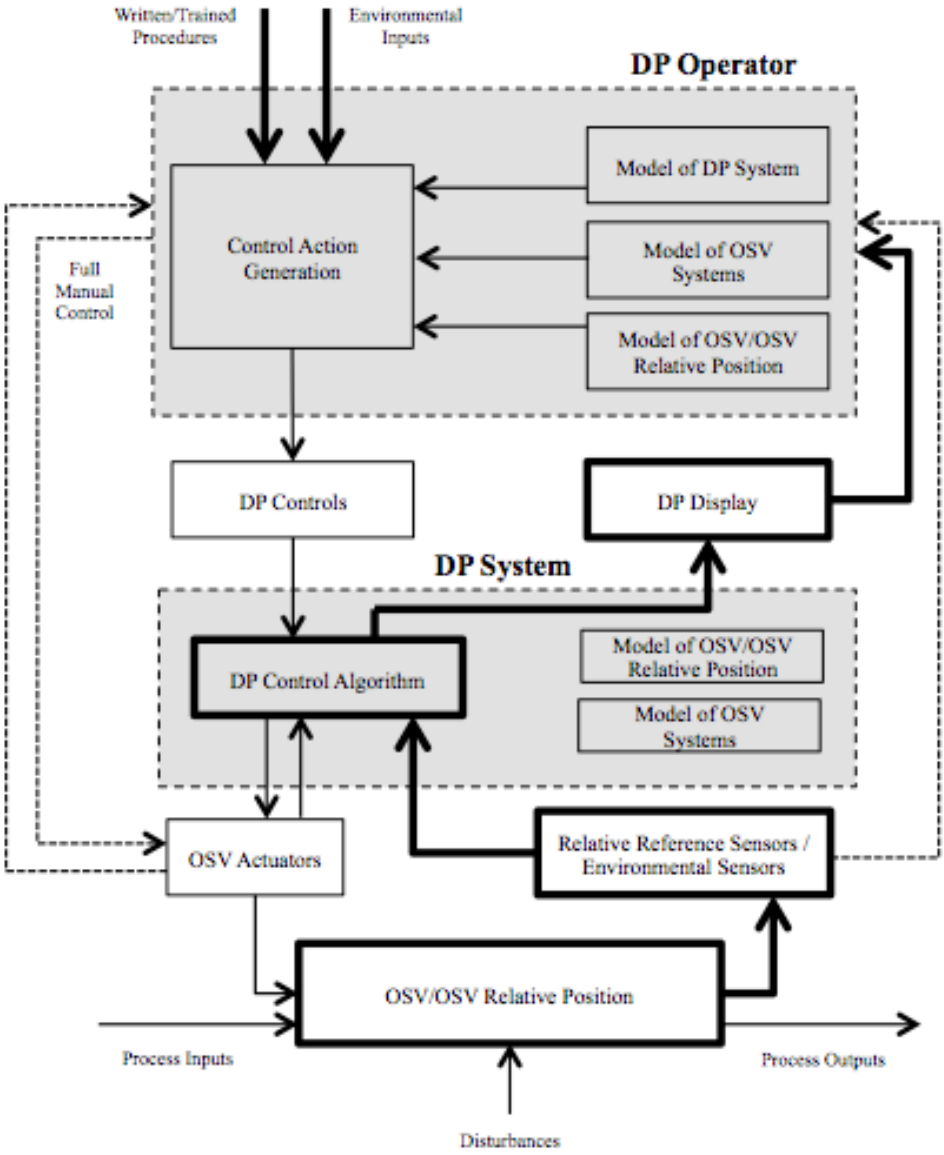

Figure 11: Functional Control Structure with highlighted feedback to the DP Operator in Target-Follow Mode and Dead Reckoning Mode

The DP Operator received two main forms of feedback when the DP System automatically switched to Dead Reckoning Mode. The main form of feedback was the DP Display notifying the operator with an alarm banner across the DP Display stating Dead Reckoning Mode has been entered. The DP Operator also had the ability visually see the Target OSV through the window; however, DP Operators do not usually rely this environmental input while the DP System is in control of the OSV.

DP Operator Delayed Breakaway

Test procedures and training are a main form of input to the DP Controller's decision to either stay in Dead Reckoning Mode or to breakaway. The Target OSV – Follow OSV Test Plan specifically outlines the breakaway criteria. One of the breakaway criteria directly states the DP Operator must breakaway whenever all position data from all RSSs are lost. Because Dead Reckoning Mode only occurs during the loss of all Reference Sensor Systems, anytime the vessel enters Dead Reckoning Mode would dictate a breakaway according to this criterion. However, the term "Dead Reckoning Mode" was not specifically codified in any of the test documents. The DP Operator would have to understand that the loss of all RSS data equates to Dead Reckoning Mode, which was a particularly uncommon mode outside of the testing environment. The DP Operator did not strictly follow the Target OSV – Follow OSV Test Plan.

Several contextual factors influenced the DP Operator's decision not to immediately breakaway upon receiving the Dead Reckoning Mode notification at event 18.B and 18.C. A main influence was that Dead Reckoning Mode was entered on the Test Event #17, which was the immediately preceding test event where a breakaway was not performed. The Software Engineer warned the DP Operator that the DP System may enter Dead Reckoning Mode again before Test Event #18, which also indicates the OSV Testing Team did not view the loss of all RSS data as a reason to immediately breakaway. Performing a breakaway causes a 15-20 minute delay in testing because the Follow OSV must realign with the Target OSV and resume automatic Target-Follow Mode in order to begin test event again. This delay in testing created an incentive within the OSV Testing Team to wait to see if the DP System would recover from Dead Reckoning Mode before conducting a breakaway.

Unassigned Responsibility

One breakaway criterion dictates a breakaway should occur after an extended period of time with the loss of one RSS. Further, the OSV Testing Team believed that only after a certain amount of time that the DP System remained in Dead Reckoning Mode should a breakaway occur. However, no documentation specified a controlling time limit or time range in which Dead Reckoning Mode operation would be allowed. This problem was exacerbated because the DP System did not display the amount of time it was in Dead Reckoning Mode. The responsibility

to track the DP System's time in Dead Reckoning Mode was never assigned to any controller on the bridge. Humans are already poor at precisely tracking time, and given the added stress of the test, it is unfeasible to believe the DP Operator would be able to track time before executing a breakaway.

Unsafe Controller Coordination

The Bridge Officer began clearing the alarms for the DP Operator due to the excessive number of alarms propagated by the DP System during the testing event. There is no guidance directing the Bridge Officer not to clear alarms, however, the OSV Safe Operating Manual only places the Vessel Master and/or DP Operator(s) in charge of control while operating the DP System. Allowing an extra controller to clear and cancel alarms may result in unsafe unintended consequences. Incidents may arise when inconsistencies between the DP Operator's process model does not match the Bridge Officer's process model. For example, if the Bridge Officer clears an alarm that the DP Operator does not notice, the DP Operator may not realize the OSV is in an alarmed state. The DP Operator may make unsafe control actions based on the resulting flawed process model. This is particularly relevant in testing and tuning events at close proximity with another OSV.

Missing Environmental Inputs

At the time of Test Event #18, the System Analyst, OSV Master, and Test Director were all missing from the bridge due to a lunch break. This resulted in the DP Operator missing both experience and guidance from the individuals directing the test plan. The absence of these individuals may have also changed the DP Operator's assessment and tolerance of risk during this particularly high-risk event.

The following **recommendations** address the unsafe delay in conducting a breakaway:

- If portions of test documentation are designed as guidelines meant to be flexible, these portions must be identified and communicated appropriately. Similarly, safety procedures designed not to be flexible should be identified.
    - Breakaway criteria must match the test event. If a time in Dead Reckoning Mode is part of the breakaway criteria, it must be included in the test documentation.

- Responsibility, to either DP System or a Bridge Officer, must be assigned to track time in Dead Reckoning Mode and warn the DP Operator when to breakaway.
- Engineering and Testing Development must establish operation policy / documentation regarding:
    - Minimum number and type of OSV Testing Team on bridge during test events.
    - Establish policy for crew transfer and temporary crew absence from bridge.
    - Provide procedures for transfer of shared safety related responsibility (ex: clearing DP alarms).

The DP Operator eventually switched to Full Manual Mode and conducted a breakaway 9 seconds after Dead Reckoning Mode was entered for the second time. Upon entering Full Manual Mode, the DP Operator failed to correctly configure the tunnel thrusters in a breakaway direction for 17 seconds. It takes the tunnel thrusters an additional 9 seconds to achieve full thrust after they correctly positioned. Thus, it took a total of 26 seconds after entering Full Manual Mode for the tunnel thrusters to begin pushing away from Target OSV with 100% thrust. Figure 12 is the Hierarchal Control Structure with the highlighted feedback channels available to the DP Operator between the time of the breakaway and the minor collision.

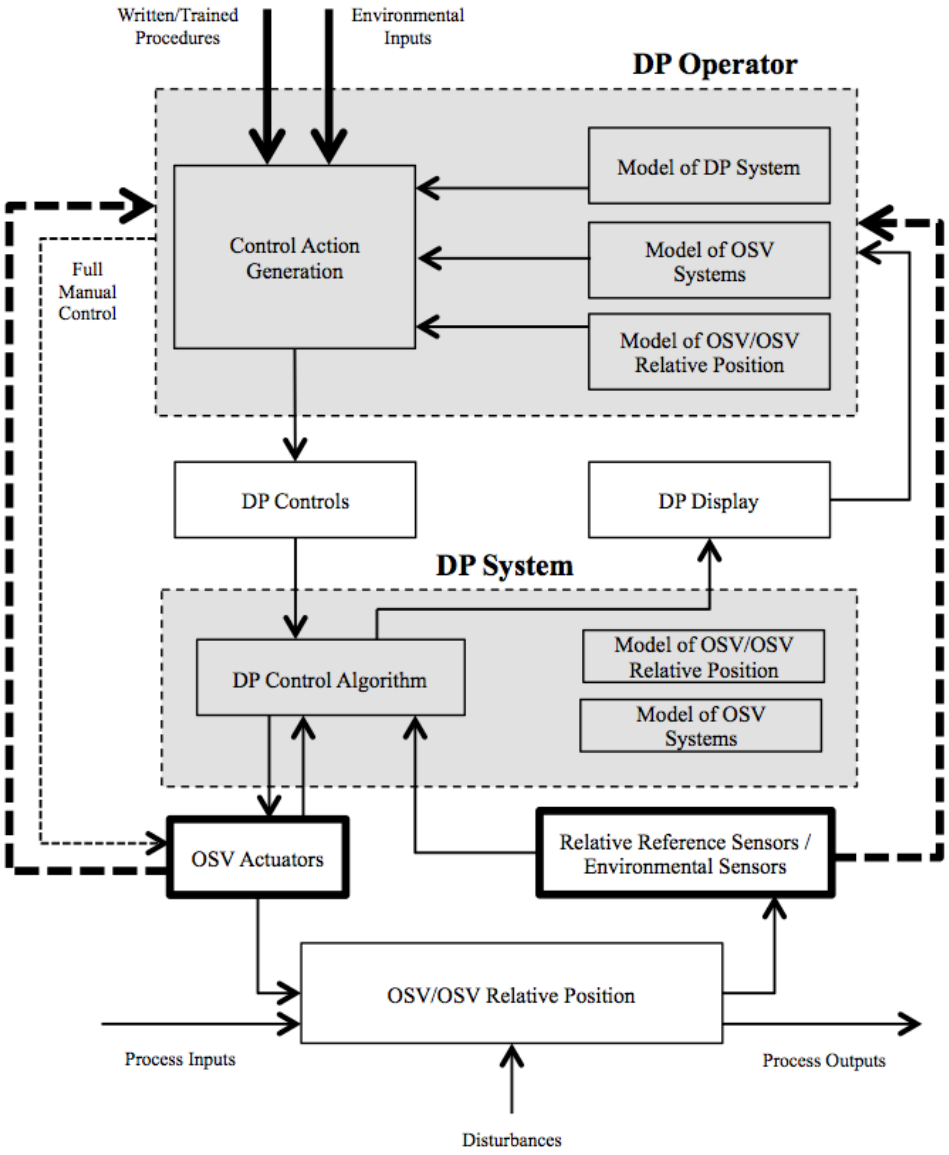

Figure 12: Functional Control Structure in Full Manual Mode

In Full Manual Mode, the main inputs to the DP Operator were feedback from the OSV Actuators on the Manual Control Station, and any environmental inputs. The DP Operator mainly uses his/her vision to estimate the relative position between the two OSVs. The DP Operator only looks at the Manual Control Station if a problem with the controls occurs, or to fine-tune the OSV Actuators. While the Environmental Sensor data is still available in Full Manual Mode, it is unlikely the DP Operator uses this feedback channel in an emergency breakaway procedure.

The DP Operator did not rely on the DP Display to gather information and update process models after switching to Full Manual Mode. The data from the Reference Sensor Systems was filtered and rejected, thus, feedback in the form of lateral separation alarms was no longer available. These particularly critical alarms indicate when the Follow OSV has violated the established minimum separation with the Target OSV. The DP Operators are trained to immediately commence breakaway procedures when the minimum separation alarms are received. However, in Full Manual Mode there is no system on the OSV to notify the DP Operator if the minimum lateral separation between the OSVs has been lost. The DP Operator must rely on visually looking at the Target OSV when breaking away to determine relative position.

DP Operator's Flawed Process Model

The DP Operator experienced mode confusion between the time Full Manual Mode was entered and when the tunnel thrusters were aligned 17 seconds later. The DP Operator first rotates a barrel switch to transition from Target-Follow Mode to Full Manual Control. The barrel switch has several end states, which place the OSV in different control configurations. Once the DP Operator turns the barrel switch to the correct configuration, the DP Operator is in control of all OSV Actuators except the OSV's tunnel thrusters. The DP Operator must then press the Control Request button to transition thruster controls from the aft control station to the forward control station. At Event 18.D the DP Operator believed he turned the barrel switch to shift into Full Manual Mode and pressed the Control Request button to take control of the OSV tunnel thrusters. However, either the DP Operator did not fully press the Control Request button down, or the DP Operator forgot this step. The DP Operator believed he was in full control of the OSV at this time. However, between Event 18.D and 18.E the Aft Control station was inputting commands to the tunnel thrusters based on their last used settings. There were no Bridge Officers at the aft station during this breakaway.

