MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

The Maritime Security Center (MSC)

at Stevens Institute of Technology

Hoboken, NJ

Annual Report

Year 4

July 1, 2017 through June 30, 2018

April 4, 2019

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

TABLE OF CONTENTS

1. Background

The Maritime Security Center (MSC), a Department of Homeland Security (DHS) Science and Technology (S&T) National Center of Excellence (COE) was established in 2014 as a result of a competition conducted by DHS's Office of University Programs (OUP). MSC is led by Stevens Institute of Technology and this report is based on activities that were conducted by the MSC at Stevens under the Cooperative Agreement during Year 4 (July 1, 2017 through June 30, 2018).

MSC is composed of a consortium of internationally recognized research universities, including Stevens, MIT, the University of Miami, the University of Puerto Rico, Louisiana State University, Florida Atlantic University, and Elizabeth City State University as well as industry partners, including the American Bureau of Shipping (ABS). The contributions of each partner institution during the reporting period are provided with the corresponding projects in this report.

MSC's mission is to develop both fundamental and applied research to support DHS's and other agencies' maritime security mission goals, including improved detection and interdiction capabilities, enhanced capacity to respond to catastrophic events, and a more secure and efficient Marine Transportation System (MTS). MSC has been focusing on interdisciplinary DHS mission-driven research, education, and technology transition in maritime security, maritime domain awareness, and resiliency issues. Our goal is to develop and transition research and technology solutions and educational programs to DHS maritime stakeholders, such as the US Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and other related agencies and to improve capabilities and capacities for preventing and responding to events in the maritime domain. The next section describes the research projects.

2. Research Projects

This section discusses the Port Resiliency, Maritime Cybersecurity, and VTS Radar research projects. These projects were in the work plan that was approved for Year 4.

2.1. Port Resiliency Project

2.1.1. Introduction

Led by Florida Atlantic University and including collaborators from LSU (Louisiana State University) and University of New Orleans (UNO), the project was aimed at developing a modular, simulation-based, tool to assess and plan for resiliency of a port to major natural and man-made disruptions. Resiliency of a port is defined in terms of the severity of the impact of the disruption to a performance measure such as port capacity and throughput as well as in terms of the duration of the impact on the performance measure. Micro and meso scale modeling and simulations of port operations enable quantifying the consequences of a disruption at a port and associated responses in support of avoidance and mitigation of damage and capacity reduction and aiding rapid recovery from disruptions.

The project involved the development of a simulation model for selective intermodal facilities that covers operation and logistics and study and analysis of optimization problems related to resilience that are commonly encountered in intermodal/port facilities. The model incorporates various stochastic elements such as uncertainty for the terminal's performance measures in order to evaluate the performance of optimization algorithms under different scenarios. The research and the tool being developed provide better understanding of the consequences of disruptions at a port.

This Year's effort involved the completion of the modeling and simulation tasks and competition of the final report.

2.1.2. Project Objective

The principal objective is to develop a cost-effective port resiliency assessment and planning tool that can be adapted, through a choice of interchangeable event modules, to assess and plan for evolving threats and hazards to a port and its waterside and landside distribution capacity, in support of avoidance and mitigation of damage and capacity reduction and aiding rapid recovery from disruptions. The aim is to develop an integrated tool based on a systems approach to port distribution capacity, port operations, risk management, and policy and jurisdiction considerations and involving simulation and modeling. Other objectives include: 1) Development of a simulation model for selective intermodal facilities that is going to cover operation and logistics, 2) Study and analysis of optimization problems related to resilience that are commonly encountered in intermodal/port facilities to incorporate various stochastic elements such as uncertainty for the terminal's performance measures in order to evaluate the performance of optimization algorithms under different scenarios, and 3) Promotion of graduate and undergraduate education in transportation and marine engineering.

2.1.3. Research Approach and Tasks

The tool development is based on modeling and simulation, taking a systems approach to port distribution capacity, port operations, risk management, and policy and jurisdiction considerations. Risk management of a catastrophic event (Conger, 2011) involves careful assessment of the vulnerability of the port to natural and human-caused catastrophic events; implementation of prevention or risk reduction measures to avoid or mitigate damage; advance preparation for quick and effective response and proactive measures to ensure financing is available to cover the costs of response and recovery. Principal considerations in the approach include:

- *Identification of threats and hazards to port transportation system*
- *Safety, security and resiliency of the port infrastructure*: Requirements for port operations and increase in capacity, weather readiness, exposure and mitigation of threats and hazards, and disaster response
- *Safety, security and resiliency of the waterside distribution capacity*: Requirements for sea freight, navigation infrastructure, ship traffic management, maritime surveillance, weather readiness, exposure and mitigation of threats and hazards, and disaster response

- *Safety, security and resiliency of the landside distribution capacity*: Requirements for road and rail freight, road and rail infrastructure, Intermodal connections, weather readiness, exposure and mitigation of threats and hazards, and disaster response
- *Interagency and stakeholder coordination*: Community resources and societal impact, compliance with policy, jurisdiction and maritime security governance

The basis of the simulation is integrated modeling software Aimsun NG (Xiao et el., 2005), which is used in transportation simulations by governments, planners, industry and academia worldwide.

Identified Tasks

The tasks for Year 3 were Tasks 11 through 13. Tasks 1 through 12 are the scope of Years 1 and 2 and are listed for reference. Task 11 was completed, Task 12 was modified to focus on lessons learned as requested and Task 13 was completed in October 2017.

Task 1a. *Develop detailed work plan*

Task 2a. *Define the port system and scope of the project*

Task 3a. *Assess port vulnerabilities*

Task 4a. *Identify characteristics of external disruptors*

Task 3. *Establish port rules, policies and decision-making process*

Task 4. *Define requirements for the tool*

Task 5. *Develop strategies for the development of the tool*

Task 6. *Develop simulation model and conduct initial test and performance validation*

Task 7. *Formulate mathematical model*

Task 8. *Develop optimization models for resiliency and emergency management*

Task 9. *Test and validate mathematical models and optimization algorithms*

Task 10. *Identify and develop a theoretical and empirical basis*

Task 11. Complete modular algorithms and user interfaces for the new tool**.**

Task 12. Engage stakeholders in demonstrations of the tool and evaluate the tool using available real data, basing the evaluation on meeting the requirements established in Task 4**.**

Task 13. Prepare final report**.**

2.1.4. Research Milestones Met

Below are the Research Milestones for the Final Year of this project (Year 3).

Milestone	**Performance Metrics**	**Status**
1. Completion of simulation modeling, detailed algorithms and user interfaces for the new port resiliency assessment and planning tool.	The new tool-based predictions of the impact and recovery of port capacity validated against available historical data from 2 to 3 ports involving closure of a port over a period of time ranging from a few days to several weeks.	Completed. Modeling and simulation platforms were integrated and 3 disruptive port closure scenarios (oil spill/bio-hazard and labor strike) were developed and simulated to show impacts on waterside (vessel dwell time) and landside operations (cargo movement/traffic over varying time scales and full and partial port closures.
2. Completion of the development of best practices guidelines and Port Resilience Indices for specific disruptions using the new tool.	The merits of the Port Resiliency Indices and best practice guidelines evaluated through stakeholder feedback. Response from over 30 stakeholders will be sought.	Completed. 33 stakeholder responses were received from the survey (See Appendix C). The guidelines were completed based on the data that was gathered from the workshop and surveys. This data was not sufficient to complete the Port Resilience indices.

Milestone	Performance Metrics	Status
3. Completion of a final report.	Acceptance/dissemination of the report, publication of results in a technical journal and one TRB conference, and delivery of algorithms, surveys and related materials to DHS.	Final Report Completed. Algorithms are available and are currently residing in the Freight Mobility Research Institute (DOT sponsored Center at FAU).

2.1.5. Accomplishments

Based on available information and stakeholder discussions, the scope of the project was defined to include three disruptive scenarios: 1) disruption at Port Everglades due to a major storm, 2) disruption at Port of New Orleans due to an accident involving major oil spill, and 3) disruption at Ports of LA/Long Beach due to a labor dispute. Significant amount of the required data, including AIS data for ship traffic, were obtained for Port Everglades, Ports of New Orleans, and Ports of LA/Long Beach in support of developing the port resiliency assessment and planning tool. Stakeholders were contacted through various forums, described below, to solicit feedback and to acquire required data. Stakeholder survey questions were prepared and Port Authorities and related stakeholders were contacted. Literature reviews were conducted to identify existing related tools, identify threats and associated vulnerabilities, as well as to take into account various strategies employed to mitigate impact of a disruption and to rapidly recover from it. The proposed tool has been developed, involving 1) development of required port simulations on the Aimsun and PTV Vissim platforms; 2) detailed modeling and integration of Monte Carlo optimization simulation of vessel activities within these platforms; and 3) modeling for linking the waterside and the landside capacities through port operations and storage.

The Monte Carlo optimization simulations provide measures of effectiveness of port operations and landside and waterside traffic under various conditions. The tool has been used to study the three identified cases, involving three ports under different disruptive threats. With sufficient information about a port, the tool can be used to quantify consequences of a disruption at the port for different levels of threat and for various levels of port resiliency, including length of disruption, loss of capacity and throughput and recovery times. In terms of tool transition, it is proposed to house the tool in the Freight Mobility Research Institute (FMRI) that has been recently established as a Department of Transportation (DOT) Center at FAU, to provide support to stakeholders and to facilitate its further development.

1. **Modeling and Simulation**

Five cases of port disruption, in terms of the impacts on waterside and landside capacities, have been considered: 1) Closure of Galveston Channel due to an oil spill, 2) Closure of Port of New York and New Jersey due to Hurricane Sandy, 3) Simulated partial closure of Port Everglades due to flooding, 4) Simulated oil/bio-hazard spill at the Port of New Orleans, 5) Labor strike at the Port of Long Beach. These cases were described in the previous annual report. The first two, involving actual disruptions that took place, will serve to validate the tool. Due to the volume of the data needed to develop the Monte Carlo simulation of the three ports (Port Everglades, Port of New Orleans and Port of Long Beach), 12 months of AIS data from each port was purchased from MarineTraffic.com. The data contains 160,180 records of vessel arrivals, departures, and dwell time starting July 1st, 2015 and ending June 30th, 2016. For all practical purposes, this data is identical to that provided by the U.S. Army Corps of Engineers (USACE). The vessel data was analyzed to identify probability distributions of vessel arrivals and dwell time by cargo type and time of day. Partial details are provided below for cargo considerations undertaken for Port Everglades. Case studies involving Port Everglades was described in the previous annual report. Here we describe the modeling and simulation related to Port of New Orleans and Port of Long Beach.

Case Study: Simulated Oil/Bio-Hazard Spill at the Port of New Orleans

A six-week simulation, encompassing an oil/bio-hazard spill was simulated at the Port of New Orleans beginning March 13, 2017 and ending April 23, 2017. In this case study an oil tanker has collided with a container vessel within the channel leading into the Port of New Orleans on March 26, 2017. The collision caused the release of oil into the channel and the immediate closure of the port for several days, followed by a partial reopening of the port before operations were fully restored. This case study investigated vessel delay, the number of vessels waiting to enter the port minus the number of vessels exiting, as a measure of resiliency. Two scenarios were identified for analysis: Scenario 1) the port was closed to all traffic for four days (March 27 – 30), followed by 50 percent operations for another ten days (March 31 – April 9). Scenario 2) the port was closed to all traffic for three days (March 27 – 29), followed by 50 percent operations for another nine days (March 30 –April 7). In both scenarios, passenger and Ro-Ro/vehicle carries vessels were diverted to other ports and only oil/chemical and container vessels were considered. The historical data was used to identify 50 percent and full operations for port performance. 50 percent operations refer to the 50 percentile of vessel entries and exits seen in the historical data. Full operations assume the 95 percentile of vessel entries and exits. This assumes the partial reopening results in a diminished maximum throughput, whereas the full reopening assumes operations at the level equivalent to the top 5 percent of busiest days. Figure 1 shows the oil/chemical vessel traffic for Scenario one. The primary y-axis displays the number of vessels either entering or exiting the port. The secondary y-axis shows the number of vessels waiting to be serviced by the port, the number of port entries minus the number of port exits. The x-axis displays the six-week simulation period. The first two weeks show normal operations. Because container vessels were known to dock at the port for several days, it was necessary to begin the analysis well in advance of the simulated oil spill. This ensured that any vessels that arrived before the oil spill were still included in the model considerations, even if their dwell times spanned several days. This allowed for port operations to reach equilibrium before taking any measurements. Once in equilibrium, the port was closed on March 27 for four days in Scenario one. This can be seen by the sudden and drastic decrease in the number of vessels exiting the port in both figures. The number of oil/chemical and container vessels arriving at the port requesting access was not impacted by the oil spill. The model assumes that even with the closure, oil/chemical and container vessels still arrive at the port and anchor, waiting for access. With no vessel exits for four days and only half capacity for another ten days, the number of vessels waiting to gain access to the port increased drastically. After the partial reopening, the port was able to service seven oil/chemical vessels and 13 container vessels per day, for the next ten days, representing the 50-percentile production of port operations. By Monday April 10 the port begins processing 12 oil/chemical vessels and 18 container vessels daily, representing the 95 percentile of port operations. This level of service continues until the backlog of vessels has been serviced.

Figure 2 shows the vessel delay resiliency for oil/chemical at the Port of New Orleans corresponding to Scenario one. The y-axis shows the resiliency as quantified by Henry and Ramirez-Marquez (2012). The port enters the disruptive state on Monday March 27, the day of the oil spill. The figure shows a drop off in the port performance in the days following the incident. The figure shows the oil/chemical throughput did not reach its maximum delay until Saturday April 1, six days after the start of the closure and two days into the partial reopening. Oil/chemical vessels did not return to standard operations until Friday, April 14, 19 days after the oil spill.

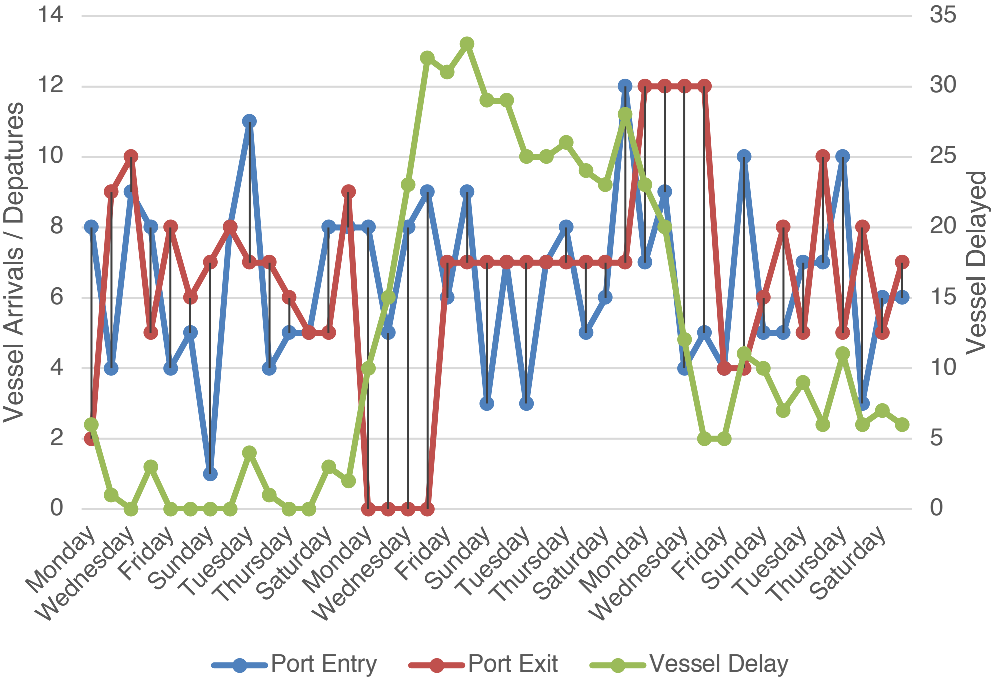


Figure 1: Port of New Orleans Oil/Chemical Vessel Traffic for Scenario One

It would appear the oil/chemical vessels were slightly more resilient when compared to the container vessels. However, this was likely because there were fewer oil/chemical vessels generated during this time period, leading to fewer vessels in the queue.

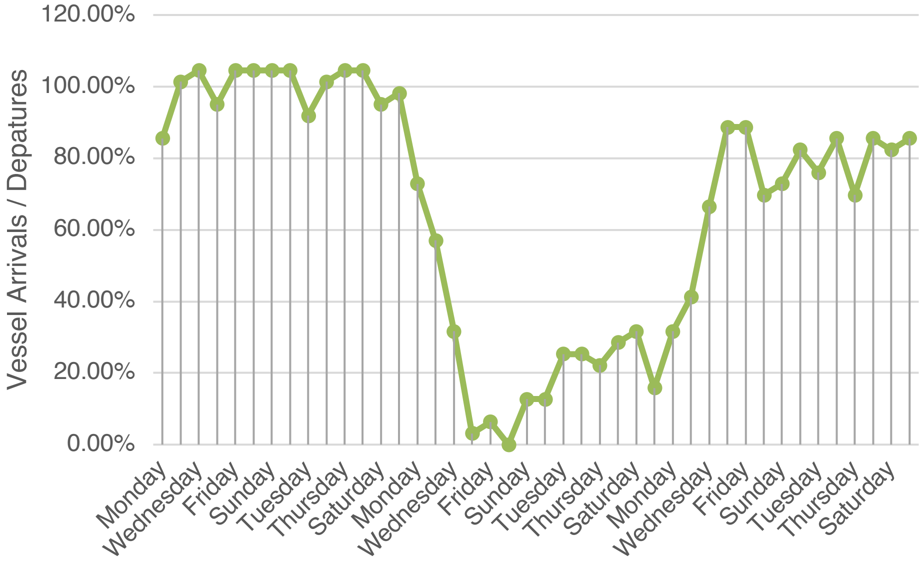


Figure 2: Port of New Orleans Oil/Chemical Vessel Delay Resiliency for Scenario One

Scenario two assumes the oil spill on March 27 resulted in a three-day closure and a nine-day partial closure. The decrease in the number of days the port was closed could be the result of better preparation or more favorable environmental conditions. In either case, the scenario was selected to investigate the relationship between the closure event and the vessel delay resiliency. Figure 3 shows the oil/chemical vessel traffic for the six-week simulation period. The three-day closure was clearly visible with the port exits drastically dropping to zero for the days following the oil spill. As in Scenario one, the partial reopening resulted in the port servicing seven oil/chemical and 13 container vessels daily. The partial reopening lasted for nine days and represented the 50-percentile production of the port. By Saturday April 8 the port begins processing 12 oil/chemical and 18 container vessels daily, representing the 95 percentile of port operations. Similar to Scenario one, this level of service continues until the backlog of vessels has been serviced.

Figure 4 shows the vessel delay resiliency at the Port of New Orleans for the oil/chemical vessels. The oil/chemical vessels reach their maximum vessel delay on Saturday, April 1 and fully recovered by Wednesday, April 12. When compared to Scenario one, the oil/chemical vessels were able to recover two days quicker. Considering Scenario two shortened the duration of the oil spill impact by two days, this was an expected finding. Correspondingly, the container vessels reached their maximum delay queue length on Wednesday, March 29, one day earlier when compared to Scenario one. The container vessels were fully recovered by Tuesday, April 11, signifying a 16-day recovery time and four days shorter than Scenario one. This suggests the relationship between duration of closure and time required to reach recovery is non-linear. The four-day savings could potentially result in significant revenue for the port. The finding also may suggest that if planning and preparations can be put in place that could reduce the closure time of the port, the duration of the disruption could see significant reductions, compounding these benefits.