Inadequate Feedback between DP System and DP Operator

There was no alarm system to notify the DP Operator of this slip. The DP Operator would have received three inadequate forms of feedback indicating the aft station was controlling the vessel. First, lights appear on the Manual Control station indicating thruster direction and engine RPM

when the forward control station is controlling the thrusters. The DP Operator did not notice these lights did not light up when he failed to press the Control Station button. Second, there was inconsistency between the DP Operator's thruster control inputs and the actual thruster direction/power display. Because the controls were coming from the Aft Control station, the manual thruster display only showed a single aft thruster pushing away, while the DP Operator was commanding both thrusters to push away. The DP Operator did not notice this inconsistency. Third, there was environmental inconsistency between the DP Operator's inputted commands to the vessel, and the actual OSV position. The OSV position was not changing in accordance with what the DP Operator was commanding the vessel to do. These forms of feedback were inadequate in fixing the DP Operator's mode confusion. For 17 seconds the DP Operator's Model of the OSV Systems did not match the actual state of the OSV Systems. The investigation after the accident found no component failures associated with the Control Request button.

The following **recommendations** address the unsafe delay in correctly configuring the tunnel thrusters upon entering Dead Reckoning Mode:

- Establish responsibility for Bridge Officer to watch lateral separation between Target OSV and Follow OSV in all testing maneuvers less than (x) feet.
    - Bridge Officer must watch lateral separation between Target OSV and Follow OSV whenever the OSV is using DP Manual Mode or Full Manual Mode.
    - Bridge Officer must communicate with DP Operator whenever vessels are not maneuvering in accordance with guidelines, or required lateral separation is violated.
- Establish a policy to prevent any obstruction of the DP Operator's view of Target OSV. For example, no personnel should be between the DP Operator and the Target OSV during any test event.
- DP System must automatically transfer thruster control to forward control station.
    - If transfer does not occur within (x) seconds, feedback must be given to DP Operator.
- OSV forward control station must give appropriate feedback and alarms to DP Controller if any controls are inputted from aft control panels when OSV is in Full Manual Mode.
- OSV control stations must provide feedback to DP Operator indicating which manual controls are providing commands to main engines, rudders, tunnel thruster, and bow rotors.
- Any abnormal controller inputs must be easily distinguishable and prevented.

- Over rotation of barrel switch must be prevented or an alarm must give proper feedback to controller.
- Control Station button design should be resized / further differentiated due to its high level of importance and high frequency of use.

- Manual thruster controls, both forward and aft, must be set to neutral prior to all DP System controlled operations.
- OSV must provide feedback, independent from the DP System, to the OSV Crew alerting of the loss of separation from a surrounding vessel, external object, or seafloor.

DP Operator's Unsafe Control Algorithm

The DP Operator used minimal rudder during the Full Manual Mode breakaway. There were two inputs that may have contributed to the DP Operator's lack of rudder during the breakaway procedure. First, the test plans and guidance may have influenced the DP Operator to use minimal rudder during the breakaway. For example, the Target OSV – Follow OSV Test Plan gives the following guidance for an OSV initiated breakaway:

a. *As situation dictates, ensure thrusters are configured to move away from the target vessel and switch to Manual Mode.*
b. *Bring the bow out first and begin coming up on power.*
c. *Use the thrusters to maintain a small toe out angle as the vessel moves away from the target.*

*****Note: An excessive toe out angle may cause the vessel to slow and be pushed back *****

Nowhere in the breakaway guidance do the procedures mention using rudder. The Target OSV – Follow OSV Test Plan also stated "in some cases, it may be more prudent for the Follow OSV to slowly open up distance from the Target OSV in lieu of conducting the breakaway procedure." [**10**] The test plan provides this option, however, it does not describe when the DP Operator should conduct a slow opening instead of conducting a breakaway procedure. This guidance may have affected the DP Operator's control action generation, and ultimately the decision not to use available rudder in the breakaway.

The second main influence may have been from the "Lessons Learned" disseminated after the 4 June 2014 minor collision. The RCA&CA for the collision identified one of the problems

leading to the accident as the OSV Master "used excessive rudder to turn to starboard" during the breakaway. [**8**] This excess rudder resulted in the stern of the OSV shifting towards the other vessel. This recent accident as well as the emphasis in the breakaway guidance not to use excessive toe out angle may have contributed to the DP Operator's unsafe control algorithm and subsequent decision not to use the rudder throughout the breakaway.

Unsafe Interaction between DP System and DP Operator

It should be noted that the OSV Operations Manual outlines five different methods to breakaway when in the automatic Target-Follow Mode. Only one of the five methods is through the use of Full Manual Control in accordance with how the DP Operator broke away in this accident. The other four methods rely on the DP Manual Mode. The DP Manual Mode still uses the DP System, but it does not rely on the Reference Sensor System data. These four outlined methods allows the DP Operator to use a single DP Joystick, rather than controlling the main engines, rudders, tunnel thrusters and bow rotors independently. However, OSV Masters and DP Operators rarely use these suggested methods because it is time consuming and difficult to use the DP Display interface to switch from the automatic Target-Follow Mode to a different DP Manual Mode. It takes more than one command to the DP System on different display screens to enter these modes. The benefits received from using the DP Manual Mode does not outweigh the time lost in enabling the mode during an emergency situation.

The following **recommendation** addresses the unsafe control inputs during breakaway:

- DP System must have usable interface to transition from Target-Follow Mode to DP Manual Mode for breakaway scenarios. This may entail minimizing necessary controller inputs to transition between DP System modes.

3.8.4. OSV Crew Analysis: OSV Master

Safety Related Responsibilities:

- OSV Masters have ultimate responsibility for OSV safe navigation and operations.
- OSV Masters are responsible for ensuring the safety of the OSV and all embarked personnel.
- OSV Masters are responsible for training, understanding, and compliance with OSV Operations Manual procedures.

- OSV Masters are responsible for retaining all checklist documents for 12 months for auditing purposes.
- OSV Masters are responsible for ensuring all applicable reference documents are available to DP Officers and Bridge Officers during operations.
- OSV Masters must 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 prior to commencing testing event.
- OSV Master must ensure the vessel is prepared in accordance with the OSV Operations Manual reference documents and checklists prior to conducting automatic operations.
- OSV Masters are responsible for ensuring the Data Logger is operational and recording data prior to the commencement of operations. OSV Masters are also responsible for training and understanding procedures for data retrieval.
- OSV Masters are responsible for ensuring Bridge Officers use correct checklists for testing event.
- OSV Masters are responsible for granting permission to the OSV Technical Team before any changes are made to the DP System software code.
- OSV Masters are responsible for terminating the exercise if deemed that it cannot be safely conducted.
- OSV Masters may suspend the exercise if environmental conditions are not satisfactory (wave height, wind speed, interfering vessel traffic, operational capability/material condition of all vessels, communications).
- OSV Masters are responsible for reporting any unsafe condition to the TD.
- OSV Masters are responsible for evaluating the OSVs' ability to complete the testing event in the Comment Sheet upon completion of the testing event.
- OSV Masters are responsible for completing "Master's Target Following Comment Sheet" after the test event.

Context:

- No contingency plan or guidance for OSV Master to leave the bridge during testing events (Ex: Lunch, Bathroom).
- Testing had been ongoing for over four hours, with only one emergency breakaway occurring after Test Event #1.

Unsafe Decisions and Control Actions:

- OSV Master was not present on the Bridge at the time of the incident.
- OSV Master did not ensure Data Logger was set up correctly.

Process Model Flaws:

- OSV Master did not believe he needed to be on the Bridge at the time of the incident.

Inadequate Responsibilities and Assigned Coordination

OSV Masters are assigned several safety related responsibilities during test events. They are responsible for granting permission to the OSV Technical Team before any changes to the DP System software, terminating the exercise if deemed it cannot be safely conducted, reporting any unsafe conditions to the TD, and suspending the exercise if environmental conditions are not satisfactory. However, these are all shared responsibilities with other controllers in the OSV Crew.

The OSV Master left the wheelhouse for lunch after four hours of testing with minimal incidents. The OSV Operations Manual dictates that a minimum of three Bridge Officers will be assigned to the wheelhouse during particular in-channel target follow mode operations. This applies to all OSV operations, not just testing events. However, the July 2014 test event was conducted outside of in-channel designated areas, so there were no policies regarding the minimum number of Bridge Officers necessary during the operation.

The flexible view of test documentation, and multiple controllers assigned to the same responsibilities, may have lead the OSV Master believe he was not needed on the bridge during all test events.

Recommendations in the Section 3.8.3 OSV Crew Analysis cover the missing requirements regarding minimum number and type of OSV Testing Team on the bridge for testing events.

3.8.5. OSV Technical Team: System Analyst, Software Engineer

Safety Related Responsibilities:

- Software Engineer is responsible for inputting NRL Parameters in accordance with the Software Update Tuning Procedure.
- Software Engineer is responsible for installing Testing Software Package before tuning and testing events.
- Software Engineer is responsible for installing Tactical Software Package after tuning and testing events.
- Software Engineer is responsible for installing and setting up the Data Logger from the Master DP Control Processor prior to test events.
- Software Engineer is responsible for communicating intentions to OSV Master, DP Operator, and Bridge Officers before making changes to the DP System software code, parameter, gains, or actuators.
- Software Engineer is responsible for informing the OSV Crew of the expected parameter change results.
- Software Engineer may modify tuning and calibration procedures to facilitate tuning process.
- Software Engineer is responsible for communicating with the Test Director about modifications to the tuning procedure to facilitate the tuning process.
- System Analyst is responsible for recording test data.
- System Analyst is responsible for communicating with the Test Director and the Software Engineer about the time for each test event.
- The System Analyst and Software Engineer are responsible for collecting the completed data sheets post-operation.

Context:

- Software Engineer was the only individual on either OSV that had a working understanding of the Kalman filter effect on the inability to recover to Automatic Follow Mode from Dead Reckoning Mode upon NRL Filter rejection.
- Software Engineer verbally communicated with the DP Operator and Bridge Officer that the DP System may enter Dead Reckoning Mode again for Test Event #18.
- No test guidance was created for OSV Technical Team to leave the bridge during testing events (Ex: Lunch, Bathroom).
- Testing had been ongoing for over four hours, with only one emergency breakaway occurring after Test Event #1.

Unsafe Decisions and Control Actions:

- Software Engineer incorrectly installed and set up the Data Logger on the backup DP Control Processor.
- System Analyst was not present on the bridge at the time of the incident.
- System Analyst and Software Engineer did not collect the post-operation comment sheets from the OSV Masters and the Test Director.

Process Model Flaws:

- Software Engineer expected less measurement noise at the smaller lateral separation as compared to the two tests that failed with the same parameters at the large separation distance.
- System Analyst did not believe he needed to be on the bridge during all test events.
- Software Engineer did not expect the Kalman filter resetting the estimated relative OSV velocity to zero upon entering Dead Reckoning Mode would affect the DP System's ability to recover from Dead Reckoning Mode.

Process Model Flaws

The Software Engineer was the only individual with a technical understanding of how the parameters in the NRL Filter may affect the performance of the DP System. It should also be noted that the Software Engineer altered the parameters on the DP System for the testing operation was the same individual who created the Software Update Tuning Procedure detailing the test sequence. The proposed purpose of starting at the higher lateral separation for testing events was both for beginning the test at a safe separation distance. Starting at a higher lateral separation would also invoke greater measurement noise from the sensors. It would make sense then, even after failing Test Event #1 and #2, to try to complete Test Event #17 and #18 because there would be less environmental noise and less likelihood of NRL Filter rejection. This flawed process model went unchecked during the document review processes and led to the degradation of the initial safety margin of starting the test sequence at a higher lateral separation. No specific requirements were given to the OSV Testing Team informing them at what point the test events should have been halted.

Inadequate Feedback Channel

The System Analyst and Software Engineer make up the Data Collection Team. The Target OSV – Follow OSV Test Plan assigns the Data Collection Team with the responsibility for collecting and inventorying the DP System logger data, RSS logger data, Follow OSV Master Comments,

TD Comments, and Target OSV Master Comments following the exercise. However, the Follow OSV Master Comments, TD Comments, and Target OSV Master Comments were not collected for this accident, and are rarely collected on other OSV testing missions. The test plan does not specify who on the Data Collection Team should collect which data, and there is no enforcement on the collection of the test data from the Operations Management.

Unsafe Control Action

The Software Engineer incorrectly set up the Data Logger to monitor the Backup DP Control Processor instead of the Master DP Control Processor. The entire Data Logger setup process, which is not conducted frequently, is complex and requires a technical understanding of the correct IP addresses for the system. The Software Engineer was not provided detailed procedures for the proper setup to log from the Master DP Control Processor.

Unassigned Responsibility

The System Analyst was not on the bridge during Test #18. The System Analyst is part of the Data Collection Team, and has the main responsibility to ensure the test time is recorded and communicated with the Test Director. The Software Engineer is also a part of the Data Collection Team, and was most likely given the duty to keep time of test events while the System Analyst had lunch. There were no policies or recommendations in place to dictate actions taken during lunch or other crew transfers.

The following **recommendation** addresses the identified unsafe control inputs, unassigned responsibility, and inadequate feedback channels:

- Create relevant testing procedures to specific test operations. When testing a range of parameters, there must be specific documentation on when to halt trials.
- Establish an effective feedback channel between the OSV Testing Team and Operations Management:
    - Provide feedback back to those reporters regarding any updates. Information must not go into "black hole," and reporting feedback should be encouraged or rewarded.
    - Establish responsibility to ensure mandatory feedback is collected.
    - Review feedback form. Ensure form facilitates sharing all safety information (ex: any slips or mistakes occurred that did not result in accident.)