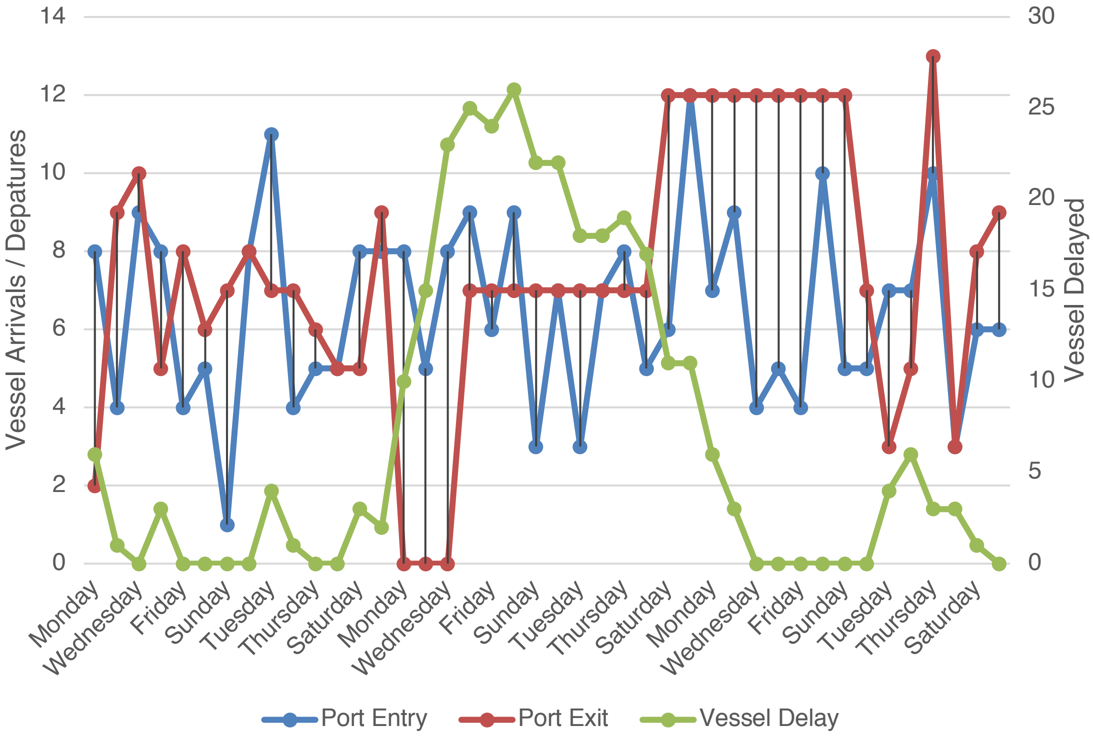


Figure 3: Port of New Orleans Oil/Chemical Vessel Traffic for Scenario Two

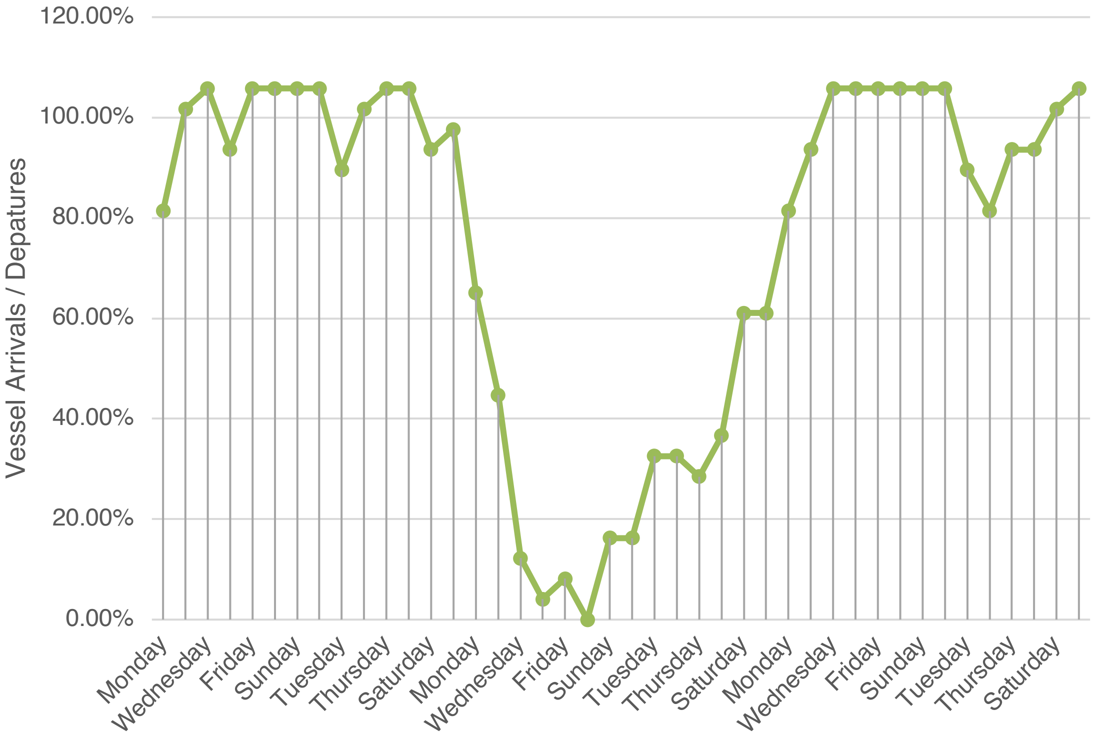


Figure 4: Port of New Orleans Oil/Chemical Vessel Delay Resiliency for Scenario Two

Landside Impact of the Oil Spill

In the Port of New Orleans case study, the research team simulated the conditions of an Oil/Bio-Hazard Spill on the Gulf Coast, which would entirely stop the operations of the port. The objective was to analyze the landside conditions that the event would create. In order to do that, after creating the road network model of the area, we blocked all the entrances to the port, so that no vehicle would be able to enter or leave the terminals. With this situation, the traffic conditions of the network would be signifantly influenced and major delays would be encountered. So, in the model, the goal was to find the average delay, queue length and level of service for 18 days in the aftermath of the event, in order to understand the impact that an event of this scale would have. In the study the group considered 3 days of total port closure and after that 15 days of partial reopening of the ports terminals. Also, for the study the team researched the influence of the block of the entrances in 5 intersections near the port: "Nashville Ave & Tchoupitoulas St", " Napoleon Ave & Tchoupitoulas St ", "Louisiana Ave & Tchoupitoulas St ", "Jackson Ave & Tchoupitoulas St ", "Felicity St & Tchoupitoulas St ". Furthermore, each day a different percentage of trucks wishing to arrive or depart from the area was considered, that way creating variations to the traffic volumes of each intersection.

The results of the simulation showed the influence that the event would have on the traffic operations of the area. First, the average daily and peak hour delay were calculated for each one of the 18 days after the event. The results of the study showed that the first 3 days, during which the port experiences total closure of all entrances, traffic conditions are influenced significantly, as average daily delays range from 300-550 seconds per vehicle and average peak hour delays from 380-650 seconds per vehicle. As the days passed, with the partial reopening of port entrances, conditions became better, as delays were constantly decreasing. But one other aspect that affected the delays was the daily percentages of trucks in the area, as there were occurances where although on a latter day in the aftermath of the event, delays were higher due to higher percentage of trucks. By day 18, conditions in the traffic network became normal, as intersection daily and peak hour delays ranged from 8-23 and 12-25 seconds respectively.

Furthermore, the group analyzed the average daily and peak hour queue lengths for the same conditions. The average queue lengths are depicted in the Figure 5. The figure presents the daily variations in the daily delay during the oil spill event. Generally, the same pattern with the delays applies to the queue lengths. For the first 3 days, the queue lengths in the intersections are extremelly high, with the daily average queues ranging from 50-65 vehicles in each intersection and the peak hour ones from 60-85 vehicles. The percentage of trucks influences the queue lengths the same way as the average delays, as higher daily percentage of trucks in the network leads to higher queue lengths. By the end of the study period, the network managed to return to normal conditions, with the average daily and peak hour queue lengths ranging between 9-23 and 12-24 vehicles respectively.

Last, based on the average delays calculated, the level of service in each intersection for each one of the 18 study days was analyzed. That way we were able to understand the variations with each passing day in the model, and confirm the return to normal conditions after the 18 days, as the LOS, started from "F" for all the intersections the first 3 days and by the pass of the study period increased to an average of "B", with one of the intersections even achieving LOS "A".

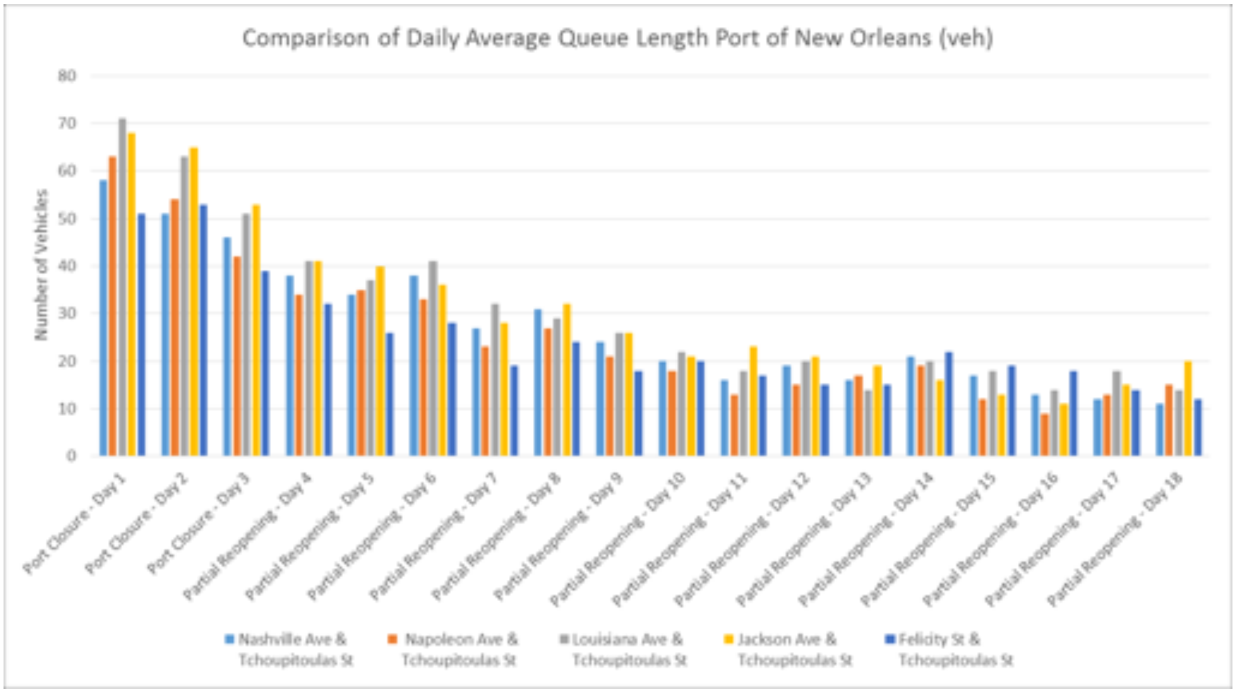


Figure 5: Daily average queue length (veh) occurring on Port of New Orleans Network for 18 days

Case Study: Simulated Labor Strike at the Ports of LA/Long Beach

A three-week simulation was developed to encompass a one-week labor strike at the Ports of LA/Long Beach, CA. The labor strike was modeled as a 20 percent slowdown of operations over a seven-day period. The simulation begins on Monday, June 12, 2017 and ends on Sunday July 2, 2017. The simulated labor slowdown begins on Monday, June 19 and concludes Sunday June 25. It was assumed that a labor dispute of this nature and duration would not impact the number of vessels entering the port. The 20 percent slowdown was modelled as a 20 percent increase in vessel dwell time for all vessel types (oil/chemical, ro-ro/vehicle carriers, container, and passenger).

Figure 6 shows the average dwell time for standard labor conditions and under a labor slowdown for container vessels. The y-axis shows the average dwell time of vessels entering the port. The first week, the port operates with standard labor. The second week, the labor slowdown takes effect and a significant increase can be seen in vessel dwell times within both figures. During the third week, the labor dispute is resolved and the dwell times return to normal. Oil/chemical and passenger vessels average dwell time figures are provided in the Final report.

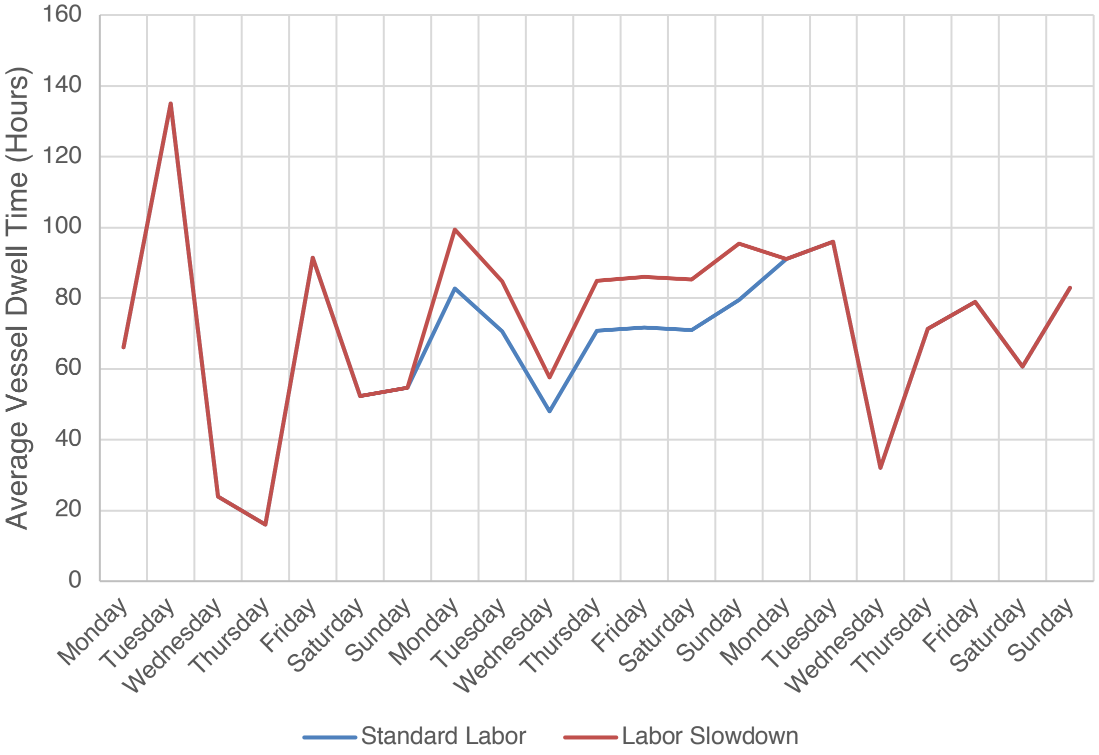


Figure 6: Ports of LA/Long Beach Container Vessel Average Dwell Time

Figure 7 shows the dwell time resiliency at the Port of Long Beach for container vessels. The average dwell times show a sharp drop and then a brief period of recovery before dropping again. This was consistent across vessel types. The maximum disruption occurs when the average dwell time is the highest, i.e. the 20 percent “loss” due to the labor dispute was most impactful on the busiest days. Furthermore, the finding suggests that a 20 percent labor slowdown may not actually correlate to a 20 percent disruption. Depending on how busy the port is during the disputed times, the “loss” may be significantly lower than the stated 20 percent. The implication of this finding may suggest the timing of labor contract negotiations could give a slight advantage to one side or the other. For example, if the labor negotiations were scheduled to coincide with the “slow season” of port traffic, then the impact of a labor slowdown could be significantly diminished.

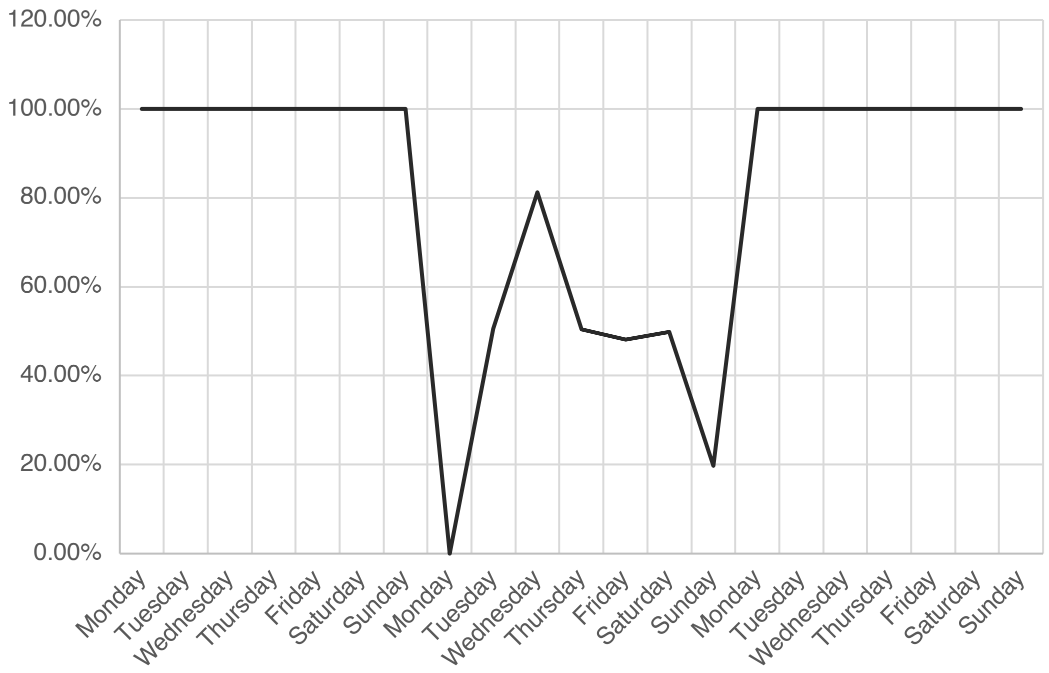


Figure 7: Ports of LA/Long Beach Container Vessel Dwell Time Resiliency

Landside Impact of the Strike

We simulated the effect of the 20% slowdown resulting from the labor dispute on the landside by considering a 20% slowdown of the overall traffic during a period of seven (7) days. The goal of the model was to determine the average delay, queue length and level of service. The intersections analyzed in the model are “New Dock St & Pier Ave”, “SR 47 & Pier Ave”, “Navy Way & Seaside Ave”, “Ferry St & Seaside Hwy”, “Navy Way & Terminal Way”, “Ferry St & Pilchard St”, “Earle St & Pilchard St”, “Ferry St & Terminal Way” and “Earle St & Terminal Way”. The results of the simulation revealed the influence of the event on the traffic operations in the area. First, the average delay was evaluated for each day separately, as well as for a normal day in the absence of the labor dispute. The results showed that the average delay was significantly decreased by the end of the seventh day. Furthermore, the average queue lengths for the same conditions were evaluated. Generally, the results follow the same pattern as with the average delay. The results are depicted in the Figure 8.

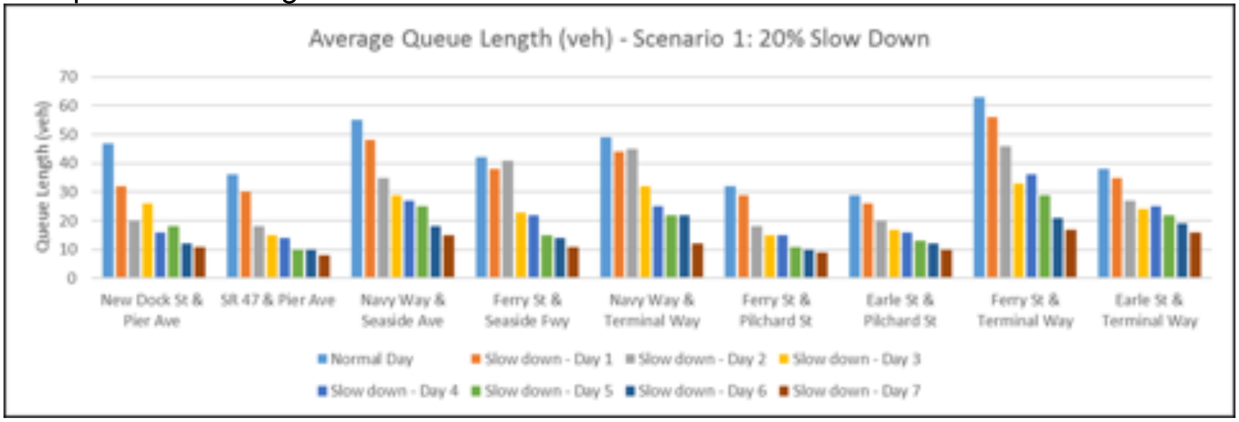


Figure 8. Average Queue Length (veh) occurring on Port of LA/ Long Beach Network – Port Slow Down Days 1-7

Finally, based on the average delays calculated, we analyzed the level of service at each intersection for each of the seven (7) days following the start of the disruption, as well as for a normal day. Through the evaluation of the level of service, the variation with each passing day could be monitored in the model, as the LOS, started from a low level for all the intersections and increased to “A” or “B” level by the end of the period. The detailed results of the LOS are presented in the Table 1.

Table* 1*. Level of Service Analysis for each observed intersection in the Port of LA/ Long Beach Network for all seven days of Labor Dispute case.

	Daily Average Delay (s/veh) – Scenario: 20% Slow Down							
Intersections	**Normal Day**	**Slow down - Day 1**	**Slow down - Day 2**	**Slow down - Day 3**	**Slow down - Day 4**	**Slow down - Day 5**	**Slow down - Day 6**	**Slow down - Day 7**
New Dock St & Pier Ave	C	C	C	C	B	B	B	B
SR 47 & Pier Ave	C	C	B	B	B	A	A	A
Navy Way & Seaside Ave	E	E	D	C	C	C	B	B
Ferry St & Seaside Hwy	B	B	B	A	A	A	A	A
Navy Way & Terminal Way	E	D	D	C	C	B	B	B
Ferry St & Pilchard St	C	C	C	B	B	B	B	B
Earle St & Pilchard St	C	B	B	B	B	A	A	A
Ferry St & Terminal Way	E	E	D	C	C	C	B	B
Earle St & Terminal Way	D	C	C	C	C	B	B	B

Additional details of the modeling and simulation are presented in the Final Project Report submitted to DHS and MSC in January 2018.

In general, the result of the research showed the benefits of quantifying resiliency and how the information gained from such analysis can be beneficial when evaluating alternatives. A quantitative assessment of resiliency provides meaning, context, and relevance to port stakeholders that may not be readily apparent at face value. This research also showed that Automatic Identification System (AIS) data could be utilized to create new methods and metrics for the assessment of resiliency in maritime systems. This methodology advances the field of disaster science by expanding on the concepts first proposed by Henry and Ramirez-Marquez (2012) and Baroud et al. (2014) and applying these methods to empirical observations. AIS data is an excellent source for quantitative data when seeking post-disaster measures of resiliency. The time dependent performance models developed from this data show the cascading effects of disruptions and quantify the benefits gained by recovery efforts in a time-progressive series. One of the more interesting findings of this effort was the manner in which the data show, in quantifiable terms, reductions in performance resulting from a simulated disruption. On a broad level, these findings also represent some of the first steps toward the development of standardized metrics for quantifying MTS operational resiliency. The use of AIS data, which collects information from commercial vessels on a semi-continuous basis, is a rich data source with many applications in disaster science. The methods developed and applied here incorporate an all-hazards approach to quantifying resiliency in navigable waters and can be applied across a range of temporal and spatial scales.

Based on the stakeholder feedback and analysis of the case studies, the following recommendations can be made:

i. Stakeholders noted that attendance in peer meetings is critical to successful agency coordination, but that it often leads to “meeting fatigue”, which results in agency principals delegating the duty to attend these meetings to other employees within the organization. As a result, critical resources are not able to be committed to important programs or decisions because employees in attendance at these meetings lack the authority to commit the resources of the agency—whether its labor or fiscal resources.

ii. Stakeholders also recommended partnering and maintaining frequent communication with the U.S. Army Corps of Engineers, their Local Harbor Safety Committee, the U.S. Coast Guard, and community business partners.

iii. In response to what steps worked in recovering from disruptions to port activities as a result of an emergency or disaster, stakeholders advised that the use of the Incident Command System (ICS) for managing a port disruption and subsequent re-formation of the port was critical. Stakeholders noted that the use of the ICS ensures that all parties’ interests are incorporated into the Incident Action Plan, so that there is a unity of effort and a common operating picture.

iv. Stakeholders noted that it was important to have well-prepared communication and emergency response plans. Also, one stakeholder noted that emergency response drills should be conducted often to ensure smooth performance during real events; moreover, community stakeholders should be very familiar with each other, since the emergency is not the time for stakeholders to be meeting for the first time and providing feedback on important decisions to be made during this emergency situation.

v. One recommendation that emerged from the survey data was that port organizations should adopt the following items to enhance resilience in their port or organization: a)

Train people to understand complex sociotechnical systems that are at work in maritime environments; b) Educate individuals and groups of individuals on the variability in performance due to local conditions and on keeping operations within safe limits to prevent loss of situational control; and c) adopt system safety models of accident prevention that build on social infrastructure, similar to the U.K. Port Safety Marine Code, instead of placing limits on physical conditions.

In terms of the major challenges or obstacles to improving port resiliency, key recommendations were to do the following:

1) Enhance knowledge of system safety and safety management systems at all levels of government, in a variety of port districts, and in a variety of agencies such as the U.S. Coast Guard, similar to how the Federal Aviation Administration and the Federal Railroad Administration has required that all airports, airlines, railroads, and service providers use the same safety management system;
2) Replace the use of sequential modeling of accident prevention with a systems model of accident prevention;
3) Increase understanding by organizations that resilience is not the property of maritime organizations; but, instead, it comes from the capabilities of its employees to implement resiliency efforts that lead to the most cost-effective and efficient models of resiliency for organizations and ports;
4) Realize that the inability to recognize where the boundaries are of safe operations leads to serious unintended consequences such as the deepening of channels without the widening of channels on hydrodynamic interactions with moored vessels; also to recognize the inability of an organization or port to cut back on extreme boundaries or limits in a controlled fashion;
5) Enhance the ability of a port or organization to recover from an emergency or disaster where there was loss of control in a safe manner; and,
6) Deal with the challenge of finding time for increased emergency management training and improved emergency management plans and tools as well as getting employee buy-in on cooperating and participating in emergency management and resiliency efforts at port and organizations.

Based on the case studies conducted for the three ports in the hypothetical event of corresponding disruptive scenarios, the following observations can be made with respect to the developed tools and their applications in predicting possible consequences of making a particular decision from a set of alternative decisions in responding to a disruption and developing an optimal response:

1) In the case of the two-day disruption at Port Everglades, the tool quantified that the recovery period could be reduced by three days if a 24-hour emergency shift schedule is implemented instead of a 12-hour schedule.
2) When analyzing the Port of New Orleans, the simulation model and analysis of two scenarios showed that a 25 percent reduction in the length of disruption could be archived if the port closure was shorted by one day. This can assist port stakeholders in evaluating the cost and benefits of infrastructure investment and emergency planning and preparedness. The resiliency analysis conducted as part of this research can provide a quantitative justification for investing in resiliency as part of a strategic plan.

3) In the case of the 20 percent “labor slowdown” due to a labor dispute at the Port of LA/Long Beach, the model suggests that the maximum disruption occurs when the average ship dwell time is the highest, i.e. the 20 percent “loss” due to the labor dispute is most impactful on the busiest days. Furthermore, the findings suggest that a 20 percent labor slowdown may not actually correlate to a 20 percent disruption. Depending on how busy the port is during the disputed times, the “loss” may be significantly lower than the stated 20 percent.
4) Based on acquired traffic and truck volumes, the model suggests that at the Port of LA/Long Beach the most critical daily times for port resilience are from 7:15-9:00am and 3:45-5:00pm.

These simple examples clearly demonstrate the need for modeling and simulation based quantitative analysis in resiliency planning and allows for a more rigorous evaluation of the cost and benefits associated for resiliency strategies.

Final Report

A detailed Final Report has been prepared that describes the work completed, including the modeling and simulation case studies, stakeholder engagement and feedback, recommendations and lessons learned, and plans for transition. The Final Report was submitted to DHS and MSC in January 2018.

Publications

- *Port Resiliency Study*. M Dhanak, E. Kaisar, A. Sapat, S. Parr, and B. Wolshon. A brief provided to the Area Maritime Security Committee, Dania Beach Florida, August, 2016
- *“Simulation-based Port Resiliency Planning and Assessment Tool”.* M Dhanak, E. Kaisar, A. Sapat, S. Parr, and B. Wolshon. Presentation made at the Workshop on Enhancing Port Resiliency, FAU, December 2016.
- Peer-reviewed conference and journal papers in preparation.

Bibliography

Beatley, T. (2009). *Planning for coastal resilience: Best practices for calamitous times.* Washington, D.C.: Island Press.

Cambridge Systematics, 2008. “Waterborne Freight Transportation Bottom Line” Report prepared for American Association of State Highway and Transportation http://downloads.transportation.org/AASHTO_Waterborne_Freight_COMPLETE.pdf

CMTS, 2008. National strategy for MTS, Committee on MTS.

Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). *Designing resilience: Preparing for extreme events*. Pittsburgh, PA: University of Pittsburgh Press.

Committee on U.S. Army Corps of Engineers Water Resources Science, Engineering, and Planning: Coastal Risk Reduction, Water Science and Technology Board, Ocean Studies Board, Division on Earth and Life Studies and the National Research Council of the National Academies. (2014). *Reducing coastal risk on the East and Gulf coasts.* Washington, D.C.: National Academy of Sciences.

Comprehensive Annual Financial Report (CAFR). (2015). *Port of Long Beach: Comprehensive annual financial report*. Retrieved from http://www.polb.com/finance/annualreports.asp

Conger, Sue. Process Mapping and Management. Business Expert Press, 2011.

Dixit, V., Montz, T., and B. Wolshon, “Validation Techniques for Region-Level Microscopic Mass Evacuation Traffic Simulations,” Transportation Research Record: Journal of Transportation Research Board, No. 2229, 2011, pp. 66-74.

Eksioglu, B., Eksioglu, S., Allen, A., & Myles, A. National Center for Intermodal Transportation, (2009). *A simulation model to analyze the impact of crisis conditions on the performance of port operations* (10-03-09)

Holguin-Veras, J., Jaller, M., Taniguchi, E., & Aros-Vera, F. (2013, January). *The lessons from catastrophic events for post-disaster humanitarian logistic efforts: The port au prince earthquake and the tohoku disasters*. 13-1771 Trb 92nd annual meeting compendium of papers.

Gil, I. C. & Wulf, C. (Eds.). (2015). *Hazardous future: Disaster, representation and the assessment of risk.* Berlin: Walter de Gruyter.

Harbor Highlights. (1961). *Port of Long Beach Harbor Highlights,* 7(1). Retrieved from http://www.polb.com/about/history/historicalpubs.asp

International Institute for Sustainable Seaports. (2014). Sustainable design and construction guidelines. Retrieved from http://www.getf.org/our-projects-partnerships/the-international-institute-of-sustainable-seaports/

Jin, M. (2013, January 03). *Framework development for scalable and user-friendly port recovery planning simulation*. Retrieved from http://trid.trb.org/view/2010/P/1229721

Kaisar E., Hess L., and Portal-Palomo A.B., “An Emergency Evacuation Planning Model for Vulnerable Population Utilizing Public Transportation Systems” Journal of Public Transportation Vol. 15, No. 2, 45-70.

Kaisar E., and Austin M., “Synthesis and Validation of High-level Behavior Models for Narrow Waterway Management Systems” Journal of Computing in Civil Engineering, ASCE, September, pp. 373-378

Kaisar E., “A Model for Heavy Truck Freight Movement at the Intermodal Facilities in the Port of Baltimore” conference proceedings at the 7th Conference on Access Management, Park City, Utah.

Kaisar E., Pathomsiri S., Haghani A., and Kourkounaki P., “Developing Measures of US Ports productivity and Performance: Using Data Envelopment Analysis and Free Disposal Hull Approaches” conference proceedings at the 47th Transportation Research Forum, New York.

Kaisar E., Austin M., Lagakos V., Papadimitriou S., and Haghani A., “Hierarchical Object-Oriented Models for Management of Narrow Passageways” European Research Studies Journal, Volume VI, Issue (3-4), 2003, pp 95-108.

Kostro, S. S. & Riba, G. (2014). *Achieving disaster resilience in U.S. communities: Executive branch, congressional, and private-sector efforts.* Lanham, MD: Rowman & Littlefield.

Miller, J., & Wakeman, T. (2013, January). *Lessons from hurricane sandy for port resilience*. Retrieved from http://trid.trb.org/view/2010/P/1229721

Morris, L. L., & Sempier, T. (2016). Ports resilience index: A port management self-assessment. *Ports Resilience Expert Committee,* GOMSG-H-16-001. Available at www.masgc.org/ri

MTSNAC, 2006. “The Marine Transportation System and the Global Supply Chain,” Marine Transportation System Advisory Council Report.

Naghawi, H. and B. Wolshon, “Performance of Multi-Modal Evacuation Traffic Networks: A Simulation Based Assessment,” ASCE Natural Hazards Review, August 2012, Vol. 13, No. 3, pp. 196 - 204.

NOAA Coastal Service Center. 2011. Port Resilience Planning Tool. http://www.csc.noaa.gov/port/

Paul, A., & Maloni, M. (2010). Modeling the effects of port disaster. *Maritime economics & Logistics*, *12*(2), 127-146.

Petersen, D. J. (1980). *Port of Long Beach Harbor Highlights,* 4(2). Retrieved from http://www.polb.com/about/history/historicalpubs.asp

Port Everglades. (2015). *Annual commerce report.* Retrieved from https://res-1.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/2015_Commerce_Report_ADA_FINAL_3c5a5627-ba3e-4446-a43d-38f7bcef85b2.pdf

Port Everglades. (2015/2016). 2015/2016: *Facilities guide and directory.* Retrieved from http://www.bluetoad.com/publication/?i=265901

Port Everglades. (2014). *Harbor deepening and widening*. Retrieved from https://res-2.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/Harbor_Deepening_Widening_updated_May_19_2015_cb6b34e0-b406-47ca-be9b-7706134a8bf9.pdf

Port Everglades. (2014). *History*. Retrieved from http://www.porteverglades.net/about-us/history/

Port Everglades. (2014). *Master Vision Plan*. Retrieved from http://www.porteverglades.net/expansion/master-vision-plan/

Port Everglades. (2015). *Waterborne Commerce Chart*. Retrieved from https://res-4.cloudinary.com/simpleview/image/upload/v1/clients/porteverglades/2015_Waterborne_Commerce_Chart_228bb813-20cb-4b6a-a730-d337798cf7b7.pdf

Port of Long Beach. 2016. *About the Port*. Retrieved from http://www.polb.com/about/default.asp

Port of Long Beach Annual Report. (2000). *2000 Annual Report*. Retrieved from http://www.polb.com/about/history/historicalpubs.asp

Port of Long Beach. (2016). *Facts at a Glance.* Retrieved from http://www.polb.com/about/facts.asp

Port of Long Beach. (2016). *Frequently Asked Questions*. Retrieved from http://www.polb.com/about/faqs.asp

Port of Long Beach. (2016). *Tonnage Summary.* Retrieved from http://www.polb.com/economics/stats/tonnage.asp

Port Nola. (2016). Port of New Orleans: History. Retrieved from http://portno.com/history

Port Nola. (2016). *Port Directory: The 2016 Official Directory of the Port of New Orlean*s. Retrieved from http://portno.com/port-directory

Port Nola. (2016). *Port of New Orleans: Port Statistics*. Retrieved from http://portno.com/port-statistics

Portal M.I., Kaisar E.I., Golias M., and Ivey S., “Scheduling Container Vessels Under Handling and Arrival Time Uncertainty” conference proceedings at the 92th Transportation Research Board Annual Meeting, Washington DC.

Portal Palomo I., Kaisar E., “Ports as a Growing Factor in the Supply Chain”, Conference proceedings at the 9th Latin American and Caribbean Consortium of Engineering Institutions, Medellin, Colombia

Pounds, B. J., Ward, K. R. & Forsythe, D. (2013). *NOAA rapid survey response for Hurricane Sandy*. Retrieved from http://ushydro.thsoa.org/hy13/pdf/0326P_10L_58.pdf

Rice, Jr., J. B., Trepte, K., Nickerson, J., Python, G., Luettich, R., & Beck, K. (2014). *Port resilience decision framework toolkit-Decision processes.* Retrieved from http://coastalhazardscenter.org/dev/wp-content/uploads/2015/03/2014-1405a-enclosure-1.pdf

Scarlatos P., Kaisar E., and Teegavarapu R., "Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems", In Mathematical Methods and Applied Computing", ISBN 978-960-474-124-3, pp. 324-346.

Stich, Bethany and Chad Miller. "Collective Action Regimes in Inland Marine Port Clusters: The Case of the Tenn-Tomm Waterway System," MS Water Resource Conference. Proceedings, 2009.

Stich, Bethany and Chad Miller. "Using the Advocacy Coalition Framework to Understand Freight Transportation Policy Change." Public Works Management and Policy. Vol. 13, No. 1, 62-74, 2008.

Stich, Bethany and Bill Martin. (2011) Measurements for Success of Container on Barge Utilization on the Tennessee-Tombigbee Waterway Prepared for: The National Center for Intermodal Transportation (NCIT)

Smongesky, P. P. (2007). Port of Long Beach Chronological History: Introduction. In C. F. Connors (Ed.), *Chronological History By Pier: 1909-2002* (pp. 1-13). Retrieved from http://www.polb.com/about/history/historicalpubs.abs

Southworth, Frank, Jolene Hayes, Shannon McLeod, and Anne Strauss-Wieder. 2014. "Making U.S. Ports Resilient as Part of Extended Intermodal Supply Chains" TRB Report. http://onlinepubs.trb.org/onlinepubs/ncfrp/ncfrp_rpt_030.pdf

Sturgis, L. A., Smythe, T., & Tucci, A. E. (2014). Port recovery in the aftermath of Hurricane Sandy: Improving Port resiliency in the era of climate change*. Center for a New American Society: Voices from the Field.* Retrieved from http://www.cnas.org/sites/default/files/publications-pdf/CNAS_HurricaneSandy_VoicesFromTheField.pdf

U.S. Government Accountability Office. (2012). Critical infrastructure protection: An implementation strategy could advance DHS's coordination of resilience efforts across ports and other infrastructure (GAO-13-11). Retrieved from http://www.gao.gov/assets/650/649705.pdf

Wakeman, III, T. H. & Miller, J. (2013). *Final report: Lessons from Hurricane Sandy for port resilience* (UTRC-RF Project No. 49997-56-24). Retrieved from http://www.utrc2.org/research/projects/hurricanesandy-port-resilience

Wang, J., Olivier, D., Notteboom, T., & Slack, B. (Eds.). (2005). *Ports, cities, and global supply chains.* Burlington, VT: Ashgate Publishing Company.

Wolshon, B., and V.V. Dixit, "Traffic Modeling and Simulation for Regional Multimodal Evacuation Analysis," International Journal of Advanced Intelligence Paradigms, Vol. 4, No. 1, 2012. pp. 71-82.

Wolshon B. and B. McArdle, "Traffic Impacts and Dispersal Patterns on Secondary and Low Volume Roadways During Regional Evacuations," ASCE Natural Hazards Review, February 2011, Vol. 12, No. 1, pp. 19 - 27.

Wolshon, B. and V.V Dixit. "Planning and Management of Transportation Systems for Evacuation," Chapter TBD, Handbook of Emergency Response: A Human Factors and Systems Engineering Approach, ISBN: TBD, Taylor & Francis Publishing Inc., New York, anticipated publication in May 2013.

Wolshon, B. and P. Murray-Tuite, “The Role of OR in Emergency Evacuation from Hazmat Incidents,” Chapter 4, Handbook of Operations Research and Management Sciences Models in Hazardous Materials Transportation, ISBN: TBD, Springer Publishing Inc., New York, anticipated publication in March 2013.

2.2. Maritime Cyber Security Project

2.2.1. Overview

In July of 2016, this project started and has focused on six separate topic areas as shown in Table 1. The research was conducted to inform government stakeholders in the development of cybersecurity-related regulations and policies. In addition, the research should support interactions with industry to improve awareness of cyber threats and provide actionable guidance to improve cybersecurity by addressing vulnerabilities.

Table 1. Research Topics and Questions

Topic Area		Research Questions
1	Risk-Based Performance Standards	What risk-based performance standards can be developed for cyber risk management of the Marine Transportation System (MTS)? How would performance standards inter-relate with other infrastructure sectors and their performance standards? How would performance standards inter-relate with existing safety and security management systems?
2	Framework for Cyber Policy	What type of criteria should be utilized to develop an academically rigorous framework for Cyber Policy for the MTS?
3	Critical Points of Failure	Based on a multi-node analysis, what are the critical Points of Failure within the cyber system supporting the MTS?
4	Requirements for Maritime Cyber Range	What are the critical requirements that should be considered when developing an academically rigorous and multi-use Maritime Cyber Range?
5	Framework for Point of Failure Detection Methodology	What methodologies can be utilized or invented to develop a framework to analyze a point of Failure Detection Methodology?
6	Maritime Cyber Deterrent Strategy Effectiveness	What methodologies can be employed to conduct a quantitative analysis of maritime cyber deterrent strategy effectiveness?

Over the course of the project, the team performed and documented new research across all six topic areas. Topic areas 1, 2, and 5 were completed and discussed in the Center’s Year 3 annual report and topic areas and research questions 3, 4 and 6, bulleted below, were addressed in Year 4, and are discussed herein:

- Topic Area 3: Critical Points of Failure
- Topic Area 4: Requirements for Maritime Cyber Range
- Topic Area 6: Maritime Cyber Deterrent Strategy Effectiveness

Milestones

Milestones	Performance Metrics	Status
Critical Points of Failure	• Doctrine Review • Asset Class Screening • General Architecture Development • Corruption Vector and Penetration Point Taxonomy • Scenario Development • Risk Assessment • Results Documentation	Complete. Current cybersecurity maturity models (CMMI and C2M2) and resilience models (CERT-RMM) were referenced and reviewed. Architectures of vessel IT/OT and integrated systems were developed. A maritime cybersecurity risk taxonomy model and associated implementation tools that express threats, vulnerabilities, and consequences in countable and calculable terms was developed. Results of model are documented here within and in the final project report and are intended to provide a consistent, clarifying, and countable method for organizing thinking about maritime cybersecurity risk.
Requirements for Maritime Cyber Range	• Use Case Development • System Behavior Definition • Test Boundary Development • Equipment and Software Requirements • Test Documentations • Develop Training Requirements	Complete. A Cyber Range Requirements Report was completed taking into consideration the USCG's Cyber Strategy. An in-depth review of government, academic and commercially available cyber ranges was conducted. Requirements were developed based on USCG mission support use cases and recommendations were made.
Maritime Cyber Deterrent Strategy Effectiveness	• Define Current Cyber Deterrent Strategy • Decision Definition	Complete. A methodology and Cyber Deterrence Ef-

	• Information Requirements • Methodology Identification/Development • Model Development • Perform Analysis • Document Results	fectiveness Model was created to conduct a quantitative risk analysis of a wide portfolio of assets including vessels and facilities of different types. The model allows for multiple output measures and visualizations. The model includes assessments for environmental, economic and mobility consequences, as well as death and injury. An analysis of current USCG Risk Assessment Models was conducted and stakeholder needs were taken into consideration. Results of the model are found herewith and in the final project report.