3.8.6. Test Director

Safety Related Responsibilities:

Target Follow Software Tuning and Testing Procedures 1.022

- Test Director is responsible for directing testing and tuning in accordance with Target-Follow Software Tuning and Testing Procedures policy.
- Test Director is responsible for ensuring the OSV Master, DP Operators, and Bridge Officers are qualified in accordance with the current automatic operations qualification requirements prior to testing.
- Test Director is responsible for ensuring the OSV Crew and OSV Technical Team are familiar with the objectives of the test prior to commencing operations.
- Test Director is responsible for ensuring OSV Crew and OSV Testing Crew attends a pretest brief to ensure understanding of the purpose of the test.
- Test Director is responsible for ensuring a Job Safety Analysis has been completed prior to commencing operations.
- Test Director is responsible for communicating the parameters and objectives of each tuning/test run to the OSV Crew and OSV Technical Team during testing.
- Test Director is responsible for ensuring OSV Testing Crew communicates intentions for changing any DP System software code to OSV Crew prior to any changes.
- Test Director is responsible for ensuring all DP System software code changes by the OSV Technical Team are in accordance with the approved software tuning event.
- Test Director is responsible for communicating to the OSV Crew and OSV Technical Team of any changes to the test/tuning objectives that result from unexpected DP System behavior.
- Test Director is responsible for ensuring the data logger for OSV Target is operating and recording data.

Target OSV – Follow OSV Test Plan (R19)

- Test Director is responsible for communicating with the Target OSV Master, and Follow OSV Master to agree that the environmental conditions, the navigational picture, and the operational capability of all vessels are satisfactory prior to commencing each run.
- Test Director is responsible for observing the exercise events.
- Test Director is responsible for coordinating events to ensure initial conditions regarding safety and listed cautions are followed.
- Test Director is in charge of managing the sequence of test plan events.

- Test Director is responsible for assigning test team duties.
- Test Director is responsible for contacting Navy Programs if he/she is unable to comply with the test memorandum.
- Test Director may delay the commencement of, or delete, test events with the concurrence of the Navy Programs representative (if present).
- Test Director may suspend the exercise if environmental conditions are not satisfactory (wave height, wind speed, interfering vessel traffic, operational capability/material condition of all vessels, communications)
- Test Director is responsible for announcing Commence Exercise (COMEX) and announcing the completion of each run.
- Test Director is responsible for completion of the Daily Comment Sheet post-testing event, commenting on exercise status, exercise issues and resolution, lessons learned, and any operational issues

Software Update Tuning Procedures (R1/2)

- Test Director may modify tuning and calibration procedure to facilitate tuning process.
- Test Director may request execution of additional test runs listed in Tuning Procedure.
- Test Director is responsible for ensuring data logger is operating and recording data.
- Test Director is responsible for filling out exercise data sheets post-operation.
- Test Director is responsible to communicate with the Software Engineer about modifications to the tuning procedure to facilitate the tuning process.

Context:

- Testing had been ongoing for over four hours, with only one emergency breakaway occurring after Test Event #1.
- No test guidance was created for the Test Director to leave the bridge during testing events (Ex: Lunch, Bathroom).
- Test guidance was hierarchically stacked and no clear lines of enforcement had been set to fix any inconsistencies within the guidelines and procedures. The main guidance the Test Director used was the Test Guidance for NRL Filter Testing and Software Update Tuning Procedure.
- Many of the personnel partaking in the test event, including the Test Director, System Analyst, and Software Engineer, had a large part in creating the test guidelines and memorandums.

Unsafe Decisions and Control Actions:

- Test Director was not present on the bridge at the time of the incident.

- Test Director allowed Test Event #18 occur after the unsuccessful completion of the same Test Event #2 in the Alpha Matrix.
- Test Director did not control all target-follow operation procedures in accordance with the Test Guidance for Software NRL Filter Testing, Target OSV – Follow OSV Test Plan, or the OSV Operations Manual.
- Test Director failed to communicate the parameters and objectives of each tuning/test run to the OSV Testing Crew during the test events.

Process Model Flaws:

- Test Director did not believe he needed to be on the bridge during all test events.
- Test Director did not believe the Test Guidance for Software NRL Filter Testing, Target OSV – Follow OSV Test Plan, or the OSV Operations Manual needed to be followed explicitly.

Flawed Process Model and Unsafe Control Actions

The Test Director is in charge of holding a pre-test safety brief with all participating personnel. It is unclear from the RCA&CA what information was actually shared during the pre-test brief. The outline for the safety brief is fairly vague, and only suggests discussion of the test documentation, potential hazards, breakaway procedures, and roles and responsibilities for the test participants. The Software Engineer, a key controller who had intimate knowledge of the parameter changes, was not required to give any safety related information during the brief.

The Target-Follow Software Tuning and Procedures instructs the Test Director to communicate the parameters and objectives of each tuning/test run to the OSV Crew and the Technical Team during testing. [**11**] It is unclear if the Test Director was present during the decision to continue to Test Event #18 after Test Event #17 failed. If he was present, test procedures dictated he had the authority to communicate any changes to the test/tuning objectives that resulted from unexpected DP System behavior when Dead Reckoning Mode was entered in Test Event #17. As noted by the original assumptions held by DP Software Engineering, the DP System was not expected to enter Dead Reckoning Mode. The only two safety barriers built into the test plan where starting testing at a higher lateral separation and having test runs listed in order of increasing difficulty. All safety margins were degraded prior to allowing Test Event #18 to occur. The specific test documentation regarding assigning responsibility to halt or skip test events is further analyzed in Section 3.9 Operations Management Controller Analysis.

The Test Director was not on the bridge at the time of the collision even though the test documentation assigned to the Test Director several safety-related responsibilities that would have required him to be present during all test events. The Target OSV – Follow OSV Test Plan assigned several pertinent responsibilities for the Test Director that could not be accomplished off the bridge. In particular, the Test Director was responsible for announcing the commencement and completion of each test run. The Test Director was also responsible for managing the sequence of test plan events, as well as overall observation of the exercise events. Within this Test Plan was a section with the example Alpha and Bravo Test Matrices. A criterion to carry out the Bravo Test Matrix was, "successful completion of Event Alpha is a prerequisite to conducting Event Bravo and the Test Director must identify the minimum designated lateral separation distance established in Event Alpha." [**12**] However, this documentation was not directed to the actual test sequence used for the test event, rather, it was merely required for an example test sequence within the Test Plan.

After four hours of testing with minimal incidents, the Test Director did not believe his presence was necessary to enforce any safety related responsibilities assigned to him. In addition to the lack of documentation or policy related to minimum crew numbers for testing events, the Test Director believed taking a lunch break during testing was sanctioned. It is apparent from the RCA&CA that the test guidelines were not exacting procedures, but viewed as recommendations for test events. This sentiment was derived from the structure of how test documentation was given to the OSV Testing Team. Documentation was nested within other documentation, and several different documents assigned responsibility in various sections. This inconsistency created an environment where only parts were recognized as important, and over time, some safety requirements were no longer enforced.

Previous recommendations covered many off the issues regarding inconsistent and inadequate testing documentation. The following **recommendation** addresses the Test Director's flawed process model and unsafe control actions:

- Provide training and testing procedure policy for OSV Testing Team and Test Director prior to test event to ensure full understanding of safety related responsibilities and types of safety risk.

- Establish policy for transfer of shared safety related responsibility (ex: COMEX, recording time of test event).
- Update pre-test safety brief:
    - All testing documentation must available and physically present if enclosed in test plan.
    - Any changes to test documentation should be emphasized to OSV Crew, particularly if different from normal OSV operations.
    - Include safety brief from Software Engineer regarding specific test runs and parameter changes.
    - Communicate specific breakaway criteria relevant to test event.

3.9. Operations Management Controller Analysis

Analyzing the safety related responsibilities and component interactions within high level organizational control structure, shown in Figure 6, helps identify systemic issues that may have influenced the lower level controller actions. The main responsibility for the Engineering and Testing Development organization is to provide safety constraints, training manuals, operating requirements, and test plan guidance to the Operations Management. The main responsibility for the Operations Management organization is to approve and provide safety test plans to the OSV Crews. The Operations Management then determines maintenance priorities, management changes are formulated, and hazard analyses are reviewed.

3.9.1. Navy Programs Analysis

Safety Related Responsibilities:

- Approve Target Follow Software Tuning and Testing Procedures and Target OSV – Follow OSV Test Plan.
- Prepare and send NRL Filter Test Memo to Test Director.
- Ensure the overall safety of the OSV testing mission, including identification of hazards and safety risks.
- Request test plans, procedures, and guidance to be prepared by appropriate Engineering and Testing Development personnel.
- Approve and provide all relevant test documentation to OSV Testing Team.
- Ensure Test Director, OSV Technical Team, and all extra personnel assigned for testing duties are properly trained/briefed to conduct testing mission.
- Ensure OSV Manufacturer Management abides by all contractual obligations in regards to operations, manufacturing, and training requirements.

- Communicate with OSV Operations Management to promote safe operation and testing during Target OSV – Follow OSV trials.

Context:

- Target OSV – Follow OSV Test Plan lacked specific breakaway procedures and any pretest safety briefings prior to the 3 June 2014 accident. The Test Plan was updated to include specific breakaway procedures and pretest safety-briefing requirements. The Test Memo guidance was also instituted after the 3 June 2014 accident due to the lack of guidance.
- The NRL Filter software update was given priority after two previous incidents were directly linked to NRL Filter inadequacies. There was schedule urgency to fix these problems to ensure safety for overall OSV operations.

Unsafe Decisions and Control Actions:

- Did not conduct proper safety analysis prior to conducting OSV operations.
- Enclosed the Software Update Tuning Procedure in the test package for OSV Testing Team without a proper review.
- Did not assign responsibility for someone to ensure all test documentation approved by the Test Memo was current, relevant, and non-conflicting.
- Did not ensure controller within the Operational Management team approved Software Update Tuning Procedure before enclosing document in test package.
- Did not ensure a Target OSV – Follow OSV Test Plan, Test Guidance, and Software Update Tuning Procedures were consistent and relevant to each test event.
- Did not ensure frequency training requirement for OSV – OSV breakaway procedures were created and conducted prior to testing event.
- Did not provide adequate pre-test safety brief instructions for OSV Crew in test guidance.
- Did not provide adequate guidance to the OSV Testing Team on when to halt testing on over-restrictive NRL Filter parameters.
- No contingency plan or guidance was created for The OSV Testing Team to leave the bridge during testing events (Ex: Lunch, Bathroom).
- Inadequately defined roles and responsibilities within OSV Testing Team (responsibility overlap in clearing alarms)
- Inadequate test design criteria regarding actions of Target OSV (vessel was in incorrect DP System Mode throughout test event)

Process Model Flaws:

- Navy Programs did not understand how the previously identified problem with the Kalman filter affected the DP System's ability to recover from Dead Reckoning Mode.

- Navy Programs believed the test guidance was adequate and the specific tuning matrix runs were listed in order of increasing difficulty.
- Navy Programs did not fully understand the how specific NRL Filter parameter changes affected safety of the vessel.
- Navy Programs believed OSV Manufacturing Management was responsible for defining specific responsibly roles within OSV Crew.

3.9.2. OSV Operations Management Analysis

Safety Related Responsibilities:

- Approve Target Follow Software Tuning and Testing Procedures, Target OSV - Follow OSV Test Plan, and Test Guidance for Software NRL Filter Testing.
- Request for test plans, procedures, and guidance to be prepared by appropriate Engineering and Testing Development controllers.
- Appoint a Test Director for each target-follow tuning/testing operation.
- Review and approve vessel procedures, checklists, guidance, regulations, training, ect.

Context:

- OSV Operations Management approved all test documentation other than the Software Update Tuning Procedure. The Test Guidance for NRL Filter Testing that enclosed the software tuning procedures was approved, however, the enclosure referenced the incorrect version 2 that did not exist nor was used at the time.

Unsafe Decisions and Control Actions:

- Did not create frequency training requirement for OSV – OSV breakaway procedures.
- Provided inadequate oversight on test guidance and pre-testing safety brief procedures. Did not ensure all test documentation was consistent, understood, and followed by OSV Crew.

Process Model Flaws:

- Belief that all reviewed documentation was adequate for test event.

Inadequate and Inconsistent Test Guidance

Navy Programs had recently issued two test documentation procedural changes prior to the late July 2014 test event:

1. Update Target OSV – Follow OSV Test Plan to include specific OSV/SV breakaway procedures and briefing requirements.
2. Add test memorandum to standing Target OSV – Follow OSV Test Plan for each OSV test to occur.

These two changes were created to address an identified problem after the 3 June 2014 minor collision that the Target OSV – Follow OSV Test Plan lacked specific breakaway procedures and pretest safety briefing requirements. Both of these updates were inadequate in addressing documentation inconsistencies and safety oversight prior to the testing event.

The updated Target OSV - Follow OSV Test Plan introduced breakaway procedures, however, they were slightly different than the OSV Operations Manual the OSV Crew was accustomed to. Specifically, for breakaway procedures in the OSV Operations Manual one of the breakaway criteria was upon the loss of lock on both reference sensors. However, the updated Test Plan slightly altered this criterion to "upon loss of position data from both RSSs or the loss of position data from one RSS for an extended period of time." [**10**] The rest of the five breakaway criteria were identical for both documents. This slight change may have been issued to tailor the breakaway criteria to testing operations, but its inconsistency was not emphasized within the document.

A review of the chain of events listed in Section 3.2.1. Chain of Events shows that the two reference documents indicate two different breakaway criteria. At 18:52:05 the updated Target OSV – Follow OSV Test Plan would have dictated a breakaway. At this time the NRL Filter had eliminated the position data from all three RSSs and Dead Reckoning Mode was entered. The Follow OSV RSSs maintain their lock on the Target OSV even while in Dead Reckoning Mode. The data is continually sent to the NRL Filters in order to allow for recovery to Target-Follow Mode when any of the RSS data is sent within the NRL Filter's acceptable parameters. The RSS sensors eventually lose their lock on the Target OSV reflectors when the relative position inhibits reflection and collection of data. According to the OSV Operations Manual, it is when there is the loss of lock on both reference sensors that dictates a breakaway. The breakaway condition did not occur until 18:52:33 according to the OSV Operations Manual when the actual loss of the

lock on the sensors occurred. It is not clear that the DP System provides any feedback differentiating between an NRL Filter data rejection, and a loss of the lock on the RSSs.

The OSV Operations Manual's breakaway criteria were created to be applicable for normal OSV Operations; however, changes to the breakaway criteria may be necessary for testing operations. It is unclear from the RCA&CA if these discrepancies were recognized or addressed prior to the exercise. Either way, the OSV Testing Team followed neither the Target OSV- Follow OSV Test Plan nor the OSV Operations Manual breakaway criteria on the day of the accident. The Target OSV – Test OSV test plan instructed the breakaway procedures be covered during the safety meeting, however, it did not cover when a breakaway should be performed. It is apparent from the RCA&CA that the breakaway criteria did not match the operation conducted. Whenever Dead Reckoning Mode is entered, it is a result of a loss of position data from all RSSs, which means Dead Reckoning Mode is an immediate breakaway criterion event. However, it seems that the controllers only believed entering Dead Reckoning Mode for a certain amount of time was a breakaway event. This uncertain amount of time was never identified and covered in any test guidance.

The second recent procedural change of instituting a Test Memo prior to any Navy Programs instructed test event was also inadequate. As seen in Figure 13, the Test Memo was the final approval document from the Navy Programs head to the Test Director. This Test Memo effectively approved all enclosed and referenced test documents for use.

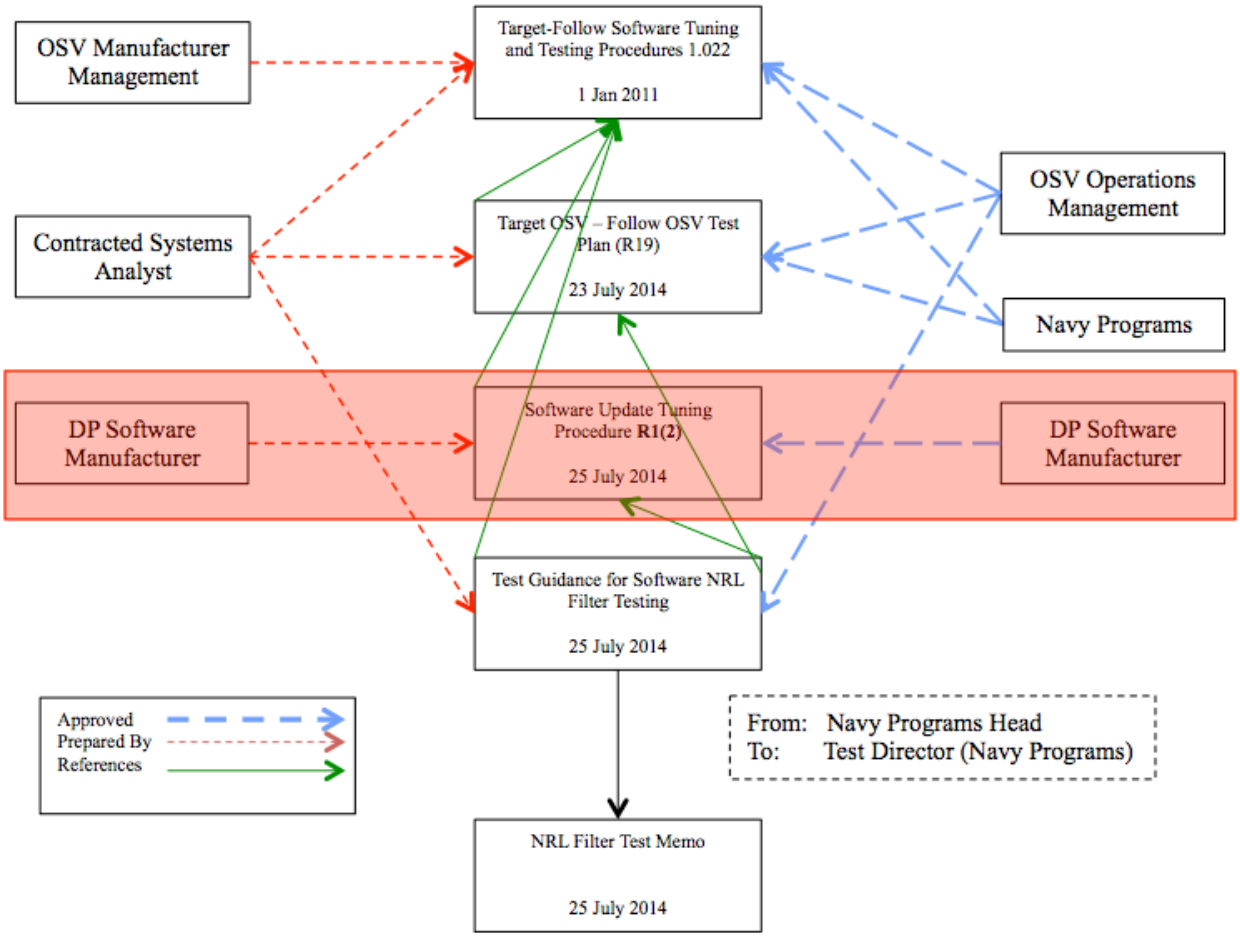

Figure 13: Test guidance documentation sent to OSV Testing Team

However, as Figure 13 illustrates, Operations Management reviewed and approved all documents except for the Software Update Tuning Procedure. This tuning procedure was created and approved by the DP Software Manufacturer. No formal responsibility was set up by the NRL Filter Test Memo to ensure all documents were previously approved prior to enclosure. There was a further problem where the Test Memo enclosed the Software Update Tuning Procedure Revision 2, when only Revision 1 was completed. Revision 2 of the tuning procedure was not produced until after the accident occurred. [**13**] There was no safety review process in place to find and correct this mismatch of document revisions.

Safety Review Responsibility Unassigned

Responsibility to ensure all documents were approved and consistent as a whole was not assigned by either Navy Programs or OSV Operations Management. The NRL Filter Test Memo,

referencing the Test Guidance for Software NRL Filter Testing, specifically stated "the test runs are listed in order of increasing difficulty and the easier runs should be executed first to ensure vessel performance before more difficult runs are attempted." [**13**] No responsibility was assigned to ensure this was met, primarily due to the lack of understanding on how each parameter affected vessel performance. Furthermore, no responsibility was assigned to ensure uniformity and consistency within all enclosed test documents. While each document was approved and considered safe for use as a stand-alone procedure, many of the documents were inconsistent as a whole. Additionally, each guiding document assigned different responsibilities to the OSV Testing Crew, possibly making it difficult to understand their full duties during a test. These inconsistences, ranging from different verbiage to different breakaway criteria, may have caused the OSV Testing Team to only follow whichever criteria they deemed significant at the time.

Another example of an inconsistent major requirement found within the Target OSV – Follow OSV Test Plan was the "successful completion of Event Alpha is a prerequisite to conducting Event Bravo." [**10**] This requirement referred to an example test plan. There was no similar requirement for the actual test events conducted in the late July 2014 test, and consequently, the requirement was not adhered to. Test Event #17 and #18 did not meet this prerequisite and would have been skipped had this requirement been applicable and properly enforced. It would be unreasonable to assume the OSV Testing Team would have taken the time to correlate the requirements of a test matrix example to the actual test events of the day. A safety review of responsibility was not specifically established with the goal of finding these inconsistences prior to testing operations.

Inadequate Feedback Channel

Inadequate feedback between the OSV Crew and the Operations Management may have influenced the inadequate and inconsistent test guidance. Feedback is necessary for the Operations Management to understand when guidance should be changed, particularly if it is deemed irrelevant or unnecessary. For example, the Test Director was given the responsibility to communicate the parameters and objectives of each tuning/test run to the OSV Crew and OSV Technical Team during testing. While it is understandable to have an overview of the objectives

and parameter changes of 32 Test Events during the pre-test safety brief, restating the objective prior to each event may not add any benefits in regards to safety. The Test Director did not follow this specific task, possibly because it was deemed unnecessary. A proper feedback channel to the Operations Management was not established to take note of these discrepancies and either change or reinforce their necessity. The Data Collection Team, as noted in Section 3.8.5, did not collect any comment sheets that could be used to communicate this type of feedback to Operations Management. Feedback channels must be enforced if the Operations Management strives for continual improvement outside of feedback after incidents occur.

Missing Hazard Analysis

Navy Programs relied on the Software Engineering simulation results as the only hazard analysis for OSV testing operations. The formal review, in the form of a Fault Tree Analysis and Probabilistic Risk Assessment only occurred after the OSV collision took place. However, assessments only analyzed normal OSV operations conducting escort missions with U.S. Navy Vessels and assumed all equipment and that the DP Systems were set up with correct parameters, calibrated and installed properly. This situation is distinct from OSV testing operations and must be analyzed beyond a simulation result. A proper hazard analysis focusing on the software update and all component interactions would be necessary to find problems like the unsafe component interaction between the DP System and NRL Filter as described in Section 3.8.2.

The following **recommendations** address the identified inadequate feedback channels, missing hazard analysis, unassigned responsibility, and inconsistent test guidance:

- Establish an operations process safety organization to provide oversight that is responsible for:
    - Enforcing safety policy.
    - Conducting a hazard analysis prior to future physical and software testing.
    - Conducting a hazard analysis for any changes to organizational and safety control structure.
    - Ensuring all hazards identified in previous system safety assessments, feedback reports, and accident reports are addressed and tracked for completeness.
    - Ensuring unaddressed hazards are identified and mitigated in the test development process. System changes must be understood with respect to previously identified hazards.

- Establishing a controller responsible for:
  - Ensuring all Engineering and Testing Development test documentation is reviewed by a proper Operations Management controller. If new test document is created by an organization within Operations Management, a separate controller is required review and approval.
  - Ensuring test documentation is approved and is consistent with all pertinent safety documentation and Engineering and Testing Development documentation. Inconsistencies between procedures, responsibilities, or general policies must be addressed prior to final approval. Any responsibilities assigned by later documentation must be checked with earlier enclosed documents (Ex: tuning procedure goes from safe trials to riskier trials).
  - Ensuring all language and references are clear and consistent throughout test documents.

- Ensuring all documents reference the correct, available, and reviewed document revisions.
- Creating data collection system to track leading indicators in unplanned or unsafe OSV activity.

3.10. Engineering and Testing Development Controller Analysis

3.10.1. OSV Manufacturer Management Analysis

Safety Related Responsibilities:

- Co-Create Target-Follow Software Tuning and Testing Procedures.
- Create and provide Safe Operating Procedures for OSV Crew.
- Ensure all up-to-date OSV procedures, checklists, and regulations are available to the OSV Crew during all operations.
- Ensure OSVs meet safety requirements and specifications as outlined in contract.
- Ensure all DP Operators, OSV Masters, and OSV Bridge Officers have required training, qualifications, and certifications to perform assigned duties.
- Communicate with DP Software Engineering and System Analyst Contractor about any material/engineering problem reports from OSV Operations.
- Send relevant vessel safety problem reports to Operations Management that arise during OSV operations.

Context:

- The DP Operators receive training to perform breakaways for normal OSV operational use, not for testing events. Due to the design of U.S. Navy Vessels, the OSV Manufacturer Management train DP Operators to use minimal rudder.

- OSV Manufacturer Management minimizes breakaway training, because each breakaway is inherently dangerous. It is the OSV Manufacturer Management's duty to keep the OSVs safe in operations and in training.

Unsafe Decisions and Control Actions:

- Manufactured vessel with unsafe interactions between control stations, and feedback for DP Operators.
- Provided inadequate procedures/training for DP Operators in regards to forward/aft thrust control.
- Provided inadequate guidance for minimum number of OSV Crew on bridge specifically for test events.
- Did not provide operation guidance or a contingency plan for crew watch transfers or meals.
- Inadequately defined roles and responsibilities for who should clear the DP System alarms.
- Provided insufficient checklists/procedures for primary set up of Data Logger.
- Provided inadequate equipment for data logging purposes.
- Provided inadequate test guidance Target OSV's operation mode during test events.

Process Model Flaws:

- Believed minimum crew guidance only was necessary for locations of operations, and not necessary for testing events.
- Did not recognize testing events as high-risk events.
- Believed test guidance provided to Operations Management and OSV Crew was adequate for safe operations.

3.10.2. Systems Analyst Contractors

Safety Related Responsibilities:

- Co-Create Target-Follow Software Tuning and Test Procedures.
- Create Target OSV-Follow OSV Test Plan, and Test Guidance for Software NRL Filter Testing.

Context:

- Systems Analyst Contractors was founded to primarily work on Navy Programs projects. The group is a major provider of technical support, planning and analysis, and operations management for the OSV/OSV program.

Unsafe Decisions and Control Actions:

- Created test documentation inconsistent with OSV Operations Manual.

Process Model Flaws:

- Believed test documentation did not need consistent language, and assigning multiple controllers for the same responsibility was acceptable.

3.10.3. DP Software Engineering Analysis

Safety Related Responsibilities:

- Create Software Update Tuning Procedure.
- Approve Software Update Tuning Procedure.
- Design procedure and outline comprehensive series of tests to tune and calibrate the DP System for the NRL Filter update.
- Conduct simulation testing prior to at-sea testing for any modifications to the DP System software to determine potential risks for event.

Context:

- Two previous accidents attributed the insufficient Noise Rejection Logic filter as a significant causal factor.
- Time pressures for the completed software update necessitated a comprehensive set of test data was collected to reinforce estimated parameter choices.

Unsafe Decisions and Control Actions:

- Determined risk solely based on lateral distance.
- Risk of entering Dead Reckoning Mode during testing labeled low probability risk (Based on simulation data).
- Did not create test runs in order of increasing difficulty, with the easier runs executed first.
- Did not fully analyze how past issues with the Kalman filter could affect an NRL Filter induced Dead Reckoning Mode.

Process Model Flaws:

- Believed the simulation testing, conducted prior to as sea trials, adequately modeled the parameter changes. Believed the simulation would alert them if Reference Sensor Systems would be rejected at a high enough frequency to have a serious risk of entering Dead Reckoning Mode.
- Did not believe specific parameter changes needed to be accounted for in risk determination with regards to test event order.
- Believed starting at a high lateral separation first, and then closing distance would meet any safety criteria.

- DP Software Engineering did not expect the Kalman filter resetting the estimated relative OSV velocity to zero upon entering Dead Reckoning Mode would affect the DP System's ability to recover from Dead Reckoning Mode.

Talking Points:

- The resetting to zero issue had already been identified and was scheduled to change. However, there was not a risk analysis done prior to the tuning event showing how past issues could affect future missions.

Unsafe OSV System Design

The OSV Manufacturer Management is responsible for providing all equipment on the OSVs for testing operations. No components failed on the OSV the day of the accident, and every component acted in accordance with its design and operator inputs. However, there were equipment design inadequacies that were noted in the subsequent RCA&CA investigation.