2.2.2. Critical Points of Failure

This section presents a reference model and methodology that generates quantitative risk results of sufficient quality to inform critical decisions in the design, assessment, and management of cybersecurity programs for maritime companies. The results are also sufficient to provide information to cybersecurity regulators (e.g., USCG) to support their regulatory development and enforcement activities.

The results of this research are designed to support a variety of key functions for cybersecurity personnel including:

- Identify and understand potential points of failure
- Prioritize issues to address
- Control, manage, and improve risk profile through implementation of security measures
- Measure impact of implemented security measures
- Determine when program has reached diminishing returns

The research presented in this section applies the fundamental components of cybersecurity: functions, connections, and identities at the next level of detail to enable systematic accounting and simple assessment of these components as a means of quantitatively expressing an asset's risk.

Every maritime asset is unique based on the materials of construction, layout, and the chosen equipment. Similarly, the "virtual asset" which is made up of IT and OT components, systems and networks are unique. No two virtual assets are identical. They have different attributes based on how they are designed and architected; so, the model and methodology focus on the fundamental building blocks on which every virtual asset is built: functions, connections, and identities. Using these building blocks, the model can be configured to represent any virtual asset and can be assessed to generate relative cybersecurity risk scores that enable consistent risk comparison of disparate assets using same measuring stick.

Background

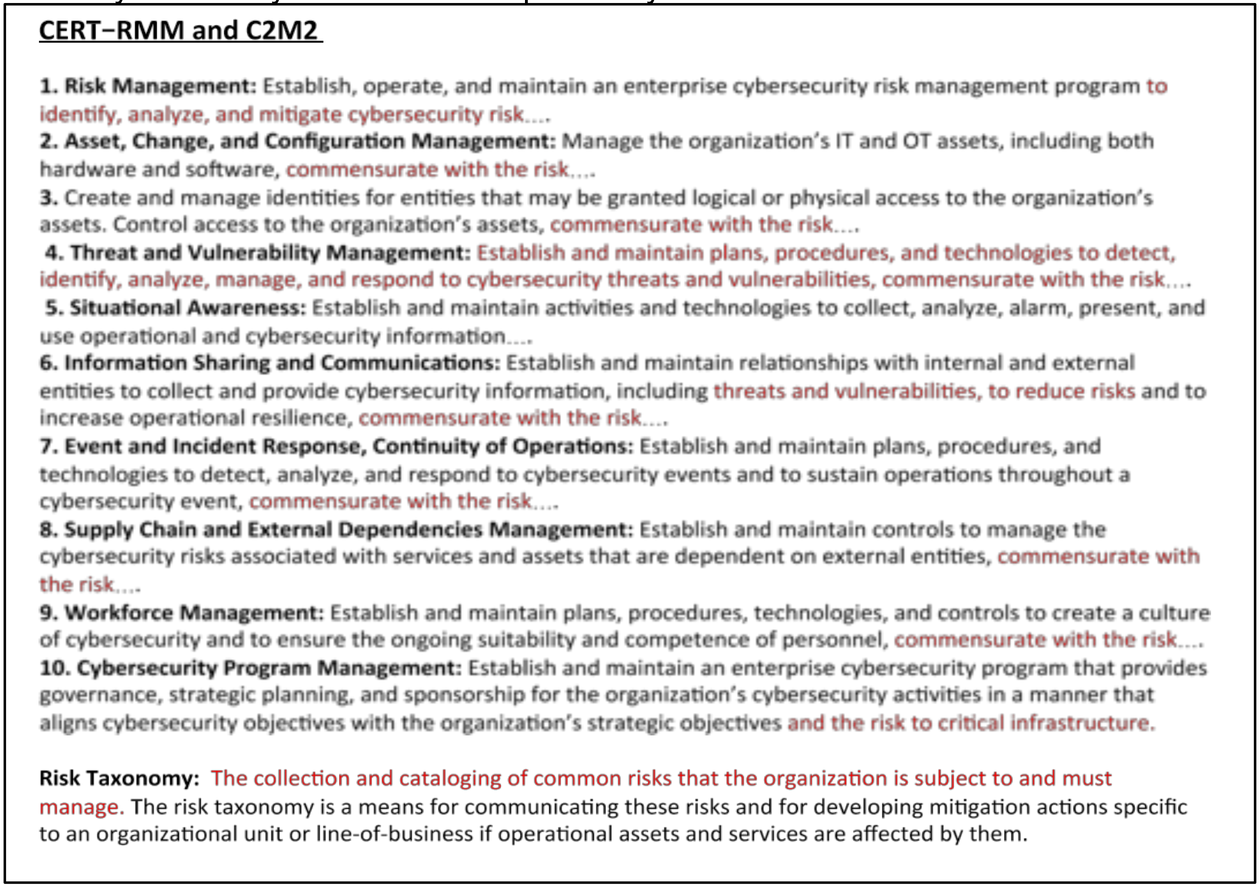
Current methods for cybersecurity system and program assessment are based on observing documented designs and procedures, staff behaviors, and physical indications (i.e., evidence) of specific implemented practices and protections within multiple cybersecurity "domains." The approach is binary in that regulators and certification assessors look for indications of protection and remediation capabilities in programs and aboard assets. The assessment is basically a "go/no-go" situation in that it determines if a protection or procedure is in place and observed, or not. There is minimal supportive guidance for questions such as, "How bad is it? How great is the risk? What do I need to fix or add? What is most at risk? What should I do to meet standard or certification criteria? Can you help me?" Answers to those questions are now within reach.

In practice, cybersecurity programs are designed and implemented based on case-specific (parochial) understandings, perceived needs, and available resources. Real-world programs are not typically designed to accommodate maturity levels but are instead designed based on interpretations of available guidance, mandated regulations, contract requirements, and internal resources. Such programs exemplify pragmatic selection of specific capabilities associated with all domains and all levels of program maturity. As a result, regulators and assessors are hard pressed to reach a formulation that will identify a program implementation as belonging in single achievement or maturity level. Pass/fail requirements criteria simply do not provide sufficient problem measurement resolution to yield answers to the questions posed above. Further, the summary result of such assessments does not provide clear insight into the overall cybersecurity preparedness of an organization or asset.

At the core of this problem is the notion of clearly understood and quantifiable risk. When referencing the SEI CMMI and the C2M2, clarifications of cybersecurity domain descriptions include specific "Approach Objectives" and "Management Objectives" with detailed implementation guidance. The larger cybersecurity problem is nicely decomposed and presented. And, a strikingly obvious foundational requirement for satisfying the requirements provided within each domain to all the domains presented. It is a deep understanding of the cybersecurity risk associated with each domain as associated with an organization, asset, and function.

Consider, the summary descriptions of the ten C2M2 domains as excerpted below, with specific references to scaling solutions to levels of "risk" highlighted in red text.

The ability to scale to risk and in turn scale programs to manage risk is a critical need in cybersecurity. This research specifically reacts to that need.



CERT–RMM and C2M2

1. Risk Management: Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk….
2. Asset, Change, and Configuration Management: Manage the organization's IT and OT assets, including both hardware and software, commensurate with the risk….
3. Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk….
4. Threat and Vulnerability Management: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk….
5. Situational Awareness: Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information….
6. Information Sharing and Communications: Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk….
7. Event and Incident Response, Continuity of Operations: Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk….
8. Supply Chain and External Dependencies Management: Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk….
9. Workforce Management: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk….
10. Cybersecurity Program Management: Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

Risk Taxonomy: The collection and cataloging of common risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line-of-business if operational assets and services are affected by them.

Figure 1. References to risk in Maturity Model References

It is noteworthy that of the ten domain descriptions presented in C2M2:

- Nine make references to managing or understanding risk
- Six contain a reference to “commensurate with risk.” Domain #4 is especially important in that it provides guidance for threat and vulnerability management:

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

- Domain #1 is specifically about risk management, and reads:

*Establish, operate, and maintain an enterprise **cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk** to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.*

Additionally, the C2M2 provides a definition of and use for a risk taxonomy:

- ***Definition**: The collection and cataloging of common risks that the organization is subject to and must manage.*
- ***Use**: The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line-of-business if operational assets and services are affected by them.*

The imperative to identify, analyze, and mitigate risk requires that risk be countable and calculable. Even so, further guidance for approaches identifying, describing, or managing threats and vulnerabilities is absent. It is left to the user to develop a representative risk taxonomy that is essential to appropriately developing capabilities in all 10 domains and develop a method of scaling risk.

The research presented in this section attempts to close this critical gap for maritime cybersecurity by providing a risk taxonomy model and associated implementation tools that express threats, vulnerabilities, and consequences in countable and calculable terms. This enables users of various cybersecurity models, standards, and procedures to gauge and characterize the relative effectiveness of specific implementations during design, operation, and improvement activities. It adds meaning to a risk management plan and fully enables users to make cybersecurity decisions "commensurate with the risk" as required by C2M2 and similar industry guidance.

Risk Assessment

Risk information fundamentally seeks to improve decision-makers' understanding by answering the three questions illustrated in Figure 2.

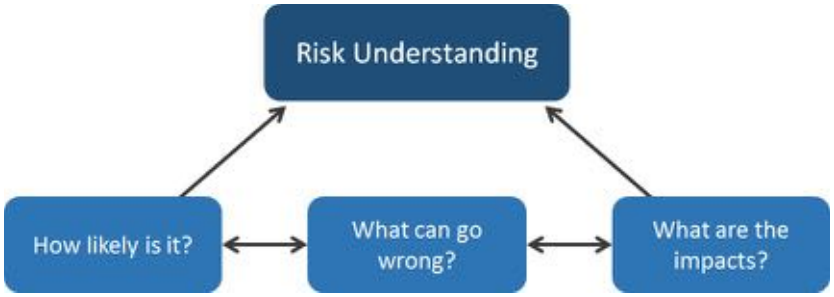


Figure 2. Fundamentals of Risk Understanding

Risk identification, assessment, and management can cover a wide range of approaches from very simple screening approaches to quite sophisticated quantitative/qualitative modeling approaches. The key is to always fit the complexity of the modeling approach to the level of information needed by decision makers; this information is typically derived from a combination of (1) historical experience, (2) analytical methods, and (3) knowledge of experts.

This section will explore how these concepts are typically applied for security risk assessment and the challenges of applying them within the cyber domain.

In 2006, the USCG established the Maritime Security Risk Analysis Model (MSRAM) program. MSRAM is a terrorism risk management tool and supporting process deployed annually to local Port Security Specialists (PSSs) in major ports across the country. MSRAM requires PSSs to perform a detailed risk analysis for all the significant potential terrorism targets (vessels, facilities, and offshore platforms) operating within their area of responsibility across a spectrum of physical attack modes.

Risk within MSRAM is assessed for scenarios, which represents a combination of a target and attack mode. For each scenario, analysts score numerous threat, vulnerability, and consequence factors to estimate the risk. Figure 3 illustrates the MSRAM risk methodology.

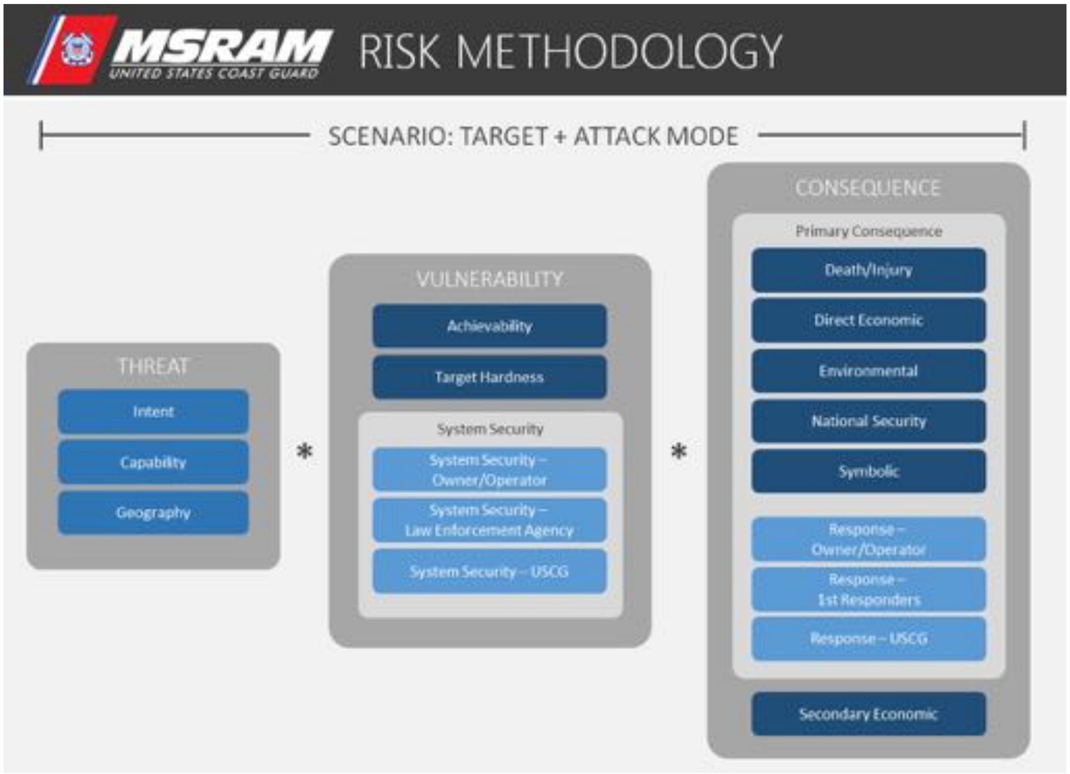


Figure 3. MSRAM Risk Methodology

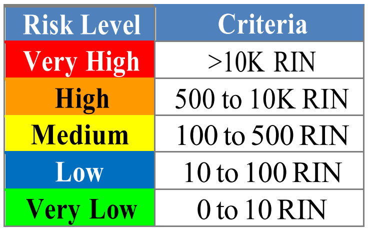
The MSRAM methodology requires analysts to score several factors in three major categories:

- **Threat** *(relative likelihood of attempt)***.** Intelligence analysts from the USCG Intelligence Coordination Center (ICC) develop quantitative, relative threat estimates for each unique combination of asset class and attack mode for each USCG Sector, providing geographic differentiation.
- **Vulnerability** *(probability of a successful attack, given an attempt)***.** Sector PSSs estimate the vulnerability of each target to each attack using several factors, including the innate difficulty of the attack, the protections offered by the owner/oper-

ator, local law enforcement, and USCG forces, and the ability of the target to withstand the attack. Vulnerability is defined as the probability of a successful attack, given an attempt.

- **Consequence** *(consequence points)*. Sector PSSs estimate the reasonable worst-case consequences that could result from a successful attack on each target from each attack by scoring a spectrum of potential impacts: deaths/injuries, primary economic impacts, environmental impacts, national security impacts, symbolic impacts, and the effects on the national economy. They also estimate emergency response mitigation of consequences based on the capabilities of the owner/operator, local first responders, and the USCG.

MSRAM calculates the risk for each scenario as a product of threat, vulnerability, and consequence factor scores. The result is a relative expected loss risk score, expressed in units of Risk Index Number (RIN), for each scenario. Scenarios are then mapped into one of five risk levels (Figure 4) based on their risk scores. Risk levels are used in many applications to help the USCG and its partners focus their resources on *very high* and *high*-risk scenarios.



Risk Level	Criteria
Very High	>10K RIN
High	500 to 10K RIN
Medium	100 to 500 RIN
Low	10 to 100 RIN
Very Low	0 to 10 RIN

Figure 4. MSRAM Risk Levels

The results of the MSRAM process yield a robust national dataset currently containing risk information for over 48,000 assets and 150,000 scenarios. This dataset is leveraged to inform a wide variety of risk management decisions, both inside and outside the USCG, at the local, regional, and national levels.

Challenges in Cybersecurity Risk Assessment

Developing accurate risk estimates for physical security assessments is very difficult but doing so for cybersecurity is even more challenging. Technology changes quite rapidly and threats in the cyber environment are extensive and multifaceted. Applying the MSRAM approach to cyber risk assessment is challenging and could possibly be misleading:

- Is “Threat” a person, a type of attack, the named intrusive software application, or a specific line of code?
- Is “Vulnerability” a point in a network at which malware can intrude, an open USB port, or a misconfigured firewall?
- Is a “Consequence” a description of the event caused by a cyber incident, or is it lost money?

In a 2010 article, Jeff Lowder *(http://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/)* wrote that applying the T*V*C risk equation in information security risk analysis (ISRA) is “mathematical nonsense”. He summed up his discussion by commenting: *“the formula is not literally intended to be used as a mathematical formula; rather, the formula is just an informal way of stating that security risk is a function of threats, vulnerabilities, and potential impact.”*

If that is so, the MSRAM risk equation is marginally useful to a cybersecurity practitioner.

When contemplating the issue of describing risk more precisely, research shows that much of cybersecurity is focused on threat versus risk management. Security processes and procedures tend to focus on threat recognition, resolution, and removal. A market analysis of commercial cybersecurity products and services reveals the market's focus on unified threat management (UTM).

The difficulty with focusing on threat is that real-life expressions of a threat may not recognizable until the threat has manifested (e.g., "The X-virus was discovered on our system today and infected 35 computers on two networks.")

Also, the current understanding of threat does not lend itself to quantification. Threats are often characterized qualitatively as:

1. The penetration mode: how the threat enters a computer) or
2. The carrier of the threat (i.e., email) or
3. The name of the threat: Stuxnet, ILOVEYOU, GoldenEye, etc.

None of these characteristics readily lend themselves to being expressed mathematically in a risk equation. This in turn makes the result of the risk equation a subjective number that provides limited uses for comparison to other subjective results based on similar assumptions.

Even with these concerns understood, the risk equation remains useful as a tidy mental model for intuitively understanding that risk is "made up" of three components. Adding to this general utility, it also infers that if just one of those three things is removed from the equation, risk can be eliminated.

These are important concepts, but the research team challenged the assumption that the removal of threat, vulnerability, or consequence does, in fact, eliminate risk. The underlying notion of these three components combining to create risk is an accepted premise. However, the question remains: Does removal or reduction of just one of those conditions reduce or eliminate risk in practice? The research team's answer is: *probably*.

For example, reduction or elimination of consequences of a successful attack makes a system an unattractive target to attackers, and probably not worth protecting from malicious or unintentional system corruption. If the consequence of loss or damage is eliminated, why bother to protect it?

Reduction or elimination of vulnerability makes the system unavailable to a threat through a path; thereby, eliminating risk. Finally, reduction or elimination of threat logically reduces risk, because if there is no adversary attempting to exploit a system, there is no risk to the system.

So, the research team believes the classic risk equation makes logical sense, and the reduction or removal of any one of the three elements does reduce risk. Combination of threats, vulnerabilities, and consequences do appear to be necessary and sufficient to yield risk.

Next, the research team considered the potential conflict of the utility of the classic risk equation as a useful logical model versus the issue that, when applied quantitatively, it might result in "mathematical nonsense".

Ultimately, cybersecurity stakeholders *need* a quantitative risk estimate to determine relative risk between assets or between alternative security solutions. So, the research team developed an approach to this simple question:

> *"How can the classic risk equation be logically expressed based on closely-related real-world cybersecurity elements that can be quantified using available technological and management solutions?"*

Put simply, can a useful approach be developed for maritime cybersecurity that is (1) consistent, (2) clarifying, and (3) countable?

Reference Model

The research team recognized a familiar concept when considering the components of the MSRAM risk model separate from its mathematical formulation. Cybersecurity risk appears to have probabilistic and set theory characteristics. Lowder reinforces this notion when he states: "…*risk analysis, including ISRA, has its roots in decision theory, especially expected value (or utility) theory. The expected value or utility of an action may be thought of as a weighted average. It can be calculated by defining a set of mutually exclusive and jointly exhaustive possible outcomes from a particular course of action, and then multiplying the probability of each possible outcome by its utility. The formula is very clear and mathematically rigorous."*

That is a strong indictment of applying the standard security risk formula to cybersecurity. The research team agrees with Lowder's conclusion, but believes that the underlying relationships are powerful, logically (if not mathematically) supportable, and arguably useful.

Triads

Conceptual triads are easy to find in science, engineering, and philosophy. In researching conceptual triads, a comparable construct was identified: The Fire Triangle **(**Figure 5)**.** The conceptual abstraction as represented by the risk equation is remarkably similar in nature to the fire triangle elements – even directly analogous in ways.

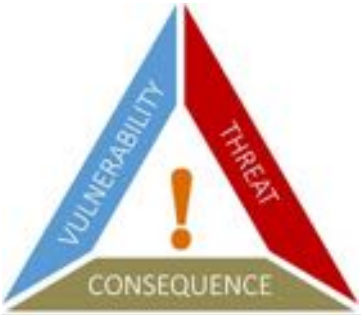


Figure 5. The Fire Triangle

- **Fuel** represents the material consumed by the fire
- **Oxygen** represents the enabling environment for starting and sustaining fire
- **Heat** represents the incidental condition that causes fire

Logically, the components of the security risk equation can replace the fire triangle elements (Figure 6).

Consequence replaces fuel as the end goal of a cyber-attack. Without an attractive target, the attack is random and purposeless. So, the presence of consequence fuels and is ultimately consumed by the cyber-attack.

Vulnerability replaces oxygen as the environment variable. As oxygen supports fire, vulnerabilities enable and "feed" a cyber attack

Threat replaces heat as the initiator of the unwanted event. As oxygen and fuel peacefully coexist until Heat enters the system, vulnerability and consequence coexist without risk until threat is present.

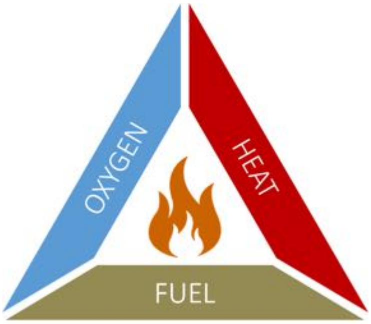


Figure 6. Security Risk Triangle

The similarities in these models for two very different systems are interesting and possibly useful. But, the issue remains that consequence, vulnerability, and threat, are not readily countable. To take it one step further, these models can be extended to the basic elements of cybersecurity (functions, connections, and identities).

Functions, if compromised, can result in negative consequences including safety, economic, and environmental impacts.
Connections, if not properly controlled, create an environment that enables or foments malicious or careless activity
Identities, if untrusted, can intentionally or accidentally introduce threats into the system.

Reconceiving the security risk triangle in this way has merit, because it is: (1) consistent with the components of the standard security risk equation, (2) analogous to a ubiquitous and well understood mental model, and (3) countable which enables quantification of risk.

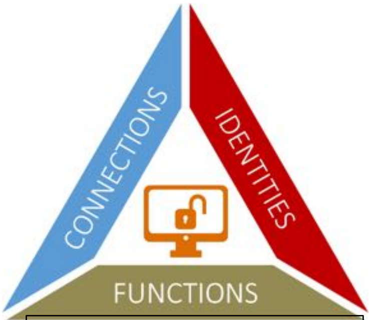


Figure 7. Cybersecurity Risk Triangle

Taxonomy

By representing consequence as impacted functions, vulnerability as connections, and threat as identity, the security risk equation becomes tractable for a variety of applications. By systematically identifying, counting, and assessing functions, connections, and identities, cybersecurity stakeholders can dramatically improve their decision making.

- Cybersecurity system designers can rapidly develop a specialized taxonomy of "things to understand."
- Auditors/assessors can develop a specialized taxonomy of "things to observe and review."
- Risk managers to develop a specialized taxonomy of "things to control, manage, and improve."

- Regulators to develop a specialized taxonomy of “things to look for or require.”

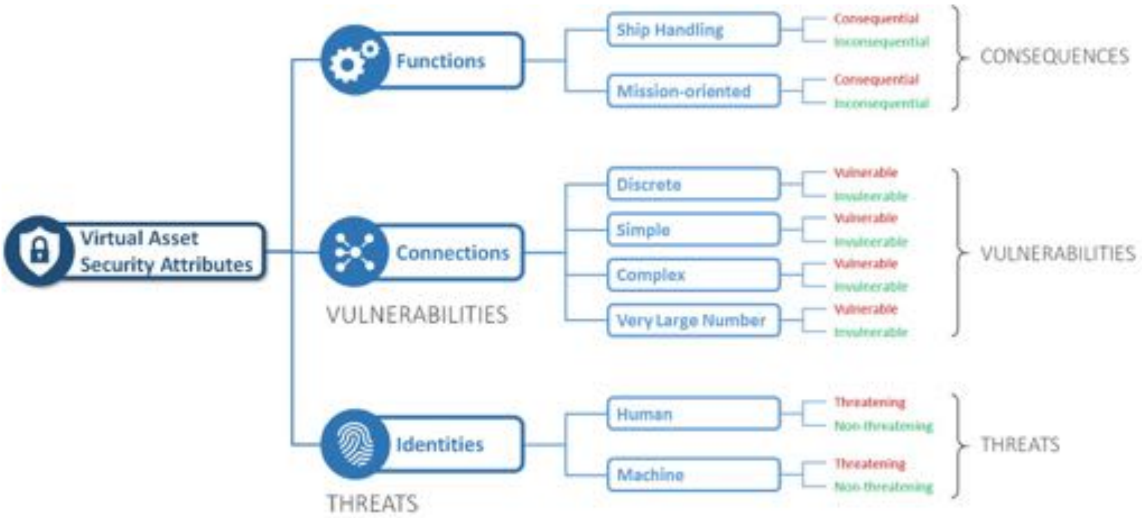


Figure 8. Cybersecurity Risk Assessment Reference Model

Functions

All ship handling and mission-oriented functions[1] residing within the protective sphere of cybersecurity must be identified for a maritime asset. This includes OT systems linked through communicating connections. Each function should be assessed as either (1) consequential or (2) inconsequential. The specific criteria and threshold for these categories must be determined by each organization to align with organizational risk tolerances. At a minimum, based on USCG policy guidance, any compromised function that could result in deaths, injuries, environmental spills, or major disruption to port operations should be considered consequential. Most organizations will also be interested in compromised functions that could result in major data loss, compliance violations, or significant business interruptions.

Note: A “Function” can be characterized with a quantitative “if-lost” value. For example, if-lost value can be the replacement or repair cost of the function alone, or a combination of derivative costs such as lost production, civil lawsuits due to loss of life, environment damage fines and remediation, etc.

Connections

Connections for each consequential function should be categorized as one of the following:

1. **Discrete** – A single (1:1) digital connection only between a single equipment controller and a single piece of controlled equipment.

[1] This research argues in favor of classifying the Internet as a virtual “Machine” being accessed by billions of untrusted identities.

2. **Simple** – More than one connection between a single equipment controller and more than one other equipment controllers, but NOT through a network.
3. **Complex** – More than one digital connection to a network linking only equipment controllers and associated interfaces.
4. **VLN** – Any of the above type connections that are also connected to the Internet or any potentially accessible proprietary wireless connection.

These connections are further assessed to identify nodes that are accessible by an identity (vulnerable), or not (invulnerable). Examples of invulnerable connections, include:

- A physical blocking device,
- A compensating protection (i.e., a locked room),
- A software security application that monitors digital activity, recognizes any unauthorized activity as anomalous and potentially threatening, and blocks the activity and/or generates an alert so that a responder can positively react to protect the connected system from intrusion. Examples of anomalous activity include, but are not limited to:
- Multiple failed logon attempts,
    - i. Out-of-pattern repeated logons
    - ii. Out-of-pattern logged on durations
    - iii. Out-of-pattern messaging activity

Identities

Lastly, the model calls for observing all identities having interactions with the communications nodes and designating those identities as “Threatening” or “Non-threatening”. In common cybersecurity terms, this mean trusted or untrusted identities. The issue of determining the constraints or parameters for designating an identity as threatening or non-threatening calls for deeper research; however, in practice this issue can initially be resolved by observing the identities of people who have authorized access to protected system, and the machines that are authorized to communicate with the protected system.

The underlying question needing deeper research is, “Are the trust/threat-indicator requirements placed on humans and machines that are authorized to access critical vessel and port operational technology functions sufficient?” Additionally, the designation of human identities as “untrusted” should be defined as untrusted and capable of malicious intent, and/or untrusted due to inadequate security training and supervision.

A digital machine or human identity is considered non-threatening or trusted if it is recognized in formal access documentation as an identity authorized to access defined (named) access points and is provisioned with appropriate access credentials. Examples of access credentials include, but are not limited to:

- Managed and protected passwords
- Identification credentials (badge, inventory identification, digital identification, etc.)
- Multifactor access credentials or tokens
- Trained in cybersecurity policies and procedures

- Temporary access authorization credentials (e.g., permissions for suppliers)

All other connection identities are considered threatening or untrusted.

Research indicates that human identities who are (or should be) considered untrusted by inadequate training are implicated in more security events than are unauthorized (malicious) actors. These nuanced issues are not addressed in this research, therefore the designation of “threatening” or non-threatening” is judgmental and subjective, but the indicators for a practical determination are not. If the identity is provided access based on access permissions policy and procedures and is on the authorized list of identities, then the identity is considered trusted, and therefore “Non-threatening”

However, if the identity is designated as trusted by being on the authorized list of identities but is not on the list of identities trained in security procedures, then that identity may be deemed as untrusted/threatening because it may promote a security incident due to careless or untrained procedural execution.

Summary

Table 1. Cybersecurity Risk Taxonomy Elements

Component	Categories	Values
Functions	• Ship Handling • Mission-oriented	• Consequential • Inconsequential
Connections	• Discrete • Simple • Complex • VLN	• Vulnerable • Invulnerable
Identities	• Human • Machine	• Threatening • Non-threatening

It is important to observe that all the risk taxonomy elements can be counted and characterized with a binary condition. This is a major simplifying characterization that is intentional in that it allows for a more transparent, more understandable calculation. It also yields to an assumption that dealing in probabilistic characteristics does not significantly improve the usefulness. Further, assigning values to indicate degree of risk associated with increasing or decreasing counts of the elements is experience-based and should be validated with “real-world” data. However, in that the model and related calculations resolve as an index, the values driving degree of risk can be altered based on both empirical data and modeling convenience.

Calculation

This section provides a way to apply the taxonomy, discussed earlier in this report, as a calculation based on the standard security risk equation to generate a risk index.

Cybersecurity Risk Index = Functions x Connections x Identities
where:

Functions: critical functions connected through digital communications links, considering:

- Function critical to preventing consequential impacts (e.g., critical to safe operations)
- Digital communication architecture linking functions as function sets
- Cardinality of linked function sets

Connections: digital access points (nodes) associated with function sets

- Access points penetrable by digital devices
- Access points penetrable by humans

Identities: Machine and human identities that can access a node

- Untrusted human identities
- Untrusted machine identities

To treat these variables mathematically, each is expressed numerically by counting the number of instances of each within a virtual asset.

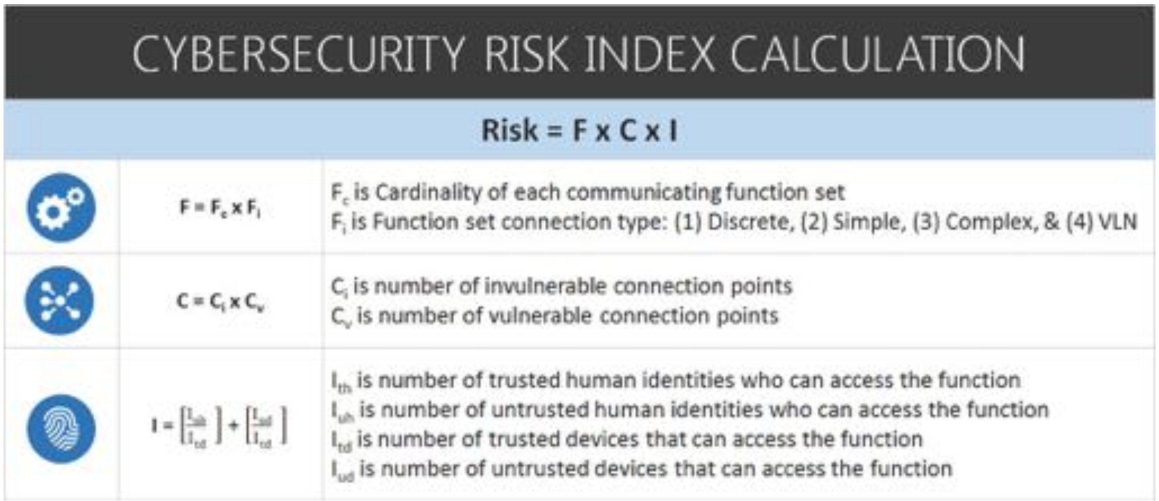
Special Case of the VLN Connection

An important idea within this risk taxonomy is the idea of the VLN connection type. When describing or reviewing the virtual asset architecture, any VLN connection to a function or function set should be identified. This is important because when the VLN connection is added to any other connection type, that connection type adopts VLN computational risk characteristics and therefore becomes a VLN connection.

Although the VLN is listed as a Connection, it also bears consideration as an Identity because of the threat posed by the potential for a very large number of unauthorized (i.e., untrusted) identities accessing connected system each time an onboard identity logs on to a website located on the Internet or any other wireless network. Further, even though connection with a very large number of unauthorized wireless network identities is possible, the user realistically connects with one (or a relatively small number of) machine identity at a time. This idea is captured computationally in the taxonomy model by adding one unauthorized machine identity for each authorized or unauthorized onboard identity that can connect through the VLN. The mathematical influence within the model is to raise risk for each onboard identity that can connect with a mirrored unauthorized identity through a VLN connection.

This approach is recognized as a simplistic treatment of risk created by a VLN connection. It certainly deserves more research. But in the model as presented with this approach accomplishes the purpose of directing the attention of a model user to the connections and identities associated with the VLN connection.

The calculation shown in Figure 9 generates a relative risk score for each function set and an overall score for the virtual asset itself.



CYBERSECURITY RISK INDEX CALCULATION

	Risk = F x C x I	
	$F = F_c \times F_i$	F_c is Cardinality of each communicating function set F_i is Function set connection type: (1) Discrete, (2) Simple, (3) Complex, & (4) VLN
	$C = C_i \times C_v$	C_i is number of invulnerable connection points C_v is number of vulnerable connection points
	$I = \left[\frac{I_{uh}}{I_{td}}\right] + \left[\frac{I_{ud}}{I_{td}}\right]$	I_{th} is number of trusted human identities who can access the function I_{uh} is number of untrusted human identities who can access the function I_{td} is number of trusted devices that can access the function I_{ud} is number of untrusted devices that can access the function

Figure 9. CRI Calculations

Figure 10 illustrates several representative functions for a tank ship, and how they are implemented using various onboard networks. This example tank ship will be used to illustrate how the risk varies for different architecture options for the same functions (shown in upper right corner of each figure).

Example 1: Segmented Architecture (Figure 11). Nearly all safety-critical functions (except the *Navigation System*) are controlled by simple control systems that are isolated from *the IT & Crew Welfare Network* and the internet. Access to safety-critical system components requires physical connections through serial or Universal Serial Bus (USB) ports. This type of architecture has lower risk exposure than those that are more integrated.

Example 2: Integration of Safety-critical OT Systems (Figure 12). In this architecture option, the *Propulsion & Steering*, *Ballast*, and *Power Systems* have been integrated through an alarm management system to provide automated monitoring and alarms to crew. All the safety-critical functions are still isolated from the *IT & Crew Welfare Network* and the internet.

Example 3: Inadvertent Integration of IT & OT Systems (Figure 13). This architecture demonstrates how cyber risk can be inadvertently introduced through improper configuration. A printer is connected to the power system to periodically generate logs of system performance. The printer's wireless is not disabled resulting in an inadvertent connection to the *IT & Crew Welfare Network.* Based on the methodology, this connection results in adding the *Propulsion & Steering*, *Ballast*, and (3) *Power Systems* to the *IT & Crew Welfare Network* function set, which is categorized as VLN. This significantly increases cyber risk to the virtual asset

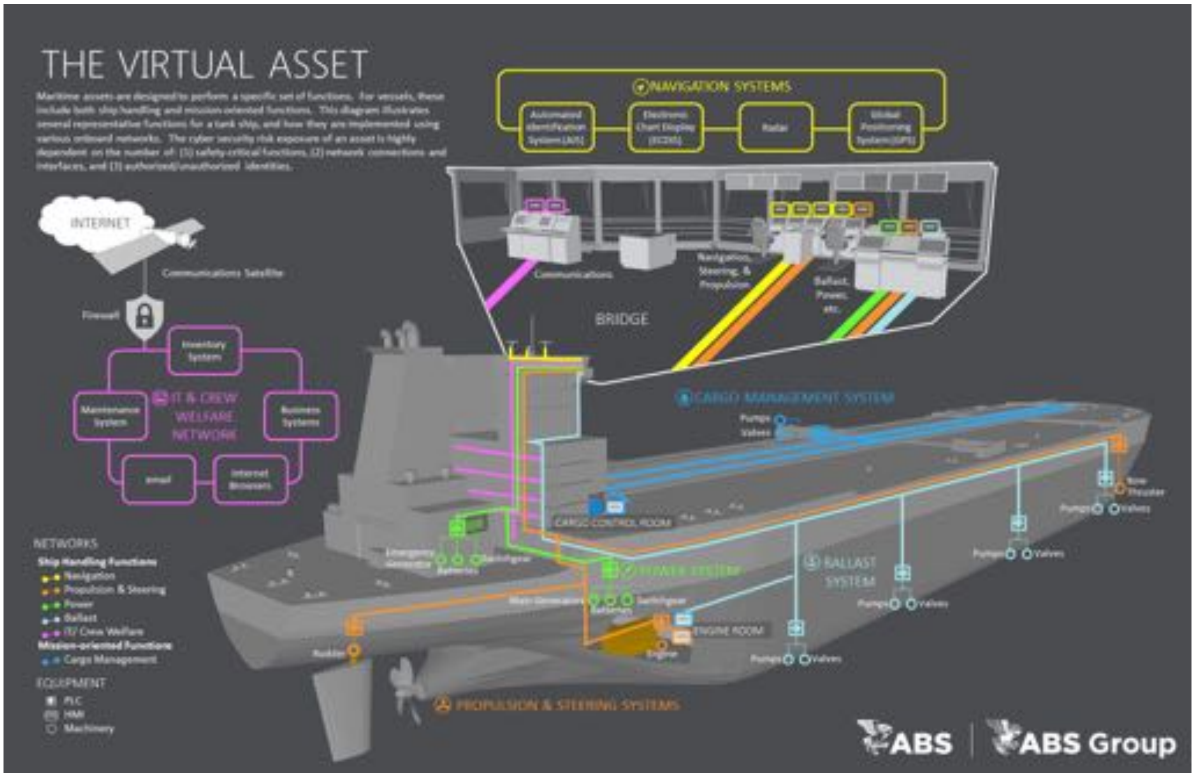

THE VIRTUAL ASSET
Maritime assets are designed to perform a specific set of functions. For vessels, these include both ship handling and mission-oriented functions. This diagram illustrates several representative functions for a tank ship, and how they are implemented using various onboard networks. The cyber security risk exposure of an asset is highly dependent on the number of: (1) safety-critical functions, (2) network connections and interfaces, and (3) authorized/unauthorized identities.
INTERNET
Communications Satellite
Firewall
Inventory System
Maintenance System
IT & CREW WELFARE NETWORK
Business Systems
email
Internet Browsers
NAVIGATION SYSTEMS
Automated Identification System (AIS)
Electronic Chart Display (ECDIS)
Radar
Global Positioning System (GPS)
Communications
Navigation, Steering, & Propulsion
Ballast, Power, etc.
BRIDGE
CARGO MANAGEMENT SYSTEM
Pumps
Valves
CARGO CONTROL ROOM
Emergency Generator
Batteries
Switchgear
POWER SYSTEM
BALLAST SYSTEM
Main Generator
ENGINE ROOM
Engine
Rudder
Bow Thruster
PROPULSION & STEERING SYSTEMS
NETWORKS
Ship Handling Functions
Navigation
Propulsion & Steering
Power
Ballast
IT/ Crew Welfare
Mission-oriented Functions
Cargo Management
EQUIPMENT
PLC
HMI
Machinery
ABS
ABS Group