The first main equipment inadequacy was made apparent after the Data Logger failed to record the correct test data. The Software Engineer, who set up the particularly complex system, was not provided adequate documentation to ensure proper set up. The Software Engineer used the incorrect IP address, which read data from the backup DP Control Processor and not the Master Control Processor. The mistake revealed the first main equipment inadequacy: the Data Logger is only able to collect data from one control station at a time. This limitation hinders any future investigations surrounding situations that involve the backup DP Control Processor. It can be reasonably understood that if the OSV is forced to use the backup DP Control Processor, an investigation team will need the data regarding the incident. Additionally, the Data Logger is only capable of recording the feedback of the system instead of the DP Operator inputs when in Full Manual Mode. This is a severe limitation to the data collected by the investigation team.

The second main equipment inadequacy is the resolution of the sample rate between the data logger and the DP Control Processor operating rate do not match. The DP Control Processor operates at an updated velocity estimate of 4hz but the data logger is limited to a 1hz sampling rate. Thus, NRL alarms may be triggered and cleared between data logger samples and Reference Sensor System measurements. The discrepancy between sample rates makes NRL alarms that are triggered and cleared consecutively difficult to analyze post-operation.

Unsafe Test Plan

The DP Software Engineering organization provided a test matrix that started with the most restrictive parameters at the beginning of the test. The DP Software Engineering organization was not given direct instructions to take parameter changes into account when creating a test matrix, so only lateral separation was used as a safety measure when the changing parameters affect on safety should have also been included. Additionally, as noted previously, there was no official review process by the Operations Management team to provide feedback on the Software Update Tuning Procedure.

Missing Hazard Analysis

An unsafe interaction between the Kalman Filter and the NRL Filter as noted in Section 3.8.2 occurred during Test Event #18. DP Software Engineering had the technical understanding of the velocity and error rates in Dead Reckoning Mode, but it did not fully understand how a NRL rejection affected the DP System's ability to recover from Dead Reckoning Mode. It is not clear that an internal safety review process of the software update would have altered the DP Software Engineering organization's test plan. However, it is clear that it was impossible to understand potential interaction effects if no review process takes place or is attempted. Because the Software Engineering Organization was the only controller that could have understood the technical details of this unsafe interaction, a safety review process within the Software Engineering Organization would be necessary to prevent software related unsafe interactions. The Operations Management only required a simulation test prior to operations and did not require a full hazard analysis. Simulation is unlikely to identify the unsafe interactions. Additionally, communication and coordination between the DP Software Engineering organization and Operations Management regarding the tracking of software issues is unclear from the RCA&CA.

The following **recommendations** address the identified unsafe test plan and unsafe system design:

- Data recorders must provide relevant feedback to controller if setup incorrectly (recording from incorrect DP Control Processor).

- Data recorders must track from all DP System consoles.
- Data Logger resolution, sampling rates, and sync time must match DP Control Processor.
- Data recorders must record all operator-inputted commands, instead of only control system and vessel feedback.
- Full hazard analysis, beyond simulation, must be completed prior to any software modifications to the OSV systems.
- All feedback from the OSV operations to the Engineering and Testing Development must be communicated to and tracked by the Operations Management.
    - Issues identified through this feedback channel must be addressed and mitigated prior to any future testing.

3.11. Overall Coordination and Communication

Inadequate or missing coordination and communication between controllers exacerbate unsafe behavior. Communication includes both the exchange of information and direct feedback. Coordination and communication become paramount in operations that involve multiple controllers where unexpected side effects of decisions occur when control actions are inadequately coordinated. Figure 14 shows an example of multiple controllers controlling a process with common boundaries.

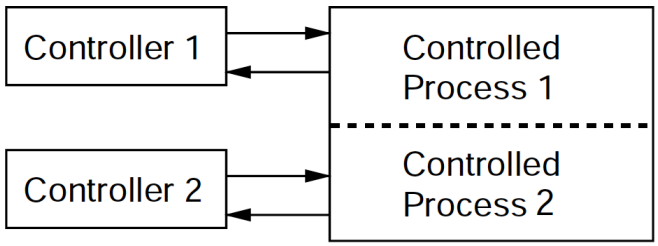

Figure 14: Example of a boundary area

Operations Management and OSV Manufacturer Management both controlled procedures given to the OSV Testing Crew safe operations. Conflicting instructions inputted to a controlled process with poorly defined boundary areas often cause unintended side affects. For example, both Operations Management and OSV Manufacturer Management were inputting safety responsibilities and test guidance where the boundary areas were ill defined. Communication and coordination is key when boundary areas exist to prevent unsafe consequences, like inconsistent breakaway criteria. Both the controllers inputting commands to a controlled process with a

boundary area as well as those controllers operating within the boundary area must have clear communication and coordination to prevent problems. One example of missing coordination and communication is how the OSV Manufacturer Management provide the OSV Crew an independent Safe Operations Manual (SOM). The SOM is the OSV Manufacturer company operations manual for vessel operations that include safety, operations, safety work practices, maintenance, and vessel security. This document is not shared with Navy Programs due to company confidentiality.

Feedback Channels

It is important for the controllers to communicate when the controlled process is providing pertinent information over different feedback channels. OSV Manufacturer Management and Operations Management both receive inadequate feedback from the OSV operations. Furthermore, the feedback from OSV operations is not adequately organized or communicated between the two controllers for operation planning purposes. OSV Manufacturer Management receives feedback in the form of the Job Safety Analysis, Master Comment sheets, personal evaluation records, and Data Logger records. This feedback channel is normally always fulfilled because it occurs for all OSV operations, not just testing events. Also, this feedback contains information that updates the OSV Crew's frequency training records. While there is a feedback channel for any component failures to be reported for fixes, a feedback channel is missing for any material problems or operational issues that do not have any apparent fixes. For example, if an incident does not arise when the DP Operator continues to accidently overrate a barrel switch or if the software freezes momentarily during certain DP inputs, there is no official feedback to OSV Manufacturing Management. If this type of feedback is received, there is no formal problem list that is tracked and communicated with the Operations Management.

The Operations Management receives feedback from testing operations in the form of Data Logger data, OSV Mission Data Sheet, and comment sheets that the OSV Masters and Test Director fill out. These comment sheets are often not filled out, preventing the Operations Management controllers from making continual updates or alterations to test guidance unless an incident or accident occurs.

Coordination and Communication

Information from both feedback channels would enable the Operations Management controllers and the OSV Operations Management controllers to keep track of any potential changes for future missions. For example, if responsibility uncertainty occurred between multiple controllers on who is supposed to cancel DP System alarms, or if test documents were unclear or uncertain, the high level controllers could institute change. As noted in the analysis of the higher levels of the control structure, some controllers had multiple responsibilities that were shared with other controllers. Any changes to procedures or responsibility, like a breakaway criteria provided by the Operations Management that differed from the OSV Manufacturer Management, must be properly coordinated to prevent responsibility or procedural uncertainty in the lower levels. Coordination and communication, prior to any feedback, can also avoid problems within the lower level boundary areas.

3.12. Dynamics and Changes in System

Systems naturally migrate towards higher states of risk. Dr. Leveson, in *Safeware: System Safety and Computers,* explains that both planned changes and unplanned changes may shift a system into a hazardous state. Intentional system changes involving both physical and safety control structure changes, without proper safety evaluation, are common factors in accidents. [**14**] Unplanned changes often move systems toward states of higher risk and are less straightforward to address unless properly detected and mitigated. Unplanned changes often occur when people naturally attempt to optimize their performance over time to meet a variety of system goals. Both planned and unplanned changes to the physical and safety control structure occurred within the OSV operation and ultimately lead the system to a higher state of risk.

The software update to the NRL Filter was a planned change intended to make the automated track-follow system more robust. No controller completed a formal risk analysis prior to the tuning or software update, or any previous tests. Safety unknowns are inherent in all testing events. However, it is imperative that a review process is completed to understand and mitigate unsafe component interactions. Another planned change occurred to the safety control structure prior to the late July 2014 test event. New test memorandum was required prior to the Test Director receiving the test plans and guidance. These documents proved not to actually integrate

or review all the enclosed documentation and likely provided a false sense of safety for the OSV Test Crew. Additionally, all OSV Operation Manuals provided by OSV Manufacturing Management and cited by Operations Management were part of a dynamic documentation system. In particular, the Target-Follow Software Tuning and Testing Procedures were nested within the larger encompassing OSV Operation Manual. Each section, like the testing procedures, was individually updated and approved for use. This was a planned documentation method. The nested documentation allowed specific procedures to be modified during the testing phases and prevented the OSV Manufacturing Management from publishing the entire OSV Operations Manual every time an alteration within a single section occurred. However, these sections all referenced other sections within the larger operating manual. This leads to older documentation, like the 2011 approved Target-Follow Software and Testing Procedures, to reference the updated 2013 sections that did not exist at the time. Each section was approved individually, but no review process was held for the system as a whole.

Unplanned changes were evident on the day of the test event. Over a span of four hours with minimal incidents, the controllers became complacent and ceased to rely on their documented responsibilities. Dead Reckoning Mode occurred in Test Event #1 and a breakaway was performed immediately. The OSV Testing Crew was still highly vigilant and canceled Test Event #2. However, by the time Test Event #17 and Test Event #18 occurred, key controllers were off deck and responsibilities in the bridge were being reassigned. The DP Operator had experienced multiple alarms, which were being cleared by another controller, and the DP System automatically recovered from Dead Reckoning Mode preceding the accident. This delayed the DP Operator's response to what was originally an immediate breakaway event. The migration toward riskier behavior was not detected or mitigated.

3.13. Generate Recommendations

Safety constraints and requirements are generated to address unsafe symptoms found by analyzing the relevant OSV controllers. The CAST analysis leads to the following compiled restraints/requirements to address the inadequacies in the safety control structure:

OSV Dynamic Positioning System

1. OSV control station must give appropriate feedback and alarms to DP Controller if any controls are inputted from aft control panels when OSV is in Full Manual Mode.
2. OSV control station must provide feedback to DP Operator indicating which manual controls are providing commands to main engines, rudders, tunnel thruster, and bow rotors.
3. Any abnormal controller inputs must be easily distinguishable and prevented.
    a. Over rotation of barrel switch must be prevented or an alarm must give proper feedback to controller.
    b. Control Station button design should be resized / further differentiated due to its high level of importance and high frequency of use.
4. DP System must automatically transfer thruster control to forward control station.
    a. If transfer does not occur within (x) seconds, feedback must be given to DP Operator.
5. DP System must give time based feedback and alarms to DP Controller for time in Dead Reckoning Mode.
6. Kalman Filter must freeze relative velocity instead of resetting relative velocity to zero upon DP System entering Dead Reckoning Mode.
7. Data recorders provide relevant feedback to controller if setup incorrectly (recording from incorrect DP Control Processor).
8. Data recorders must track from all DP System consoles.
9. Data Logger resolution, sampling rates, and sync time must match DP Control Processor.
10. Data recorders must record all operator-inputted commands, instead of only control system and vessel feedback.
11. DP System must have usable interface to transition from Target-Follow Mode to DP Manual Mode for breakaway scenarios.
12. Manual thruster controls, both forward and aft, must be set to neutral prior to all DP System controlled operations.
13. OSV must provide feedback, independent from the DP System, to the OSV Crew alerting of the loss of separation from a surrounding vessel, external object, or seafloor.

Operations Management

1. Establish an operations process safety organization to provide oversight that is responsible for:
    a. Enforcing safety policy.
    b. Conducting a hazard analysis prior to physical and software testing.
    c. Conducting a hazard analysis for any changes to organizational and safety control structure.
    d. Ensuring all hazards identified in previous system safety assessments, feedback reports, and accident reports are addressed and tracked for completeness.
        i. Corrective actions identified in a previous accident analyses must not completed prior to the future test events.
    e. Ensuring unaddressed hazards are identified and mitigated in the test development process. System changes must be understood with respect to previously identified hazards.
    f. Establishing a controller responsible for:
        i. Ensuring all Engineering and Testing Development test documentation is reviewed by a proper Operations Management controller. If new test document is created by an organization within Operations Management, a separate controller is required review and approval.
        ii. Ensuring test documentation is approved and is consistent with all pertinent safety documentation and Engineering and Testing Development documentation. Inconsistencies between procedures, responsibilities, or general policies must be addressed prior to final approval. Any responsibilities assigned by later documentation must be checked with earlier enclosed documents. (Ex: tuning procedure goes from safe trials to riskier trials)
        iii. Ensuring all language and references are clear and consistent throughout test documents.
        iv. Ensuring all documents reference the correct, available, and reviewed document revisions.
    g. Creating relevant testing procedures to specific test events.
        i. Establish specific breakaway criteria relevant to test event.
    h. If some portions of test documentation are designed as guidelines meant to be flexible, these portions must be identified. Similarly, safety procedures designed not to be flexible should be identified.
    i. Creating system to track leading indicators in unplanned or unsafe OSV activity.
    j. Provide training and testing procedure policy for OSV Testing Team and Test Director prior to test event to ensure full understanding of safety related responsibilities and types of safety risk.

i. Establish policy for transfer of shared safety related responsibility (ex: COMEX, recording time of test event).

2. Update pre-test safety brief:
    a. All testing documentation must available and physically present if enclosed in test plan.
    b. Any changes to test documentation should be emphasized to OSV Crew, particularly if different from normal OSV operations.
    c. Include safety brief from Software Engineer regarding specific test runs and parameter changes.
    d. Communicate specific breakaway criteria relevant to test event.
        i. If time in Dead Reckoning Mode is a breakaway event, the safety responsibility to keep track of time must be assigned to controller.
3. Establish an effective feedback channel between the OSV Testing Team and Operations Management:
    a. Feedback back to reporters regarding any updates. Information must not go into "black hole."
    b. Establish responsibility to ensure mandatory feedback is collected.
    c. Review feedback form. Ensure form facilitates sharing all safety information (ex: any slips or mistakes occurred that did not result in accident.)
4. Improve safety coordination and communication channels to Engineering and Testing Development controllers:
    a. Communicate any test document changes that are different than normal operating procedures.
    b. Communicate any feedback received from the OSV-Operations Management feedback channel.
    c. Establish a communication channel between DP Software Engineer and Operations Management. Both controllers must fully understand any updates or changes to DP Software. Possible unsafe interactions from updated software should be communicated prior to test event.
    d. Establish hierarchy or ultimate authority for controllers with shared safety related responsibility.
    e. Establish training requirements necessary for testing operations.