Figure 10. Virtual Asset Diagram

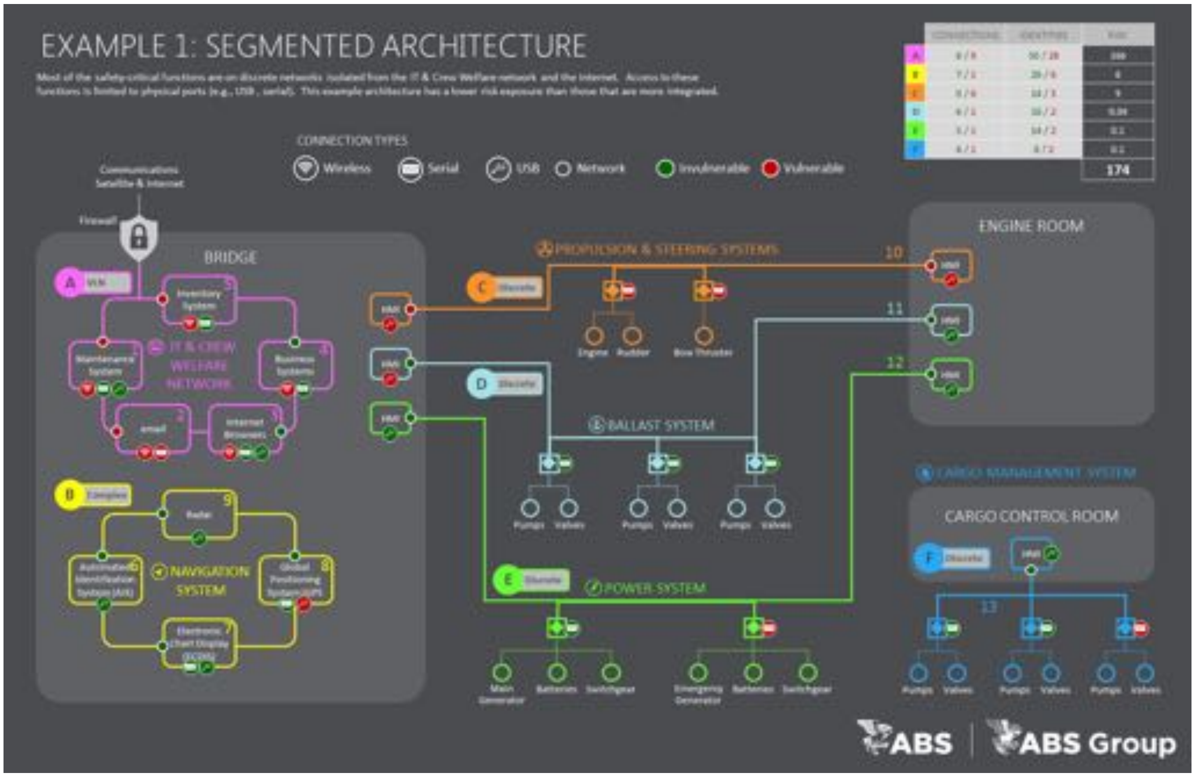
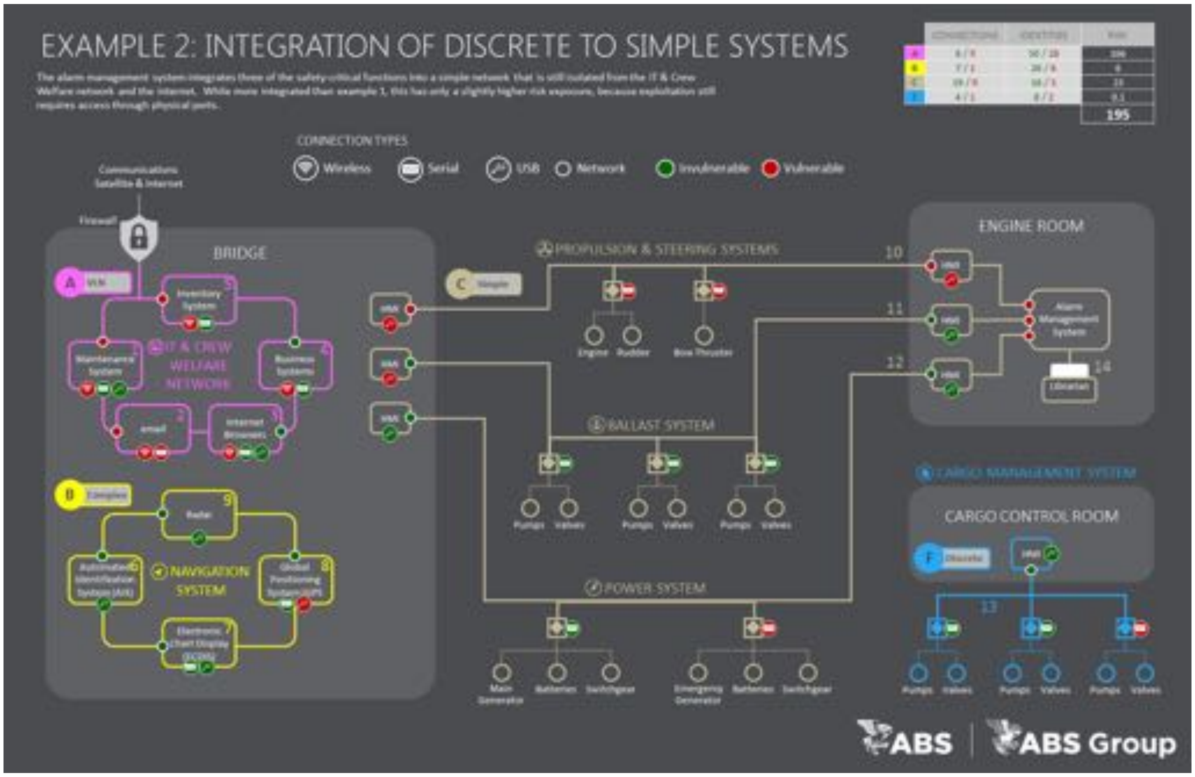
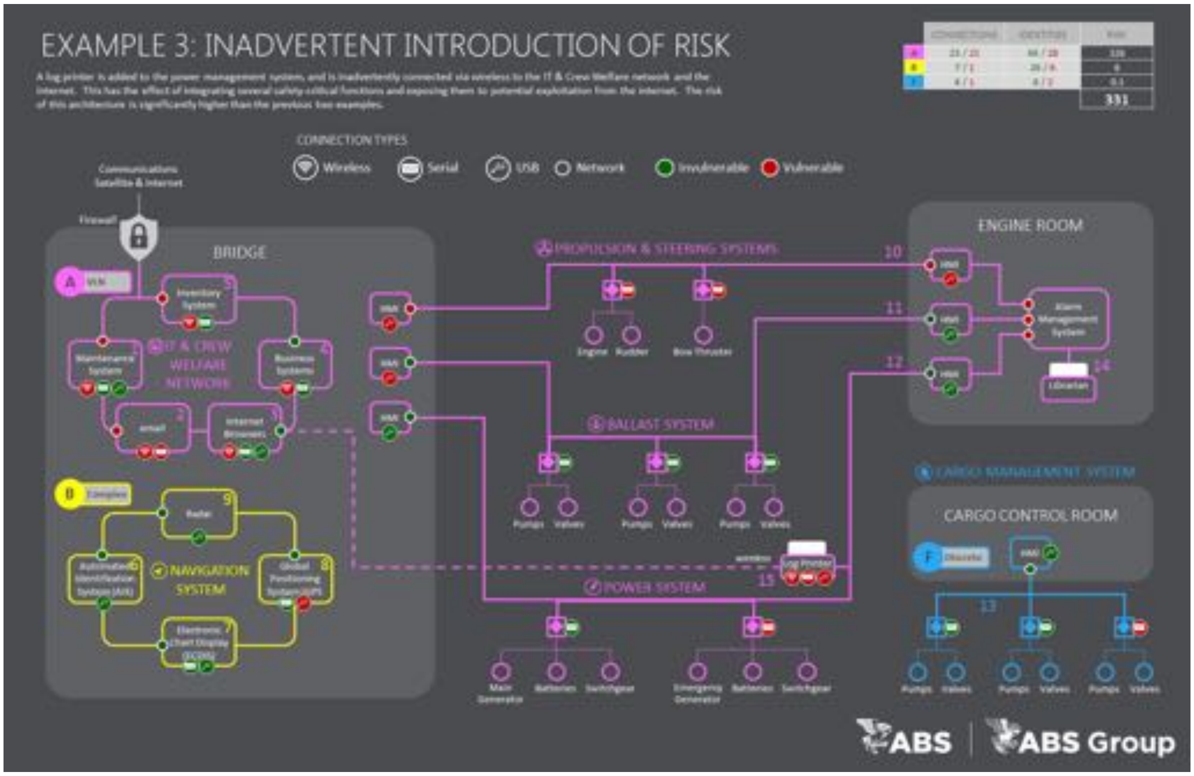

EXAMPLE 1: SEGMENTED ARCHITECTURE
Most of the safety-critical functions are on discrete networks isolated from the IT & Crew Welfare network and the Internet. Access to these functions is limited to physical ports (e.g., USB, serial). This example architecture has a lower risk exposure than those that are more integrated.
CONNECTION TYPES
Wireless
Serial
USB
Network
Invulnerable
Vulnerable
CONNECTIONS
IDENTITIES
A
B
C
D
E
F
174
Communications Satellite & Internet
Firewall
BRIDGE
A
B
Inventory System
Maintenance System
IT & CREW WELFARE NETWORK
Business Systems
email
Internet Browsers
Radar
Automated Identification System (AIS)
NAVIGATION SYSTEM
Global Positioning System (GPS)
Electronic Chart Display (ECDIS)
HMI
C
D
E
PROPULSION & STEERING SYSTEMS
Engine
Rudder
Bow Thruster
BALLAST SYSTEM
Pumps
Valves
POWER SYSTEM
Main Generator
Batteries
Switchgear
Emergency Generator
ENGINE ROOM
10
11
12
13
CARGO MANAGEMENT SYSTEM
CARGO CONTROL ROOM
F
ABS
ABS Group

Figure 11. Example 1: Segmented Architecture



The alarm management system integrates three of the safety-critical functions into a simple network that is still isolated from the IT & Crew Welfare network and the internet. While more integrated than example 1, this has only a slightly higher risk exposure, because exploitation still requires access through physical ports.

Figure 12. Example 2: Integration of Safety-critical OT Systems



A log printer is added to the power management system, and is inadvertently connected via wireless to the IT & Crew Welfare network and the internet. This has the effect of integrating several safety-critical functions and exposing them to potential exploitation from the internet. The risk of this architecture is significantly higher than the previous two examples.

Figure 13. Example 3. Inadvertent Integration of IT and OT Systems

The research team developed a spreadsheet evaluation tool to observe attribute inputs and perform the risk calculations. The tool enables capture of the following inputs:

- Categorization and counts of essential functions
- Connection categorization of digital network architectural designs that enable communications among those Functions
- Counts of Function Sets as defined by Connection types
- Counts of cardinal members of each Function Set
- Counts of vulnerable and invulnerable Connection access points
- Counts of trusted and untrusted digital and human identities

Based on these inputs, the tool generates a variety of outputs to help users understand the virtual asset and its risk profile:

- Number of vulnerable and invulnerable connection access points onboard the asset
- Average cardinality of function sets onboard the asset
- Total functions onboard the asset
- Risk for each function onboard the asset (best used for troubleshooting security of each function)
- Average risk for each function onboard the asset
- Risk for each function set onboard the asset
- Average risk for each function set onboard the asset (best used to establish the overall asset risk)

See Appendix C-1 for a copy of a spreadsheet evaluation tool populated with the assessment data for the three example architectures.

The research team developed a spreadsheet evaluation tool to observe attribute inputs and perform the risk calculations. The tool enables capture of the following inputs:

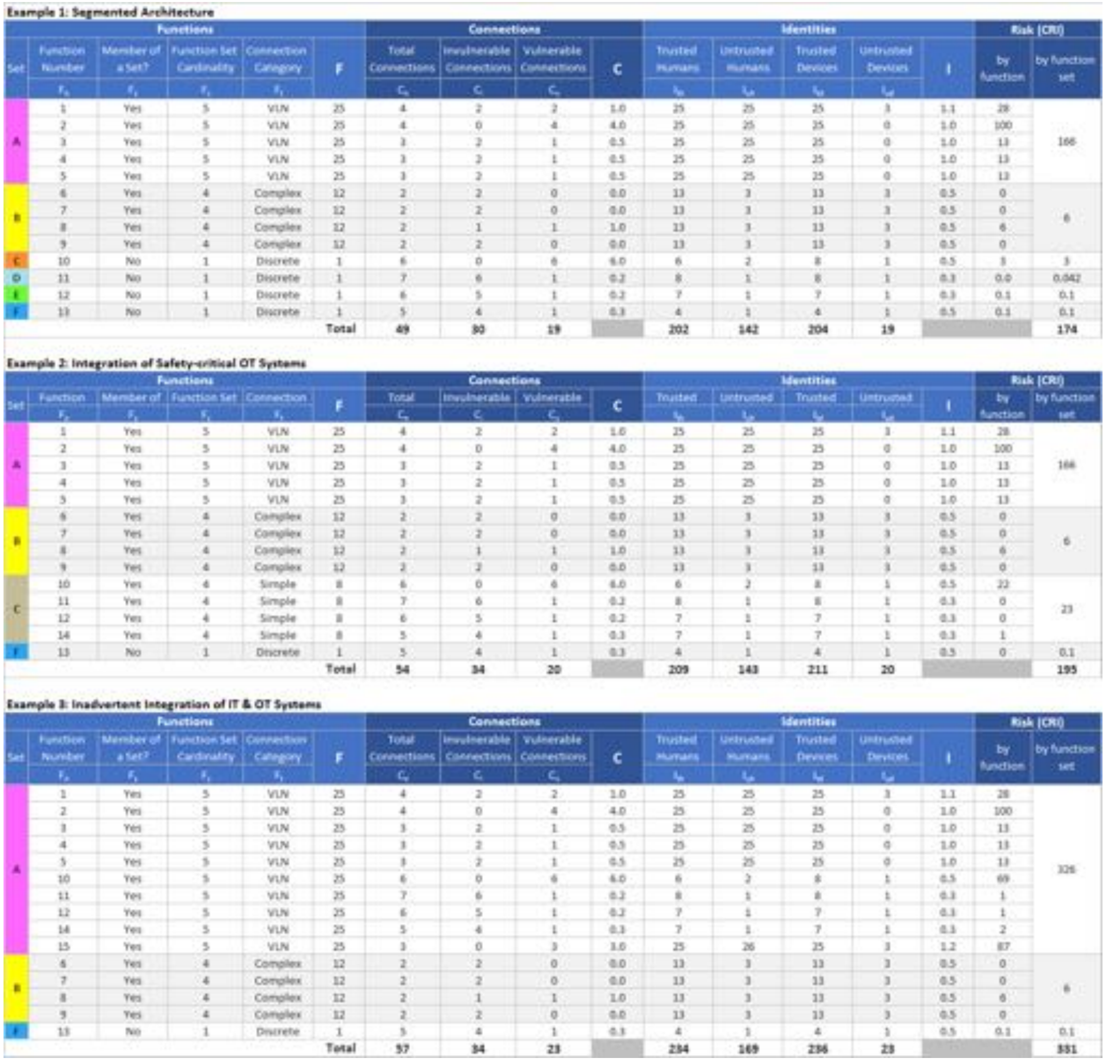
- Categorization and counts of essential functions
- Connection categorization of digital network architectural designs that enable communications among those Functions
- Counts of Function Sets as defined by Connection types
- Counts of cardinal members of each Function Set
- Counts of vulnerable and invulnerable Connection access points
- Counts of trusted and untrusted digital and human identities

Based on these inputs, the tool generates a variety of outputs to help users understand the virtual asset and its risk profile:

- Number of vulnerable and invulnerable connection access points onboard the asset
- Average cardinality of function sets on board the asset
- Total functions onboard the asset
- Risk for each function onboard the asset (best used for troubleshooting security of each function)

- Average risk for each function onboard the asset
- Risk for each function set onboard the asset
- Average risk for each function set onboard the asset (best used to establish the overall asset risk)

Figure 14 illustrates the spreadsheet evaluation tool populated with the assessment data for the three example architectures.



Example 1: Segmented Architecture

Functions						Connections				Identities					Risk (CRI)	
Set	Function Number	Member of a Set?	Function Set Cardinality	Connection Category	F	Total Connections	Invulnerable Connections	Vulnerable Connections	C	Trusted Humans	Untrusted Humans	Trusted Devices	Untrusted Devices	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	166
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
C	10	No	1	Discrete	1	6	0	6	6.0	6	2	8	1	0.5	3	3
D	11	No	1	Discrete	1	7	6	1	0.2	8	1	8	1	0.3	0.0	0.042
E	12	No	1	Discrete	1	6	5	1	0.2	7	1	7	1	0.3	0.1	0.1
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0.1	0.1
					Total	49	30	19		202	142	204	19			174

Example 2: Integration of Safety-critical OT Systems

Functions						Connections				Identities					Risk (CRI)	
Set	Function	Member of	Function Set	Connection	F	Total	Invulnerable	Vulnerable	C	Trusted	Untrusted	Trusted	Untrusted	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	166
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
C	10	Yes	4	Simple	8	6	0	6	6.0	6	2	8	1	0.5	22	23
	11	Yes	4	Simple	8	7	6	1	0.2	8	1	8	1	0.3	0	
	12	Yes	4	Simple	8	6	5	1	0.2	7	1	7	1	0.3	0	
	14	Yes	4	Simple	8	5	4	1	0.3	7	1	7	1	0.3	1	
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0	0.1
					Total	54	34	20		209	143	211	20			195

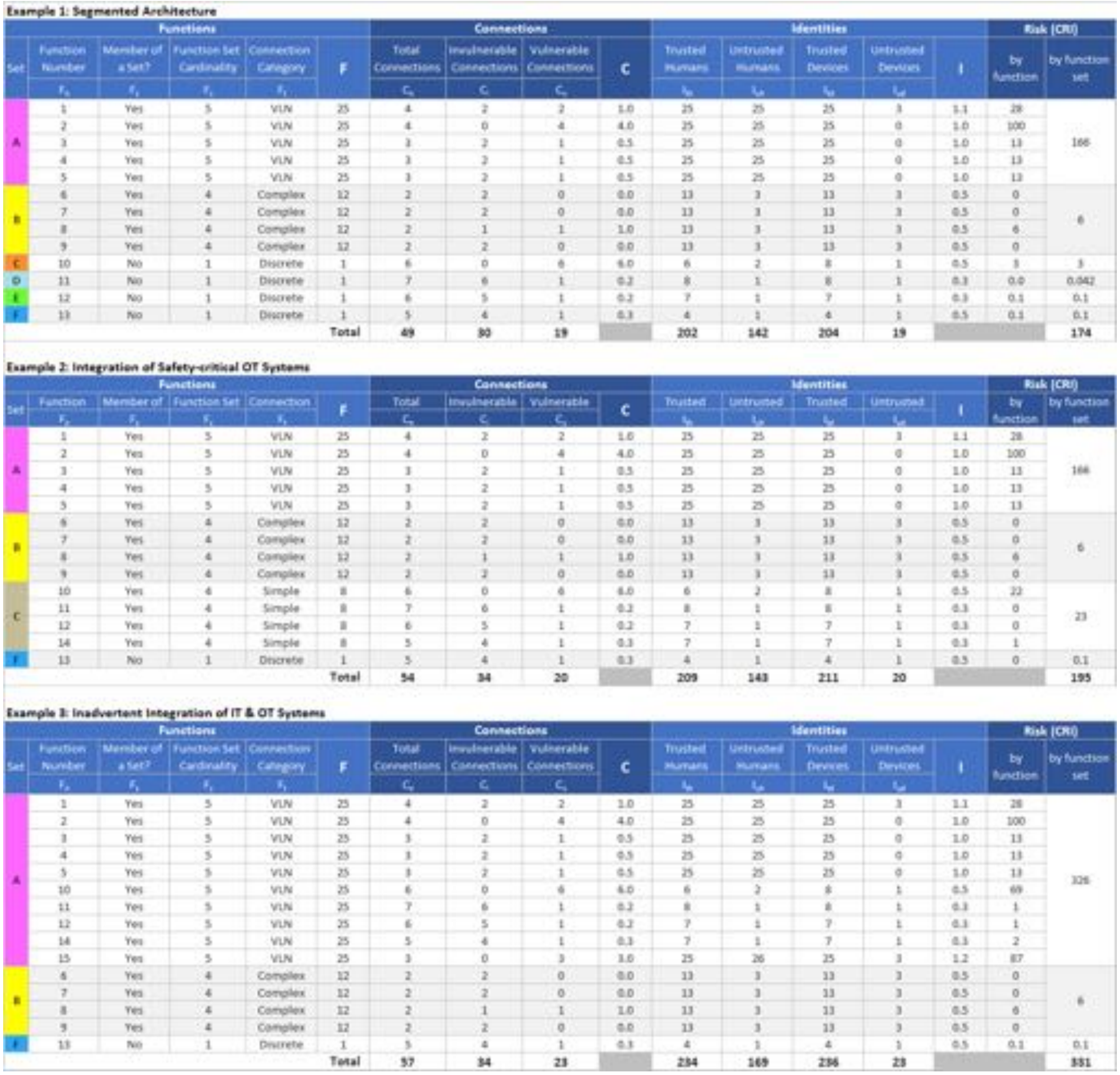
Example 3: Inadvertent Integration of IT & OT Systems

Functions						Connections				Identities					Risk (CRI)	
Set	Function Number	Member of a Set?	Function Set Cardinality	Connection Category	F	Total Connections	Invulnerable Connections	Vulnerable Connections	C	Trusted Humans	Untrusted Humans	Trusted Devices	Untrusted Devices	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	326
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	10	Yes	5	VLN	25	6	0	6	6.0	6	2	8	1	0.5	69	
	11	Yes	5	VLN	25	7	6	1	0.2	8	1	8	1	0.3	1	
	12	Yes	5	VLN	25	6	5	1	0.2	7	1	7	1	0.3	1	
	14	Yes	5	VLN	25	5	4	1	0.3	7	1	7	1	0.3	2	
	15	Yes	5	VLN	25	3	0	3	3.0	25	26	25	3	1.2	87	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0.1	0.1
					Total	57	34	23		234	169	236	23			331

Figure 14. Populated Spreadsheet Evaluation Tool for Example Architectures 1, 2, & 3

Outputs of the worksheet calculations are useful for various cybersecurity system remediation and design purposes. The two histograms are the resultant risk profiles for the three example architectures.

Figure 15 shows the relative risk for each function set for Example 1. Each bar is the summation of the risk for the member functions categorized by the function sets. These values can be used to prioritize potential remedial action for functions in the set, the network linking the functions within the set, the nodes providing access to the set, or the identities accessing the set. The observer can use the worksheet to analyze specific results and determine if the value(s) contributing to the overall result is an operational problem (e.g., untrusted identities) and/or a protection problem (e.g., unprotected nodes) – or, is a design problem such as large set sizes, complex connection types, or untrusted digital identities, such as mobile devices or the Internet. With minimal interpretation, analysts can identify and focus on potential corruption vectors and apply solutions to reduce risks.



Example 1: Segmented Architecture

	Functions					Connections				Identities					Risk (CRI)	
Set	Function Number	Member of a Set?	Function Set Cardinality	Connection Category	F	Total Connections	Invulnerable Connections	Vulnerable Connections	C	Trusted Humans	Untrusted Humans	Trusted Devices	Untrusted Devices	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	166
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
C	10	No	1	Discrete	1	6	0	6	6.0	6	2	8	1	0.5	3	3
D	11	No	1	Discrete	1	7	6	1	0.2	8	1	8	1	0.3	0.0	0.042
E	12	No	1	Discrete	1	6	5	1	0.2	7	1	7	1	0.3	0.1	0.1
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0.1	0.1
					Total	**49**	**30**	**19**		**202**	**142**	**204**	**19**			**174**

Example 2: Integration of Safety-critical OT Systems

	Functions					Connections				Identities					Risk (CRI)	
Set	Function	Member of	Function Set	Connection	F	Total	Invulnerable	Vulnerable	C	Trusted	Untrusted	Trusted	Untrusted	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	166
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
C	10	Yes	4	Simple	8	6	0	6	6.0	6	2	8	1	0.5	22	23
	11	Yes	4	Simple	8	7	6	1	0.2	8	1	8	1	0.3	0	
	12	Yes	4	Simple	8	6	5	1	0.2	7	1	7	1	0.3	0	
	14	Yes	4	Simple	8	5	4	1	0.3	7	1	7	1	0.3	1	
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0	0.1
					Total	**54**	**34**	**20**		**209**	**143**	**211**	**20**			**195**

Example 3: Inadvertent Integration of IT & OT Systems

	Functions					Connections				Identities					Risk (CRI)	
Set	Function Number	Member of a Set?	Function Set Cardinality	Connection Category	F	Total Connections	Invulnerable Connections	Vulnerable Connections	C	Trusted Humans	Untrusted Humans	Trusted Devices	Untrusted Devices	I	by function	by function set
	F_n	F_s	F_c	F_t		C_t	C_i	C_v		I_{th}	I_{uh}	I_{td}	I_{ud}			
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	3	1.1	28	326
	2	Yes	5	VLN	25	4	0	4	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	5	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	10	Yes	5	VLN	25	6	0	6	6.0	6	2	8	1	0.5	69	
	11	Yes	5	VLN	25	7	6	1	0.2	8	1	8	1	0.3	1	
	12	Yes	5	VLN	25	6	5	1	0.2	7	1	7	1	0.3	1	
	14	Yes	5	VLN	25	5	4	1	0.3	7	1	7	1	0.3	2	
	15	Yes	5	VLN	25	3	0	3	3.0	25	26	25	3	1.2	87	
B	6	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	6
	7	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
	8	Yes	4	Complex	12	2	1	1	1.0	13	3	13	3	0.5	6	
	9	Yes	4	Complex	12	2	2	0	0.0	13	3	13	3	0.5	0	
F	13	No	1	Discrete	1	5	4	1	0.3	4	1	4	1	0.5	0.1	0.1
					Total	**57**	**34**	**23**		**234**	**169**	**236**	**23**			**331**

Figure 15. Populated Spreadsheet Evaluation Tool for Example Architectures 1, 2, & 3

Outputs of the worksheet calculations are useful for various cybersecurity system remediation and design purposes. The two histograms are the resultant risk profiles for the three example architectures.

Figure 16 shows the relative risk for each function set for Example 1. Each bar is the summation of the risk for the member functions categorized by the function sets. These values can be used to prioritize potential remedial action for functions in the set, the network linking the functions within the set, the nodes providing access to the set, or the identities accessing the set. The observer can use the worksheet to analyze specific results and determine if the value(s) contributing to the overall result is an operational problem (e.g., untrusted identities) and/or a protection problem (e.g., unprotected nodes) – or, is a design problem such as large set sizes, complex connection types, or untrusted digital identities, such as mobile devices or the Internet. With minimal interpretation, analysts can identify and focus on potential corruption vectors and apply solutions to reduce risks.

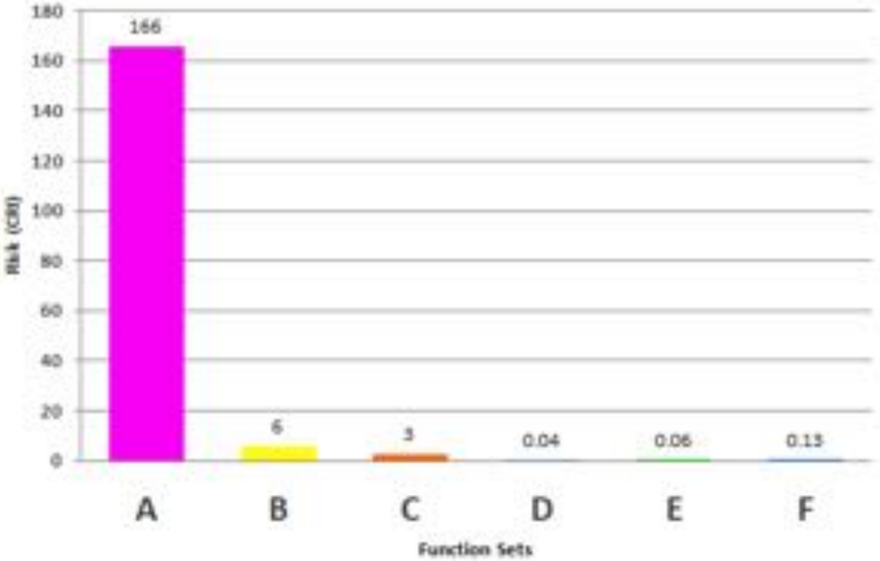


Figure 16. CRI for Each Function Set

Figure 17 provides risk results at the next level of detail for individual Functions. The example below provides very clear indication of which individual functions contribute the most risk to the control system and should therefore be given priority in a security improvement program. By focusing on only 15% – 23% of the control system functions, the overall security of the system can be improved significantly. For example, by looking at the detailed data, an analyst can quickly recognize that the number of untrusted identities that can access the function, only a single access point that is vulnerable, and membership in a 7-Function Set make that Function a high risk to the system. Close inspection of the function may provide insights that justify the design and operational choices; however, management is alerted to the potential risk inherent in those choices and can make an informed decision about remedial actions.

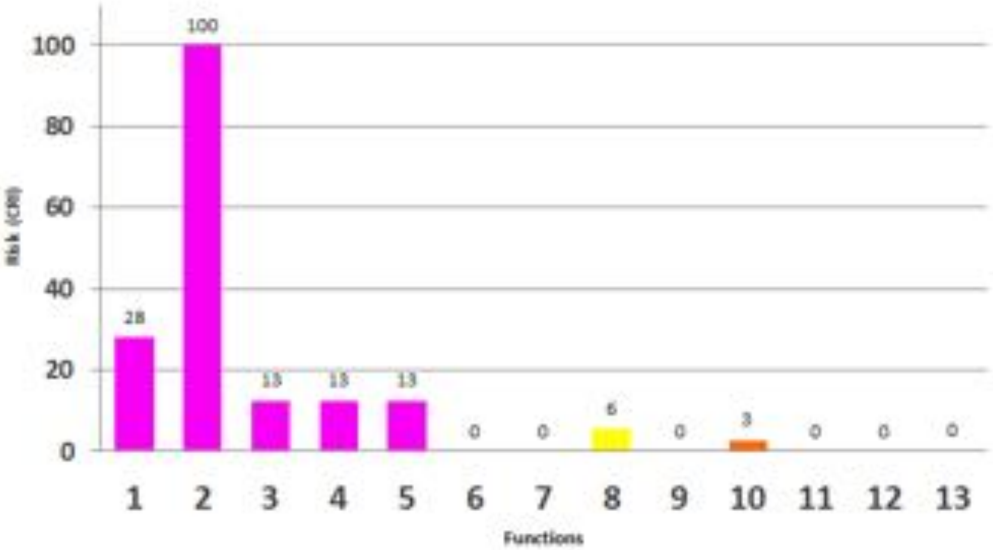


Figure 17. CRI for Each Function

Application

The risk metrics presented above provide a few examples of how countable indicators of risk can be applied, but there are many other applications. The model elements of Functions-Connections-Identities can be further deconstructed to yield more specific (and arguably useful) types of information. The simplistic view of function sets can be supplanted by set theory calculations that could include set ordinals ranked based on relative criticality of each set member, and therefore prioritize countermeasure expenditures on protections within sets. With more research and empirical validation, the risk values associated with nodes can be varied based on node types (e.g., HMI, serial port, USB port, or wireless). The same is true for connection types. The relative risk factor selections associated with connection types in the example case should be subjected to real-world examples and experimentation. Complex and VLN Connection types may be far riskier than the current multiplier factors examples indicate. Research and experimentation is needed to refine the factors.

Lastly, the notion of “Identity-as-Threat” merits much more research. When critically reviewed, the MTSA regulation stresses the need for strict identity management of humans, vessels, and cargo. However, the regulations offer little guidance for human-related identity management parameters that clarify the meaning of “trusted identities” for personnel and provides no guidance on management parameters for machine trusted identities.

In the simple form presented in this research, the notion of human identity is binary at only two evidential observation points. At the first point, trust is defined by the question, “Is the accessing person on the authorized access list, or not?” At the second point, trust is further defined by the question, “Is the person in the learning management system record as having been trained in cybersecurity, or not?” If those questions are both answered affirmatively, the human identity is declared to be trusted; but, this simple model provides no guidance or deeper insight into trust verification and validation points based on role (need to access), background checks, access minimization, access profiling, etc. Further, the implications of Identity-as-Threat are sufficiently important now, when human identity trust determination is mostly referring to onboard crew. As autonomous vessels come into widespread use, and as identity security becomes more of a shore-based issue, these and other identity management issues will become even more critical.

Equally critical are machine or digital identity issues. At the top of machine identity risk is arguably the Internet. It is best understood as a virtual machine containing billions of untrusted identities. It increasingly accesses vessels and OT systems. Vendors may connect to assets over the internet for remote condition monitoring and maintenance. Mobile wireless devices can access vessel functions and the internet. The lowest level of machine identity is possibly a USB drive. It represents a machine identity that can, and frequently has, bridged the air gap between systems.

From the Internet to the USB memory stick, digital machines must be trusted or regarded as threats and excluded from accessing critical systems. As with humans, machine identities must be trusted, or considered a threat.

Conclusion

In conclusion, the taxonomy and tool presented in this section are useful; but, deeper research and real- world application is needed to refine the approach. The model provides traction for continued development of quantifiable and actionable information to decision makers. It is intended to focus cybersecurity research and practice on patterns and potential sources of readily observable characteristics of the virtual asset, but even more importantly, it is intended to provide a consistent, clarifying, and countable method for organizing thinking about maritime cybersecurity risk.

2.2.3. Requirements for a Cyber Range

A well designed and implemented cyber range is a valuable capability for an organization to have to simulate their networks and applications, spanning both IT and OT, to improve their cybersecurity posture. Organizations can use ranges for a wide variety of purposes from application testing to vulnerability identification and mitigation.

These simulated environments provide a safe and secure environment to assess their capabilities and learn and optimize performance of cybersecurity measures. They are an essential part of research and development where new monitoring strategies can be conceived and tested for efficacy. They can simulate cyber events for exercises to train personnel-in real time response and recovery actions.

The scale of cyber ranges can vary dramatically from small-scale representations of systems to simulated environments of the entire enterprise. They can include actual or virtual hardware and software components, and depending on the scope, they can simulate network services and internet traffic.

The following sections will identify potential applications of cyber ranges to support USCG strategic priorities, identify and summarize the capabilities of several relevant cyber ranges in operation, and provide recommendations for the USCG going forward.

Strategic Priorities

In its Cyber Strategy which was published in June 2015, the USCG identified three strategic priorities crucial to the service's mission:

1. Defending Cyberspace. Secure and resilient USCG IT systems and networks are essential for overall mission success. To ensure the full scope of USCG capabilities are as effective and efficient as possible, the USCG must serve as a model agency in protecting information infrastructure and building a more resilient USCG network.

2. Enabling Operations. To operate effectively within the cyber domain, the USCG must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations, inside and outside USCG information and communications networks and systems, can help detect, deter, disable, and defeat adversaries. Robust intelligence, law enforcement, and maritime and military cyber programs are essential to enhancing the effectiveness of USCG operations, and deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure. USCG leaders must recognize that cyber capabilities are a critical enabler of success across all missions and ensure that these capabilities are leveraged by commanders and decision-makers at all levels.

3. Protecting Infrastructure. Maritime critical infrastructure and the MTS are vital to our economy, national security, and national defense. The MTS includes ocean carriers, coastwise shipping along our shores, the Western Rivers and Great Lakes, and the Nation's ports and terminals. Cyber systems enable the MTS to operate with unprecedented speed and efficiency. Those same cyber systems also create potential vulnerabilities. As the Maritime Transportation Sector Specific Agency (as defined by the National Infrastructure Protection Plan), the USCG must lead the unity of effort required to protect maritime critical infrastructure from attacks, accidents, and disasters.

Strategic priority 1 could benefit from a cyber range capable of simulating USCG systems and networks. In such an environment, personnel from USCG CYBERCOM and other relevant offices could establish and evaluate cybersecurity capabilities, exercise proposes and policies and procedures and train system and network administrators in the test environment. Ideally, this environment could extend to address not only IT networks, but also critical OT systems on cutters, boats, and aircraft.

Strategic priority 3 could be supported by a cyber range through simulation of common systems and networks among regulated vessels, facilities, and platforms. In this test environments, government, commercial, and academic researchers could test various configurations to determine critical vulnerabilities to support policy and regulatory recommendations.

Cyber Ranges

There are numerous government, academic, and commercial cyber ranges and cyber range solutions that are already in operation. The team identified several and performed an in-depth review of those most relevant to potential USCG application. They are introduced and described below based on available literature and discussion with representatives, and visits by ABS personnel.

U.S. Marine Corps (USMC) Cyber Security Range (CSR)

The USMC CSR, located in Stafford, Virginia, was chartered and funded by the Comprehensive National Cybersecurity Initiative (CNCI) to develop and host a realistic simulation of the DoD Information Network (DoDIN). The CSR is a fully accredited environment for conduct of cyber training, testing and exercises to reduce risk to DoD networks and systems.   The CSR is capable of emulating complex DoD environments and can be accessed onsite or remotely via a secure VPN tunnel.

The CSR can be used at **no cost** to the DoD customer, which includes the USCG. CSR staff do not conduct actual testing, evaluations or develop and deliver customer training.

Rather, these functions are performed by customers while CSR personnel operate and maintain the environments required to execute effective cyber tests and training.

The CSR provides a robust simulation capability with a wide array of capabilities, including modular architecture constructs that offer customer-configurable Security Technical Implementation Guides (STIG) and non-STIG enclave machines running multiple operating systems/patch levels. Tier 1 DoDIN replication with multi-protocol support, Tier 2 boundary suites with industry leading connection appliances, and Tier 3 interactive bases using industry standard models (Core, Distribution, Access) are offered.

Other capabilities include:

- Enterprise Information Assurance and Computer Network Defense tools
- Network services
- Traceable and relevant traffic generation and threat injection enabling cyber forensics
- Virtual interactive Internet with 5000+ malicious and benign sites
- Accessible on-site in Stafford, VA and remotely
- Interoperable with other lab environments (National Cyber Range)

The DoD Cyber Security Range has supported missions for the USMC, Army, Navy, Air Force, Defense Intelligence Agency, Defense Information Systems Agency, and the National Security Agency. The research team visited the CSR and documented detailed questions and answers in Appendix C-2.

Air Force Multi-Application Practical Learning Environment (MAPLE)

The Air Force's MAPLE range is a realistic network training range. Comprised of virtual machines simulating a network enclave complete with a firewall, intrusion detection software, and typical network web and email traffic. Malicious and unauthorized traffic also transits the simulated network. Teams of operators can utilize monitoring tools to detect, identify and mitigate the malicious and/or unauthorized traffic on the friendly network while maintaining the legitimate web and email traffic.

MAPLE's white force controllers monitor the range and provide support to the participants throughout test and exercise activities. They will provide debrief of the team's performance detailing traffic that traversed the network and actions taken by the team. This is done to highlight best practices and lessons learned that the team members can then apply to real world operations.

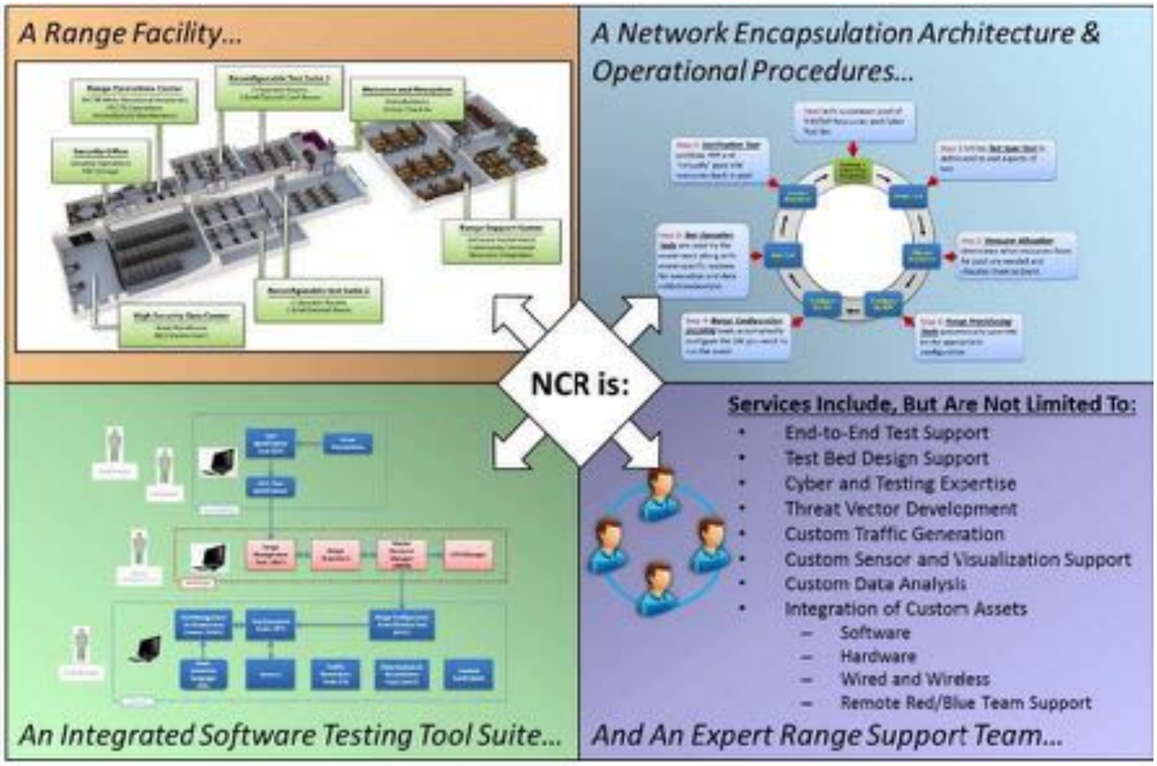
The MAPLE range is a training environment designed to emulate a realistic network where teams can safely exercise the following:

- Detect malicious/unauthorized network traffic
- Identify the source of the 'red' traffic, and act to
- Mitigate the threat traffic while maintaining essential 'blue' web and email services.