Engineering and Testing Development

1. Review all nested documentation for inconsistencies within version dates.
2. Provide safety review of all referenced or encoded nested documentation for every section update.
3. Provide operation policy / documentation regarding:

a. Minimum number and type of OSV Testing Team on bridge during test events.

b. Establish policy for crew transfer and temporary crew absence from bridge.

c. Establish responsibility for Bridge Officer to watch lateral separation between Target OSV and Follow OSV in all testing maneuvers less than (x) feet.

    i. Bridge Officer must watch lateral separation between Target OSV and Follow OSV whenever the OSV is using DP Manual Mode or Full Manual Mode.

    ii. Bridge Officer must communicate with DP Operator whenever vessels are not maneuvering in accordance with guidelines, or required lateral separation is violated.

d. Establish policy to prevent DP Operators obstruction of view from Target OSV within bridge. For example, no personnel should be between the DP Operator and the Target OSV during any test event.

e. Provide procedures for transfer of shared safety related responsibility (ex: clearing DP alarms).

f. Provide procedures for Follow OSV on actions in testing operations (ex: Target OSV should be in Transit Mode, not Hold Heading Mode).

g. Provide specific and detailed Data Logger set up procedures.

h. Independent check of proper setup of the Data Logger must be conducted prior to tuning and testing operations.

i. Establish training requirements for OSV testing specific maneuvering.

4. Establish an effective feedback channel between the OSV Crew and Engineering and Testing Development:

    a. Provide feedback back to reporters regarding any updates. Information must not go into “black hole.”

    b. Review feedback form. Ensure form facilitates sharing all safety information (ex: any slips or mistakes occurred that did not result in accident.)

        i. Establish periodic feedback meetings with OSV Masters and DP Operators regarding physical system or operational problems experienced in OSV operations.

    c. Ensure reporting system is non-punitive. Reward reporting if possible.

5. Identify and compile slips, lapses, and mistakes regarding control inputs to DP System and manual control panel.

    a. Ensure appropriate feedback regarding system mode/state is available to DP Operator for incorrect control inputs.

    b. Install passive or active constraints to entering abnormal control modes. Particularly if they have been identified as common in the review processes.

6. Improve safety coordination and communication channels to Operations Management:

a. Communicate any test documentation changes that are different than normal operating procedures.
b. Communicate any feedback received from the OSV-Engineering Testing and Development feedback channel.
c. Communicate any hazards identified from independent system assessments.
d. Establish hierarchy or ultimate authority for controllers with shared safety related responsibility.

4. RCA&CA and CAST Comparison

4.1. Root Cause Analysis and Corrective Actions

Navy Programs led a thorough accident investigation after the late July 2014 collision. A stakeholder team was formed after the accident to conduct a RCA&CA in order to identify and implement immediate corrective actions, as well as identify short and long term corrective actions. Stakeholders included representatives from DP Software Engineering, Systems Analyst Contractor, OSV Manufacturer Management, Navy Programs, and OSV Operations Management. All future NRL Filter tuning procedures were put on hold until immediate and short-term corrective actions were identified and completed.

The stakeholders validated the three immediate actions post-incident: [**15**]

1. The NRL tuning procedure testing was secured.
2. Damage assessments were conducted and both the Target OSV and Follow OSV were cleared for mission operations.
3. Tactical software currently in use for operations was restored for the DP System on the Target OSV

The stakeholder team decided no further immediate actions were necessary.

The RCA&CA team convened three times between the accident in July 2014 and the final report approval on 29 Oct 2014. Two of the stakeholders, DP Software Engineering and OSV Manufacturer Management, concurrently conducted independent investigations and produced independent reports. These reports were made available during the RCA&CA processes and used when determining root causes and corrective actions. The stakeholder investigation team analyzed the recorded sensor data from both the Target OSV and Follow OSV to construct a detailed timeline of events leading to the collision.

The stakeholders conducted a thorough investigation following the four phases of Preparation, Data Collection, Assessment, and Corrective Action. Utilizing the “5 Whys” and the Root Cause Mapping Methods, the RCA&CA investigation team identified five specific problems as listed in Table 5.

The team noted that two specific problems, Problem 1 and Problem 2, were significant and "directly led to the minor collision and rise above the others with respect to importance / severity." [**15**]

#	Problem	Root Cause
1	There was a delay by the Follow OSV's DPO to fully implement the OSV breakaway procedure. The total time from the DP System entering DR mode until the vessel was in a full breakaway posture with thrust applied from both the bow and stern tunnel thrusters was 35 seconds.	Lack of experience, plan/task not properly briefed
		Inadequate design criteria
		Watch bills do not support the evolution
2	While in Dead Reckoning mode, the estimated relative velocity/rotation rate between the Follow OSV and the Target OSV are reset to zero, resulting in higher estimated velocity error rates and difficulty in recovering from a NRL rejection if significant relative motion between the vessels exists.	Inadequate design criteria
		Lack of Experience, Plan/task not properly briefed
3	Although within the Master's discretion, during the OSV breakaway procedure, the Follow OSV's DPO did not use available rudders to minimize the closure rate toward the target vessel.	Lack of Proficiency
4	The NRL tuning procedure was not sequenced to test less restrictive (position and heading) parameters first which would have reduced the risk of entering DR mode and meeting a criteria for OSV breakaway.	Lack of questioning attitude
		Lack of coordination between teams/Organizational culture
5	DP logger setup not optimal, and does not record both DP consoles. Reconstruction in the event of Master computer malfunctions would be difficult.	Inadequate documentation
		Inadequate design criteria

Table 5: Accident Problem Identification and Root Causes

The RCA&CA team identified high-level overarching themes that were used to aid the creation of corrective actions.

- Human Interface Delays: Personnel misconceptions, pre-breakaway setup
- Management Failures: Testing procedure understanding, watch bill adequacy, sense of urgency

4.2. RCA&CA and CAST Comparison

The problems identified by the investigation team are mapped to the corresponding CAST safety control structure in Table 6.

Issue Identified	Corresponding CAST Component
There was a delay by the Follow OSV DPO to fully implement the OSV breakaway procedure. The total time from the DP System entering DR mode until the vessel was in a full breakaway posture with thrust applied from both the bow and stern tunnel thrusters was 35 seconds.	OSV Operations/Navy Programs➔ Offshore Supply Vessel(s) DP System (auto) ➔ OSV Crew Control Subsystems ➔ OSV Crew
While in DR mode, the estimated relative velocity/rotation rate between the following vessel and the target vessel are reset to zero, resulting in higher estimated velocity error rates and difficulty in recovering from a NRL rejection if significant relative motion between the vessels exists.	OSV Operations/Navy Programs➔ DP Software Engineering OSV Operations/Navy Programs➔ Offshore Supply Vessel(s) DP System (auto) ➔ OSV Crew
Although within the Master's discretion, during the OSV breakaway procedure, the Follow Vessel DPO did not use available rudders to minimize the closure rate toward the target vessel.	OSV Operations/Navy Programs➔ OSV Manufacturer Management OSV Manufacturer Management ➔ OSV Crew
The NRL tuning procedure was not sequenced to test less restrictive (position and heading) parameters first which would have reduced the risk of entering DR mode and meeting a criteria for OSV breakaway.	OSV Operations/Navy Programs➔ DP Software Engineering Navy Programs and DP Software Engineering Communication
DP logger setup not optimal, and does not record both DP consoles. Reconstruction in the event of Master computer malfunctions would be difficult.	OSV Operations/Navy Programs ➔ OSV Crew DP System (auto) ➔ OSV Crew

Table 6: RCA&CA Problems mapped to Corresponding CAST Component

The full list of corrective actions is listed in Appendix B. The CAST recommendations include all of the identified issues and most of the subsequent corrective actions listed in the RCA&CA.

However, some of the corrective actions are not supported by the CAST analysis. These specific corrective actions are detailed below:

Corrective Action 2.A.1: *Until the Kalman filter is fixed, breakaway should be performed if a shift to Dead Reckoning occurs. Update NRL tuning procedure to add precaution associated with Kalman filter Dead Reckoning mode recovery effect and add a safety parameter in tuning procedure.*

This corrective action indicates the safety organization does not view Dead Reckoning Mode as a breakaway event. The problem with an over-delayed breakaway was not singular to the Kalman Filter unsafe interaction with the DP System's ability to recover from Dead Reckoning Mode. The problem with the delayed breakaway is the lack of properly enforced safety constraints. Allowing the vessel to stay in Dead Reckoning Mode violates the current breakaway criteria as described in Target OSV – Follow OSV Test Plan Revision 19. If this Test Plan changes to include a certain amount of time the vessel is allowed to be in Dead Reckoning mode, as this corrective action suggests, then a specific time limit must be indicated. A controller must be in charge of keeping track of the time in Dead Reckoning Mode. A proper feedback channel must be created to notify the DP Operator when the time threshold is broken.

The investigation team did a thorough root cause analysis of why the breakaway was delayed 9 seconds by the DP Operator. The investigation concluded the reason for the delay was [**15**]:

> Because in-situ environmental noise conditions were greater than predicted conditions, the stating NRL filter heading and position parameters chosen for this test, which were also too restrictive, resulted in multiple alarming conditions of reference sensors. The continued acknowledgement and clearing of individual Reference Sensor System alarms decreased DP Operator sensitivity to the loss of all reference sensor inputs. Additionally, there was a lack of experience among DP Operators and participating personnel that recovery from an NRL rejection could potentially occur and execution of a breakaway could be briefly delayed if the DP System recovered. The combination of these factors delayed the DP Operators actions to transition the DP System to manual mode.

This explanation indicates that the participating personnel would make the decision on when a breakaway could occur on the day of testing. As noted in the STAMP Model overview, hazards must be first identified at the system level, and then safety constraints may be constructed top down through the hierarchical safety control structure. The safety constraints set by Operations Management regarding a breakaway were not being enforced. It is clear that the DP Operator in this test event was not the only one with a flawed process model of when to breakaway.

Three months after this incident, during a normal OSV operation with a U.S. Navy Vessel, the OSV's DP System entered Dead Reckoning Mode. It took the DP Operator 8 seconds to breakaway while in Dead Reckoning Mode. This incident conflicts with the RCA&CA explanation for the DP Operator delay, as OSV in this incident was using operational software, and none of the conditions listed by the RCA&CA team were present. The delay, as noted by the CAST analysis in Section 3.8.3, was a result of inadequate feedback, unassigned responsibility, and unenforced safety constraints on the DP Operator.

Corrective Action 1.C.1: *OSV Manufacturer Management codify procedure to set up the aft control station pre-breakaway thrust positions in addition to the forward station.*

This corrective action was generated to address the delay in shifting the tunnel thruster control from the aft control station to the forward control station. If the problem is framed by the idea that the Follow OSV was not producing thrust to push away from the Target OSV in a breakaway scenario, then this corrective action makes sense. By setting up both the forward and aft thrust position to immediately push away, even if the Control Station button is not pushed and the aft station controls the thrusters, the Follow OSV will still push away from the Target OSV.

While the corrective action makes sense under the concept of the Root Cause Analysis, it contradicts the findings of the CAST analysis. The CAST analysis found that the DP Operator's process model of the OSV Actuators was not being properly updated due to inadequate feedback. The lack of feedback between the OSV Actuators and the DP Operator enabled the subsequent mode confusion. The DP Operator believed he was in control of the tunnel thrusters when, in fact, his control panel was not sending command inputs to the vessel for 26 seconds. This

corrective action does not fix this problem; rather, it may increase the problem of mode confusion. From this perspective, it is easy to see how mode confusion could be exacerbated with both control stations commanding the tunnel thrusters set to push away. If a similar scenario occurs, the DP Operator could breakaway and be under the impression that the Station Control button was pushed. The DP Operator would believe he or she was in command of all OSV Actuators. The resulting mode confusion would not be fixed because the OSV would initially react normally when switched to Full Manual Mode. However, in this scenario, the OSV could be pushed into surrounding objects such as another vessel, nearby structure, or into shallow water.

To avoid mode confusion, the aft station should be pre-set to neutral instead of pre-setting both thrusters to push away. In this scenario, there would be additional feedback from the thrusters that they were being improperly controlled. The investigation team labeled this problem as inadequate design criteria. The Root Cause Analysis did not uncover the reason why the DP Operator chose the actions given the available feedback and environmental inputs.

Corrective Action 4.A.1: *Conduct a team review of the updated Software Update Tuning Procedure focusing on understanding of NRL parameter adjustments and risk to creating a condition requiring breakaway.*
Corrective Action 4.A.2: *Prior to in-situ modification of the test plan or parameters used during testing, add requirement to the tuning procedure that the Software Engineer will brief the Test Director and DP Operator on potential impacts to safety.*

These corrective actions were generated to address the root cause of "lack of a questioning attitude" as to why the NRL tuning procedure was set from most restrictive to less restrictive. The CAST analysis results support the idea that a team review should be conducted to understand the NRL parameter adjustments as proposed in Corrective Action 4.A.1. [**15**] However, a team review prior to in-situation parameter changes should not be the only time the test procedures are reviewed. The CAST analysis identified a missing formal review structure for all procedures and documents from the DP Software Engineering team to the Operations Management controllers. An official safety review process must be established between these

two controllers to prevent future accidents. A questioning attitude should not be relied upon to identify possible hazards and mitigate control actions.

Corrective Action 4.A.2 proposes a redundant documented responsibility for the Software Engineer to brief the Test Director and DP Operator on safety impacts to any in-situation modifications to the test plan. However, the Target-Follow Software Tuning and Testing Procedures already state, "Software Engineer shall inform the Officer of the Watch of the expected parametric change results. This will help the Officer of the Watch determine if a break away is necessary." [**11**] So, according to one applicable test document, the Software Engineer has the responsibility to inform the Officer of the Watch of all parametric changes, whether they are in-situ modifications to the parameters or if they are planned parameter changes. Corrective Action 4.A.2 adds redundant requirements to the test documentation. This corrective action would be unnecessary if all test plans, procedures, and documents were consistent and properly enforced.

It should also be noted that the Target-Follow Software Tuning and Testing Procedures use different and inconsistent language with the RCA&CA. Within these two documents alone, a single controller is referred to as the "Software Engineer," "Analyst," and "DP Software Analyst." These small inconsistencies between language and shared responsibility only further lead to an environment in the lower controlled levels where uncertainties exist as to which/what procedures to follow.

4.3. RCA&CA vs. CAST Discussion

RCA Missing Hold Heading

One problem with event chain models is the use of a direct or linear view of events to identify the root cause. The notion exists in the investigation that in order for a preceding event to occur, the linking condition must have been present for the subsequent event to occur. This leads to subjectivity in selecting which events are relevant, and subjectivity in selecting the chaining conditions.

During the investigation process of the July 2014 collision, the investigation team found that the Target OSV was in Hold Heading Mode at the time of the crash. Hold Heading Mode is meant to be used for OSVs at low speeds, whereas, the OSV should be in Transit Mode for higher speeds. The test events were conducted at speeds that dictated use of the OSV being in Transit Mode. According to the DP Software Engineering manual, Hold Heading Mode, "is used when the operator wants to automatically hold the vessel to a fixed heading… In this mode, the measured heading is compared to the commanded setpoint heading and thrusters are controlled to reduce the deviation between the commanded and measured heading." On the other hand, Transit Mode is described as "the DP automatically maintains the commanded heading. The operator may change the heading by entering a new heading setpoint. The vessel's course is adjusted by controlling the rudders." [**5**] While both modes were created to maintain an inputted heading, they achieve this goal differently. The difference is minor, but at higher speeds the OSV is less steady and stable in Hold Heading Mode when compared to Transit Mode.

The investigation team found this discrepancy but did not include it in the RCA&CA because it did not fit within the team's identified problems and subsequent event chains. It also did not qualify as a contributory cause because it didn't seemingly affect any events leading to the collision. Rather than asking why was the Target OSV in the incorrect mode, why did the DP Operator put it in the incorrect mode, where are the procedures that dictate which mode the DP Operator should use, or why this safety constraint was inadequately enforced, the discrepancy was not included in the final report. Upon further investigation, the direction to the Target OSV for which mode to use was not assigned in any documentation. A stipulation to operate the Target OSV in Transit Mode was added to all updated Test Guidance forms after the July 2014 collision.

The RCA&CA model limits the investigation teams to require direct causality relationships, making it difficult to incorporate nonlinear relationships. This restricts the investigation team's ability to understand and identify systemic factors. As noted by Dr. Leveson, "all models are abstractions; they simplify the thing being modeled by abstracting away what are assumed to be irrelevant details and focusing on the features of the phenomenon that are judged to be most

relevant." [**3**] Event-chain models limit the types of causality factors considered by forcing the investigation team to view an accident through direct causality.

Hindsight Bias:

Two instances of hindsight bias were present in the RCA&CA. As observed by Dr. Leveson, "after an accident, it is easy to see where people went wrong, what they should have done or not done, to judge people for missing a piece of information that turned out to be critical, and to see exactly the kind of harm that they should have foreseen or prevented." [**3**] It is critical that the investigation team avoid this psychological phenomenon. Hindsight bias inhibits understanding the underlying reasons why the operators made mistakes, and why it made sense at the time for them to make these mistakes.

The first case of hindsight bias was focused on the DP Operator:

> Minimal rudder was used to control closure rate throughout the duration of manual operation, which could have been used to limit both the closure rate and the turning moment applied from the aft tunnel thruster.

It should be noted that the collision occurred on Test Event #18. Directly prior to Test Event #17 the DP Operator successful completed a practice breakaway as required by the Target OSV – Follow OSV Test Plan.

The investigation team found the root cause for the lack of rudder use as a "lack of proficiency." The investigation team then recommended the short term recommendation to "conduct training on close quarter vessel maneuvering precautions," and the long-term recommendation to, "establish training requirements periodicity for OSV/OSV breakaway procedures." [**15**] The root cause is contradictory to the OSV Manufacturer Management investigation that found all DP Operators to be fully trained and certified for the late July 2014 test. The long-term recommendation to establish frequency training requirements was also identified in the 4 June 2014 accident report and was not yet completed. First, the hindsight bias allowed the investigation team to not look at the

relevant data presented to the DP Operator at the time of the breakaway event. Second, the investigation team did not go further to see why the current training regime was not adequate to match OSV – OSV operations. Third, the investigation team did not report on why the frequency training requirements were not completed prior to continuing OSV testing operations. The frequency training requirement was due by 31 October 2014, but Operations Management proceeded with the late July 2014 test. It is unclear if there is a policy that covers which corrective actions from previous accidents must be completed prior to future testing.

The second form of hindsight bias addressed the unsafe order of test events in the Software Update Tuning Procedure. The report stated [**15**]:

> If the sequence of tuning tests had been determined based on the risk of losing all reference sensor inputs, vice only lateral separation... as testing progressed and software parameters were lowered at a given lateral separation, the team would have anticipated and should have seen increased individual reference sensor alarm conditions…

The investigation report went further in justifying the importance of the Software Update Tuning Procedure [**15**]:

> Action to assign additional watch standers to handle alarms, suspend testing during meals or decide that the lower bound of the window had been achieved could have occurred before a breakaway criteria was met.

The report places high significance on the idea that the OSV Testing Team would have done all the right things had they seen the test progressing towards more alarms and anticipated when the test should stop. While the CAST analysis agrees the test matrix should have been created to include the parameter's effect on safety, this hindsight bias assumes many of the operators would have acted independently to safely control the situation. The operating manuals and test plans show that no requirements were set in place for any controller to assign additional watch standards, suspend testing during meals, or how to decide the lower bound of the window had

been achieved. This lack of assigned safety requirement of when to stop the testing is just as significant, if not more so, than the unsafe order of the test matrix.

Unchecked hindsight bias allowed the investigation team to avoid scrutinizing the social, organizational, and human components that led up to a condition where all safety mitigation efforts outlined in the Software Update Tuning Procedure were degraded. As noted by Dr. Leveson, "assumptions are made that operators will be trained to do the right things and that they will adapt to whatever design they are given. Sophisticated human factors and system analysis input is lacking, and when accidents inevitably result, they are blamed on the operators for not behaving the way the designers thought they would." [**3**] The investigation team identified the fact that the "lack of coordination between teams/organizational culture" was the root cause of the unsafe sequenced tuning procedures, however, little analysis was done on how the test was actually designed to end. [**15**]

The Test Guidance for 29 Software NRL Filter Testing signed by OSV Operations Management dictated the "test runs are listed in order of increasing difficulty and the easier runs should be executed first to ensure vessel performance before more difficult runs are attempted." [**13**] Before the test even started, it was already at a state of degraded safety as this requirement only too lateral separation into account rather than software parameter restrictiveness. Yet, by the time Test Event #18 started, even this final designed safety mitigation of starting at high lateral separation was lost. Test Event #2, which was the high lateral separation test correlating with Test Event #18, never occurred. Thus, both the safety margin of starting with an easier test run, and starting at higher lateral separation, had fully degraded by the collision event. Effectively, the most restrictive software parameter was tested for the first time at one of the closest lateral separations. Hindsight bias allowed for the oversimplification of causality as the investigation team started with the hazardous outcome and found the plausible causes working backwards. The direct causality view supported by root cause analysis only amplified this problem.

The RCA&CA goes further than most by looking at coordination and organizational culture, but without a systems-thinking framework that includes environmental and behavior shaping factors, it is difficult to push past symptoms implicit in the set of events leading to the accident. Blame

must be removed from the entire accident analysis process. Blame prevents an investigator from understanding why a decision was made, and provides little information needed to prevent future accidents.

5. CAST Assumptions Revisited

A chain of events model starts the analysis at the accident event and works backwards. The model deconstructs the steps leading to the accident to a sequence of mechanical or human failures. This model was formed with an assumption of simplicity that is no longer present in the complex technological system developed today. Systems viewed in the chain of events model often turn to redundancy as a failure prevention method. Redundancy frequently interjects additional complexity into the system, bringing more potential for failures to develop with increasingly unforeseen unsafe interactions. Designers of new complex technological systems often rely on automation as a safe alternative to manual systems. However, as Dr. Leveson articulates, "inadequate consideration is given to whether new, or maybe even worse, hazards are introduced by the automation system and how to prevent or minimize these new hazards." [**3**] The event-chain model's underlying assumptions fail to comprehensively consider the inherent complexity of these systems.

The seven new assumptions that lay the foundation behind the CAST model are revisited with respect to the analyzed accident in this thesis:

New Assumption 1: High reliability is neither necessary nor sufficient for safety.

- The OSV system analyzed had no component failures leading up to the accident. All issues with components occurred due to unsafe interactions between components. Redundancy within the system, with both a forward and aft control station, contributed to new hazards that were not properly mitigated in the design of the system.

New Assumption 2: Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.

- A chain of directly related events in this case did not cause the collision. One could comprehend the accident only by analyzing the entire sociotechnical system, from the operating management down to the feedback the controller received at the time of the

loss. Understanding the accident in this way can aid an investigation team in identifying changes that will prevent future accidents. As noted in the review of the RCA&CA, some generated corrective actions may not only miss some of the flaws in the system, but they may even exacerbate them. As discussed in the Section 4.3 CAST vs. RCA&CA Discussion, traditional event-chain models may exclude pertinent safety information discovered by the investigation team if it does not fit within the model.

New Assumption 3: Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.

- Probabilistic risk analysis is not the only way to assess and communicate safety and risk information. Viewing risk in this lens forces the investigation team to understand accidents only in terms of linear events. Focusing on component failures hinders the investigation team from understanding the component interactions and why the unsafe control actions occur.

New Assumption 4: Operator behavior is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.

- The DP Operator was fully certified and trained to handle the OSV's DP System. The feedback and environmental inputs were insufficient in updating the DP Operator's process model. The process model did not match the actual system controlled process, which resulted in unsafe control action generation. This mode confusion was a byproduct of the environment the DP Operator was working within. Simply making the pat recommendation to "train operators better" will not solve the problems that exist over the long term. We need to create technology that does not induce human error by being inconsistent, confusing and misleading.

New Assumption 5: Highly reliable software is not necessarily safe. Increasing software reliability or reducing implementation errors will have little impact of safety.

- All software in the OSV system acted in accordance with its design. The NRL Filter rejected all Reference Sensor Systems as designed with the inputted parameter changes. The Operations Management and the Engineering and Testing Development team did not understand possible unsafe interactions within the software. As a result, the accident became a byproduct of insufficient communication and the lack of a formal risk assessment. Reliability of the software had no effect on safety.

New Assumption 6: Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.

- Planned and unplanned changes occurred in the system leading up to the accident. This accident was not a chance simultaneous occurrence of random events. Appropriate controls were either missing, not enforced, or inadequately enforced. The control station design was inappropriate and multiple feedback channels were missing within the system. No leading indicators were used to identify the increasing risk within the system state prior to or during operations.

New Assumption 7: Blame is the enemy of safety. Focus should be on understanding how the system behavior as a whole contributed to the loss and not on who or what to blame for it.

- The RCA&CA investigation team did a good job of avoiding blame throughout analysis. However, blame persisted in the document, and led to stopping prior to fully identifying some systemic problems. Assigning this blame takes focus away from understanding the system behavior as a whole. Misdirected focus takes away from learning and instituting how changes can make the system safer.

All assumptions that formed the foundation of the CAST analysis were relevant to the July 2014 collision. This reinforces the reason for using a systems-based approach in analysis in accident investigation. Effective post-accident recommendations can only be generated through understanding the entire sociotechnical system in which the accident occurred.

6. Conclusion

This thesis analyzed the July 2014 collision between two Offshore Supply Vessels using a system-based accident causality model. The thesis aimed to demonstrate the effectiveness of using CAST for accident analysis involving a complex Offshore Supply Vessel system utilizing a software-intensive Dynamic Positioning System.

The thesis examined the existing hierarchical safety control structure to find unsafe control and feedback channels at all levels. The analysis identified unsafe control at each level of the system, which resulted in unsafe component interactions violating the system safety constraints. CAST went beyond the mere identification of unsafe control. The system's control structure itself was examined to determine why control over each component was inadequate to maintain the safety constraints. The analysis strove to account for the contextual environment, available information, and accessible feedback that enforced each controller's flawed process model. Examining each component in the context of safety constraints, the safety control structure, and process models allowed the CAST process to identify system failures and systemic causal factors that contributed to the accident.

This thesis illustrates the usefulness of CAST as a model that fosters evaluation of complex systems holistically to uncover possible changes that eliminate future losses. Incorporating the principles of system operation and design promotes adequate control actions that enforce essential safety constraints throughout the Offshore Supply Vessel hierarchical control structure. It is the hope of the author that the information garnered from this investigation will help the Offshore Supply Vessel operation appropriately focus energy and resources to prevent any future losses and adapt the operation to the point that safety becomes an emergent property.

Accidents are complex processes, and need to be analyzed at all levels of the safety-control structure to generate recommendations that will be effective in preventing the multifarious accidents of the future. While learning from accidents and incidents is important, effort is also needed up front to prevent them in the first place. Learning from accidents is a slow and costly process. A proactive hazard analysis needs to be performed using a powerful systems-theoretic method such as STPA (Systems-Theoretic Process Analysis) [**16**].

7. Bibliography

[1] Department of the Navy, "Root Cause Analysis and Corrective Action Guidance," Navy Programs , Instruction 2012.

[2] J S Carroll, "Incident reviews in high-hazard industries: Sensemaking and learning under ambiguity and accountability.," 1995.

[3] Nancy Leveson, *Engineering a Safer World*. Cambridge, Massachusetts: The MIT Press, 2011.

[4] Hornbeck Offshore. OSV History. [Online]. http://hornbeckoffshore.com/company/history

[5] L3 Marine and Power Systems. NMS6000 Class 2 Dynamic Positioning System. [Online]. www.l-3mps.com/pdfs/NMS6000-CL2.pdf

[6] Nautronix, Ltd. Hornbeck Offshore. [Online]. http://hornbeckoffshore.com/fleet/vessel-attributes

[7] Navy Programs, "26 March 2014 Near Miss," RCA&CA 2014.

[8] Navy Programs, "4 June 2014 Minor Collision," RCA&CA 2014.

[9] DP Software Engineering, "OSV Follow Incident late July 2014," Incident Analysis 2014.

[10] OSV Operations Management and Navy Programs, "Target OSV - Follow OSV Test Plan (R19)," 2014.

[11] Contracted System Analyst and Offshore Manufacturer Management, "Target-Follow Software Tuning and Testing Procedures," 1.022 2011.

[12] SPA, "OSV-VOO Test Plan," NWS Acquisition and Operations Branch, 2014.

[13] OSV Operations Management, "Test Guidance for Software NRL Filter Testing," 2014.

[14] Nancy Leveson, *Safeware: System Safety and Computers*.: Addison-Wesley, 1995.

[15] Navy Programs, "late July 2014 Minor Collision," RCA&CA 2014.

[16] Blake Abrecht, "Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System," Engineering Systems Division, Massachusetts Institute of Technology, Masters Thesis 2016.

Appendix A: NRL Filter

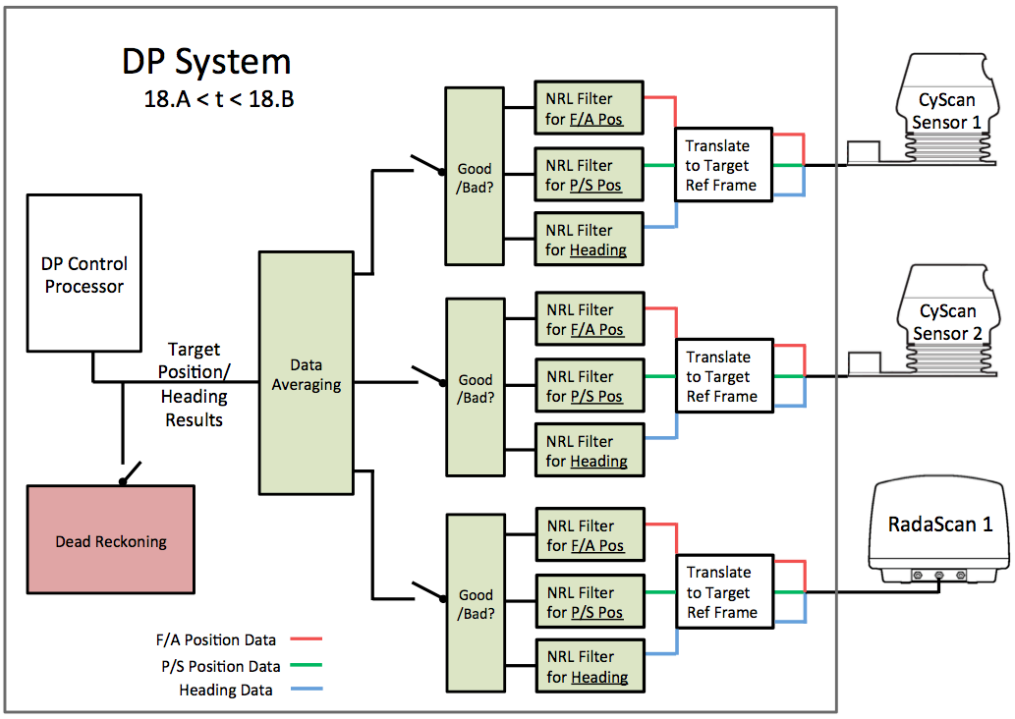

Figure 15: DP System in Target-Follow Mode between Event 18.A and Event 18.B

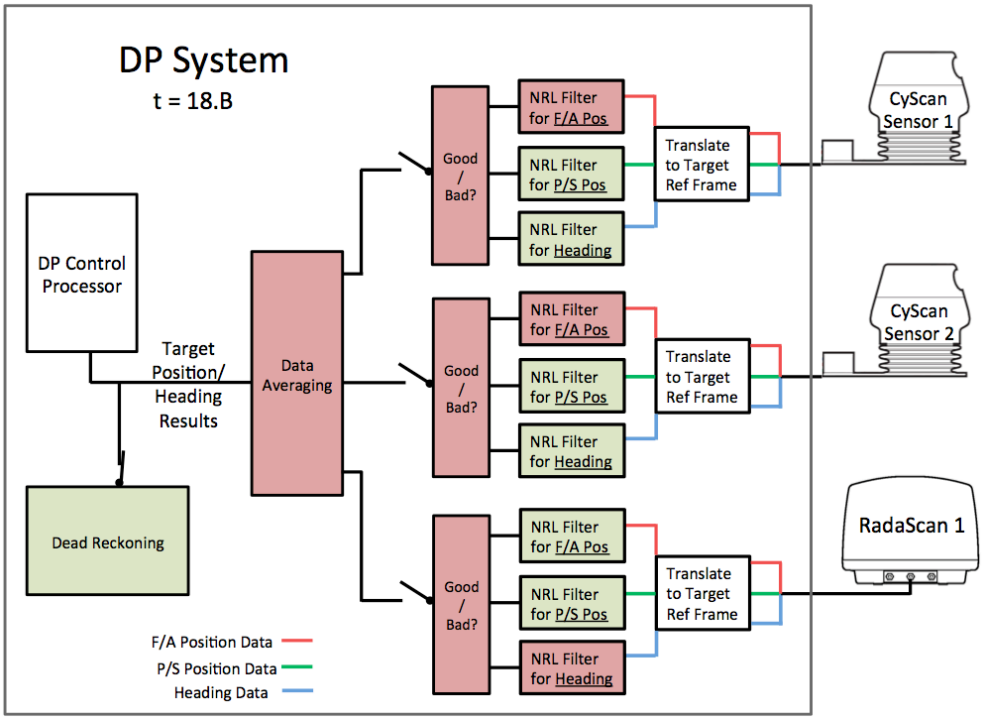

Figure 16: DP System in Dead Reckoning Mode at Event 18.B

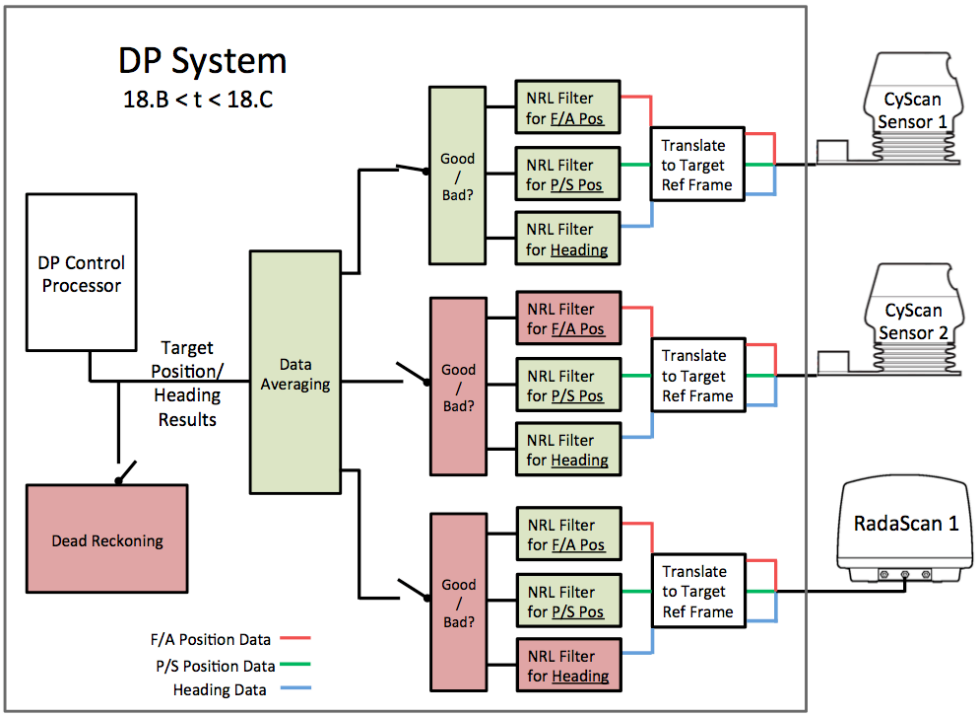

Figure 17: DP System in Target-Follow Mode between Event 18.B and Event 18.C

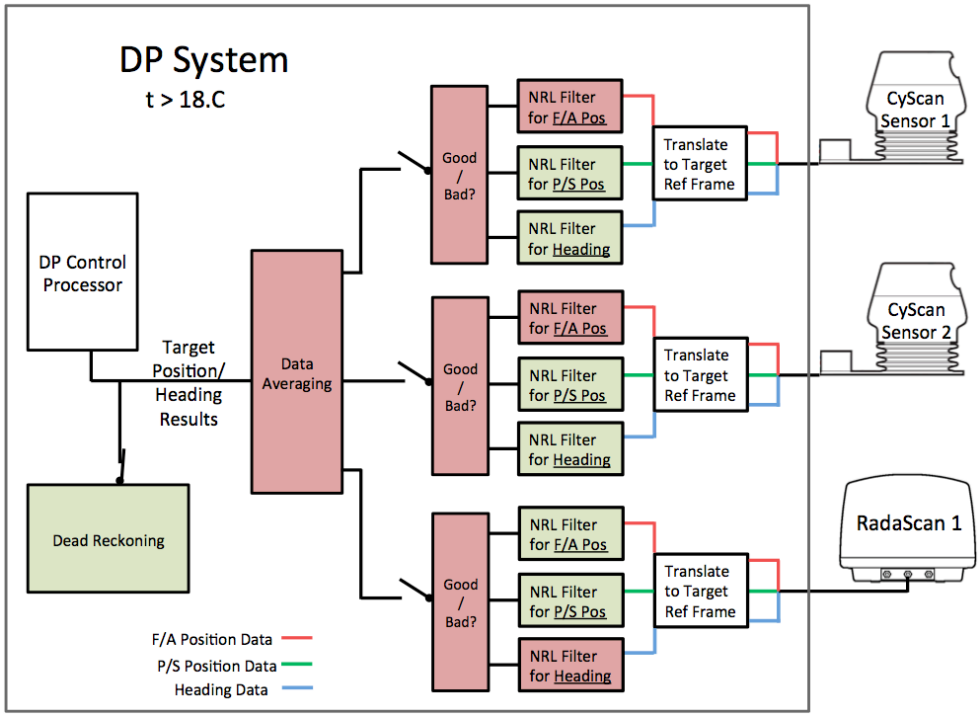

Figure 18: DP System in Dead Reckoning Mode after Event 18.C

Appendix B: RCA&CA and Corrective Actions

Problem 1:

There was a delay by the Follow OSV DPO to fully implement the OSV breakaway procedure. The total time from the DP System entering DR mode until the Follow OSV was in a full breakaway posture with thrust applied from both the bow and stern tunnel thrusters was 35 seconds.

Root Cause(s):

- Lack of experience, plan/task not properly briefed
- Inadequate design criteria
- Task not properly briefed

Short Term Corrective Actions:

1. Software Engineer provide briefing during pre-testing safety brief to team members on intended parameter adjustments and potential impacts to follow-on mode of operations.
2. Until Kalman filter is fixed, breakaway should be performed if a shift to DR Mode occurs. Update NRL tuning procedure to add precaution associated with Kalman filter DR mode recovery effect and add a safety parameter in turning procedure.
3. OSV Manufacturer Management codify procedure to set up the aft control station pre-breakaway thrust positions in addition to the forward station.
4. OSV Manufacturer Management add requirement that at least three officers will be on the bridge (one of which would be the Master) to assist with the system operating during testing. During meals, the ships will either DP in place, or maintain a slow ahead course so that all personnel can properly be focused on the safe operation of the test event.

Long Term Corrective Actions:

1. OSV Manufacturer Management investigate and provide a report on actions needed to change the default shift to manual to the forward station vice the aft station.

Problem 2:

While in DR mode, the estimated relative velocity/rotation rate between the Follow OSV and the Target OSV are reset to zero, resulting in higher estimated velocity error rates and difficulty in recovering from a NRL rejection if significant relative motion between the vessels exists.

Root Cause(s):

- Inadequate design criteria

Short Term Corrective Actions:

1. Until Kalman filter is fixed, breakaway should be performed if a shift to DR Mode occurs. Update NRL tuning procedure to add precaution associated with Kalman filter DR mode recovery effect and add a safety parameter in turning procedure.
2. Software Engineer provide briefing during pre-testing safety brief to team members on intended parameter adjustments and potential impacts to follow-on mode of operations.

Long Term Corrective Actions:

1. Continue with long term software implementation to correct velocity/rotation rate known issue.
2. Evaluate OSV-OSV testing standing procedure to address Kalman filter impact on breakaway procedures.

Problem 3:

Although within the Master's discretion, during the OSV breakaway procedure, the Follow OSV's DPO did not use available rudders to minimize the closure rate toward the target vessel.

Root Cause(s):

- Lack of proficiency

Short Term Corrective Actions:

1. Conduct training on close quarter vessel maneuvering precautions.
2. Add requirement to test memorandum that the DPO who performs the practice breakaway at [xx]ft lateral separation shall remain as the DPO operator for the testing. If a DPO operator changeout is required, then an additional practice breakaway will be performed before continuing testing at or inside [xx]ft lateral separation.

Long Term Corrective Actions:

1. Establish training requirement periodicity for OSV/OSV breakaway procedures.

Problem 4:

The NRL tuning procedure was not sequenced to test less restrictive (position and heading) parameters first which would have reduced the risk of entering DR mode and meeting a criteria for OSV breakaway.

Root Cause(s):

- Lack of questioning attitude
- Lack of coordination between teams/Organizational culture

Short Term Corrective Actions:

1. Conduct a team review of the updated DP Software Engineering tuning procedure focusing on understanding of NRL parameter adjustments and risk to create a conduction requiring break away.

2. Update NRL tuning procedure to sequence the testing runs with lower risk to enter DR mode to occur first.
3. Prior to in-situ modification of the test plan or parameters used during testing, add requirement to the tuning procedure that the analyst will brief the test director and DPO operator on potential impacts to safety.

Long Term Corrective Actions: N/A

Problem 5:

DP logger setup not optimal, and does not record both DP consoles. Reconstruction in the event of Master computer malfunctions would be difficult.

Short Term Corrective Actions: N/A

Long Term Corrective Actions:

1. OSV Manufacturer Management codify procedures with enhanced detail on proper setup to log master DP console.
2. Evaluate course of action for best method to log both DP consoles.