The range is tool agnostic and encourages team members to rely on DCO techniques as opposed to tool capabilities. Teams are not allowed to import their own tools onto the range. They are given an IDS, a software firewall, and a network monitoring tool to meet their assigned objectives.

National Cyber Range (NCR)

The NCR provides the ability to conduct realistic cybersecurity testing, evaluation, and training. The four key components of the NCR are: a secure facility, a unique security architecture, integrated tools for cyber testing, and a multi-disciplinary staff. The NCR, which is accredited by the Defense Intelligence Agency (DIA), provides an efficient and affordable cybersecurity test infrastructure. Figure 18 provides a high-level overview of the NCR.



A Range Facility...
A Network Encapsulation Architecture & Operational Procedures...
NCR is:
An Integrated Software Testing Tool Suite...
And An Expert Range Support Team...

Services Include, But Are Not Limited To:

- End-to-End Test Support
- Test Bed Design Support
- Cyber and Testing Expertise
- Threat Vector Development
- Custom Traffic Generation
- Custom Sensor and Visualization Support
- Custom Data Analysis
- Integration of Custom Assets
  - Software
  - Hardware
  - Wired and Wireless
  - Remote Red/Blue Team Support

Figure 18. NCR Overview

The NCR can represent complex network topologies with sufficient realism to portray a variety of current and anticipated attack strategies. The NCR can rapidly configure a variety of complex network topologies and scale up to 40,000 nodes. These nodes can include high-fidelity realistic representations of the public internet infrastructure including highly detailed supporting web and email servers and clients.

Academic Cyber Ranges

Louisiana State University (LSU) Joint Cyber Training Lab (JCTL)

The JCTL is focused on enhancing security IT and OT networks to minimize risks to critical infrastructure. The JCTL provides tier III cyber range comprised of actual and virtual hardware, software, and network devices that can simulate large-scale networks. It was designed to incorporate State and Federal cyber response frameworks and programs with a focus on critical infrastructure industries and private sector training. The JCTL was designed to achieve the following objectives:

- Establish a Cyber Lab that replicates specific Industrial Control Systems, DoD and Non-DoD Networks.
- Conduct Cyber Attack and Incident Response Exercises
- Offer Industry Specific Cybersecurity and Standards and Certification Coursework

University of Michigan Cyber Range (MCR)

MCR is an unclassified private cloud operated by Merit. The MCR delivers cybersecurity classes and exercises and enables product development and testing to clients. The MCR leverages Merit's network to conduct cybersecurity certification courses, hold training exercises, and operate its Secure Sandbox service. Some of the training and workshops offered by the MCR, include:

- Ethical Computer Hacking
- Digital and Network Forensics
- Network Penetration Testing
- Intro to Applied Cyber Security

Carnegie Mellon SEI Cyber Kinetic Effects Integration (CKEI)

The CKEI system combines a mature cyber simulator and a mature kinetic simulator in a way that allows effects in one environment to propagate to the other. This integration enables "whole-force training" in which cyber operators can learn to support live missions, while dealing with the realities of operating in contested networks and environments.

Within CKEI, systems can be attacked in cyberspace to produce a physical effect that provides a tactical advantage to the kinetic operators. Conversely, kinetic operators can damage or destroy systems within the kinetic simulator to deny cyber operators use of those systems in cyberspace.

Commercial Cyber Ranges

Mile2

Mile2 cyber range allows students to access the range online from anywhere and experience a live simulated environment. This commercial application supports cybersecurity exercises that simulate real world cyber security events. This capability can train personnel on a wide variety of cybersecurity disciplines, including: penetration testing, ethical hacking, incident handling, forensics, web application, virtualization and cloud computing-lab exercises. The platform provides the ability to use a wide variety of commercial and open source tools.

IBM xForce

IBM xForce is a fully operational cyber range that simulates real-world attacks to train cybersecurity personnel on how properly prepare for, respond to, and manage a wide array of threats. The range uses live malware, ransomware and other real-world exploits culled deliver realistic cyber-attack experiences. The facility features an air-gapped network of a fictitious corporation, used for simulated attacks, consisting of one petabyte of information, more than 3,000 users and a simulated version of the internet.

Raytheon Cyber Operations, Development and Evaluation (CODE) Center

The CODE Center is a cyber range used to test existing and future mission- critical systems against cyber-attacks. It offers several relevant capabilities to improve cybersecurity by enabling:

- *Test and evaluate advanced technologies*
- *Conduct force-on-force cyber games/exercises*
- *Provide an engineering environment to integrate technologies*
- *Provide cyber professional training and exercises*

Mission Support Use Cases

Use Case #1: Protection of USCG Networks & Assets.

The need for non-invasive technologies to test, prove, and disprove protections of USCG networks and assets may be met with the utilization of a cyber range. Cyber ranges may be comprised of many different levels of fidelity, or depths of simulation. Cyber range fidelity can vary from a web presence, or a desktop apparatus to a fully functional data center environment. Choices the USCG must make in using a cyber range to test USCG networks and assets start with the "fidelity" question and are directly related to the amount of budget - including facility and personnel expertise requirements to host a cyber range.

Selection of an existing range is highly recommended as most existing cyber ranges have multi-year investments in people, infrastructure, and learning. Mature desktop ranges are offered by at least one university and the USMC high-fidelity cyber range demonstrated a high-level of process and setup/tear- down automation in operating a range. The USMC range could "spin-up" an entire range in a matter of minutes that had a high level of simulation including simulation of a military base including traffic streams.

For USCG networks and assets, such as IT networks and the operational technologies aboard ships, cutters, boats, and aircraft, a cyber range could provide out-of-band or offline cybersecurity testing of critical systems. For example, a ship's bridge systems could be fixed in a cyber range and provide a non-consequential platform as a basis for red/blue team activities or host crew incident response training. A low-fidelity implementation could be entirely online. Or, a high-fidelity implementation could include an actual electronic chart display, ship steering stand, radar, Global Positioning System (GPS), voyage data recorder and other physical systems on a bridge.

Users: CYBERCOM, CG-6, CG-9

- Scope: Simulating to varying levels of fidelity (asset, network, full scale) the network, network traffic, and attacks/exploits, varying levels of fidelity (e.g., hardware vulnerabilities, commercial- off-the-shelf and specialized applications, network configurations, monitoring)
- Applications: Red team/blue teaming, vulnerability assessments, performance testing
- Covered assets:
    - USCG IT network
        - Application servers
        - Email servers
        - Web servers
        - Desktops
        - Database servers
        - Printers
    - Cutters: IT and OT systems
    - Boats: IT and OT systems
    - Aircraft: IT and OT systems

Recommendations:

- Document USCG usage requirements and leverage the infrastructure and learnings of the USMC cyber range
- Instantiate simple scenarios in the USCG cyber range that encompass widely-known threat vectors into USCG systems (e.g., phishing, USB, GPS spoofing) and train USCG personnel in these actions and defenses
- Use the USMC cyber range to perform after-the-fact analysis of breaches or exploits to gain new understanding of protections, controls, and defenses
- Use the USMC cyber range to train USCG cyber personnel (red/blue/white teams)
- Identify the inflection point where USCG should build their own cyber range

Use Case #2: MTSA-regulated assets

The value of a cyber range to MTSA regulated community assets may rely on how the community organizes and funds the development and ongoing costs associated with maintaining a cyber range. There may be value in developing a specific, low-fidelity and/or specific use case cyber range to understand vulnerabilities in the vessels, facilities, and platforms and possibly the interactions between these entities to drive understanding for eventual inclusion in policy or regulatory work. Effort would need to be applied to developing an "eco-system" for the use of a cyber range in this case.

One opportunity may be for the USCG to fund the development of a cyber range for use by Area Maritime Security Committees to demonstrate vulnerabilities that could affect the members. For example, a table-top range could simulate basic ship tracking utilizing Automated Information Services, GPS, and ECDIS. Vulnerabilities in these systems could be exploited and demonstrate the effects of the failures raising awareness. Any cyber range utilized in this manner would need to be generic in nature as the specifications of most ship-board systems are highly engineered.

- Users: CYBERCOM, CG-FAC, CG-RDC, port tenants
- Scope: Simulating to low levels of fidelity (functional systems of an asset) for a commercial asset: the network, network traffic, and attacks/exploits, low levels of fidelity (network configurations, monitoring)
- Applications: Vulnerability assessments or demonstrations w/ results to inform awareness and policy/regulatory development
- Covered assets:
  - Vessels: IT & OT
  - Facilities: IT & OT
  - Platforms: IT & OT

Conclusion

With so much variation asset to asset, company to company, and the availability of many DoD and commercial ranges, there is not much value in the USCG pursuing building their own cyber range. The availability of the USMC CSR at no cost and the high correlation between the USMC CSR capabilities and perceived USCG requirements substantially reduces cyber range risk.

The USCG should encourage industry to develop their own cyber ranges and test environments, particularly for operational technology to test and demonstrate cyber vulnerabilities.

2.2.4. Maritime Deterrent Strategy Effectiveness

This section introduces a methodology and model to conduct a quantitative risk analysis of a wide portfolio of assets spanning multiple asset classes, including vessels and facilities of different types. The methodology was primarily designed for use by the USCG in their regulatory role but could be useful for owners/operators of large and diverse fleet of assets to help understand this risk exposure and evaluate different courses of action to manage the risk.

USCG Risk Assessment Models

The foundation of the methodology in this section is risk analysis; so, the team researched other risk models the USCG has previously developed. The USCG has been steadily building, over the course of many years, its risk analysis and risk management capabilities – beginning with the roll-out of the USCG *Risk-based Decision-making (RBDM) Guidelines*. RBDM is a process that organizes information about the possibility for one or more unwanted outcomes into an orderly structure that helps decision makers make more informed choices.

The *RBDM Guidelines* were foundational research that provides a comprehensive set of methods, tools, training, and supporting materials designed to support a variety of decision making activities, including developing regulations and conducting compliance inspections. The wide array of risk methods and tools covered in the *RBDM Guidelines* provides USCG personnel with a variety of risk methods and tools designed for specific decisions that need to be made.

The USCG continued to evolve its risk management capability and has been consistently recognized as a leader in DHS and the federal government in the area. The following sections will highlight several risk management studies/programs, many of which are related to physical security (e.g., maritime terrorism issues). Collectively, they represent an evolutionary cycle that can be emulated to understand and manage cybersecurity risk. Figure 19 illustrates the agency's evolution through 6 of its select risk models. These models fall into three categories: (1) asset-specific physical security risk models, (2) strategic physical security risk models, and (3) strategic all-hazard risk models. The following sections will describe each model in more detail.

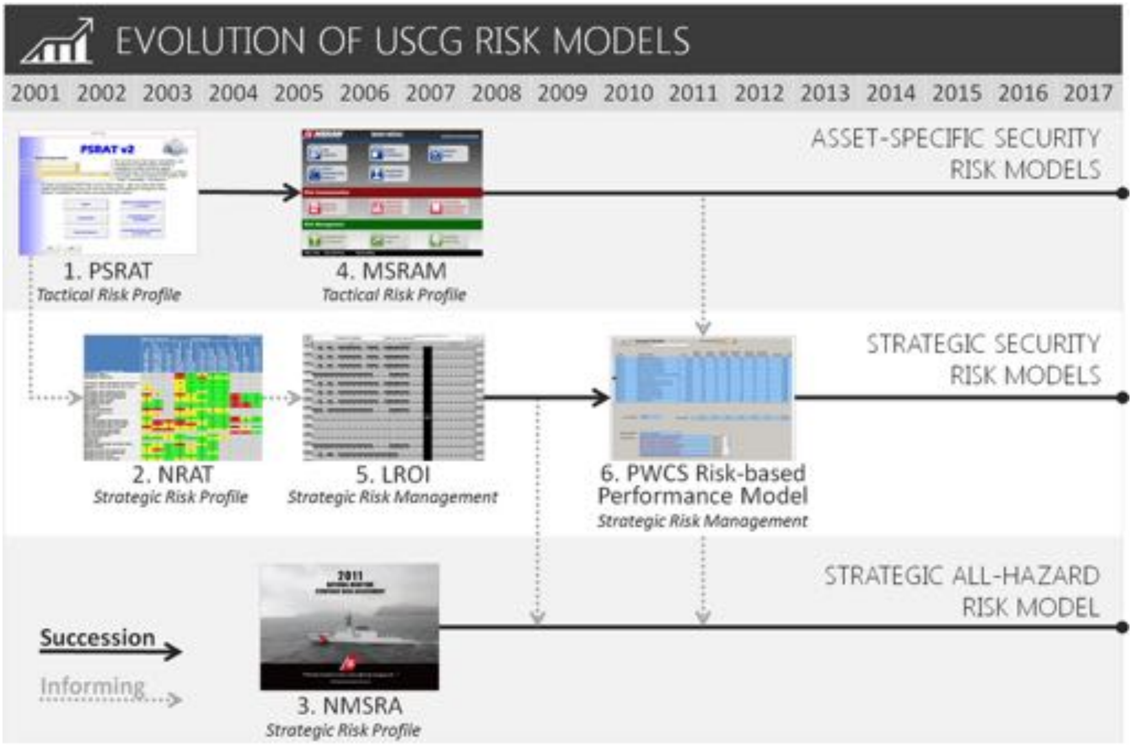

EVOLUTION OF USCG RISK MODELS
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
ASSET-SPECIFIC SECURITY RISK MODELS
1. PSRAT
Tactical Risk Profile
4. MSRAM
Tactical Risk Profile
STRATEGIC SECURITY RISK MODELS
2. NRAT
Strategic Risk Profile
5. LROI
Strategic Risk Management
6. PWCS Risk-based Performance Model
Strategic Risk Management
STRATEGIC ALL-HAZARD RISK MODEL
3. NMSRA
Strategic Risk Profile
Succession
Informing

Figure 19. Evaluation of USCG Risk Models

Port Security Risk Assessment Tool (PSRAT)
Date: November 2001

Sponsors: USCG Research & Development Center and LANTAREA

Purpose: PSRAT was developed shortly after the attacks of September 11th, 2001 to inform decisions in the execution of the Ports, Waterways, and Coastal Security (PWCS) mission. PSRAT was deployed to USCG field units across the country to evaluate the assets operating within the AORs against an array of potential terrorist attacks. The results of the initial PSRAT analysis were used to identify maritime critical infrastructure to focus USCG activities. While the PSRAT methodology included the ability to evaluate risk across multiple missions, the analysis was focused almost solely on the PWCS Mission by evaluating the risk of a variety of potential terrorist attack scenarios. A scenario in PSRAT was defined as an attack against a specific asset operating in the U.S. maritime domain.

National Risk Assessment Tool
Date: March 2002

Sponsor: USCG Commandant Planning & Policy (Resource Director) (G-CPP)

Purpose: NRAT was developed to support the USCG budget build process. Specifically, NRAT was a strategic maritime terrorism risk profile. This risk profile was used to screen PWCS-related resource proposals as part of the budget build process. This process mapped the relationships between resource proposals and maritime terrorism risk and identified resource proposals with strong risk reduction potential.

The analysis was focused almost entirely on physical security by evaluating the risk of a variety of potential terrorist attack scenarios. A scenario in NRAT was defined as an attack against representative assets operating (e.g., Commercial Passenger Vessels: Ferry boats) in the U.S. maritime domain.

National Maritime Strategic Risk Assessment (NMSRA)
Date: 2004, 2006, 2009, 2012, 2014, 2015, 2016, & 2017

Sponsor: Office of Performance Management and Assessment (CG-DCO-81)

Purpose: The NMSRA is a broad horizontal risk assessment across the USCG's enduring roles of Safety, Security and Stewardship and inclusive of all missions that analyzes:

- **USCG Risk Reduction**: the risk that is avoided due to USCG activities
- **Residual Risk:** the risk (expected societal loss) that remains after the USCG has performed all of its activities.

The NMSRA process has evolved with each cycle by: (1) increasing the scope of the assessment, (2) improving the quality of the risk information, and (3) reducing the amount of analysis effort required to perform the assessment.

Objectives

The NMSRA meets the following high-level objectives:

- Develop comprehensive risk profile that can be used to inform a wide variety of resource allocation decisions within and across missions.
- Provide an alternatives evaluation capability which enables analysts to assess risk management strategy options
- Identify data sources used to inform risk assessment that are not stored in authoritative USCG databases

Scope

The analytical boundaries of the NMSRA are:

- **All Hazards.** The NMSRA evaluates a broad set of undesirable incidents and scenarios spanning the entire USCG mission set. The analytical scope addresses all hazards that the USCG has a role in mitigating considering governing statutes, mandates, roles and missions.
- **National Level.** Risk profiles are developed at the national level, and for most missions, profiles are not broken down geographically (e.g., Districts).
- **Strategic Timeline.** Since the results are primarily intended to inform mid/long-term resource allocation decisions, the NMSRA analyzes risk 5 years into the future to inform the 5-year Future Years Homeland Security Program (FYHSP) budgetary cycle.
- **Low Fidelity.** The NMSRA process generates coarse estimates of risk. The risk profiles are accurate but are not generated with high precision. Therefore, NMSRA data is often unsuitable for performing incremental analysis for small scale resource allocation options. For instance, since reprogramming individual assets rarely affects any national risk profile; NMSRA does not have the fidelity to measure the impact.

MSRAM

Date: 2005 – Current: conducted through annual cycles

Sponsor: Domestic Port Security Division (CG-PSA-2)

Purpose: MSRAM is a terrorism risk management tool and process deployed to USCG analysts across the country enabling them to perform a detailed risk analysis for their area of responsibility. The results of this process are used to support a variety of risk management decisions at the strategic, operational, and tactical levels.

The execution of the MSRAM process across the country yields an extensive national dataset containing risk evaluations of a wide array of scenarios for all of the significant assets operating in the U.S. maritime domain. MSRAM offers a dynamic analysis interface capable of generating tailored results to support a variety of decisions. Results include:

- Risk-ranked lists of targets and scenarios
- Counts of targets and scenarios at similar risk levels
- Comparisons of scenario risk with and without government contributions
- Risk reduction value of maritime security stakeholders, including owners/operators, local law enforcement, first responders, and the USCG\
- Geographic Information System (GIS) layers displaying maritime terrorism risk

Layered Return-on-Investment (L-ROI) Model
Date: 2005 – 2009: conducted through annual cycles

Sponsor: Office of Performance Management & Assessment (DCO-81)

Purpose: Based on strategic guidance to use risk analysis and risk management, DCO-81 developed a proxy measure of USCG performance using scientifically valid probabilistic risk assessment techniques. Beginning in 2005, the USCG developed the approach and supporting L-ROI model to estimate USCG risk reduction performance in the PWCS mission. LROI is a simplified, scenario-based, event tree model used to:

- Illustrate the layered security strategy that the USCG provides against each meta-scenario to prevent, protect, respond, and recover
- Define the roles of USCG activities and how they relate to one another (e.g., detection, intervention)
- Calculate the magnitude of risk that is being reduced by the layered security strategy (outcome measure for the PWCS Mission)
- Provide a mechanism for estimating the risk reduction importance of individual activities within the layered security strategy for a scenario

From 2005-2009, the outputs of the L-ROI model were promulgated as the official measure for USCG performance in the PWCS mission. Specifically, the outcome measure reported (1) percent of USCG risk reduction of USCG-owned risk, as well as USCG risk reduction with respect to (2) threat, (3) vulnerability, and (4) consequence.

PWCS Risk-Based Performance Model
Date: 2010 – Current: conducted through annual cycles

Sponsor: Office of Performance Management & Assessment (DCO-81)

Purpose: Beginning in April 2010, DCO-81 initiated an effort to make improvements to the L-ROI model and processes the USCG has developed to (1) assess risk in the PWCS mission, (2) evaluate USCG performance within the mission, and (3) evaluate the effectiveness of USCG planning, programming and budgeting recommendations in terms of risk reduction.

Specifically, the effort involved improving the L-ROI model and process to make them more:

- Institutionalized by being integrated within the USCG's enterprise PWCS risk management system
- of record, the MSRAM
- Transparent to data analysts and decision makers
- Repeatable to generate consistent year-to-year results
- Auditable by third parties
- Sensitive to smaller changes in USCG performance
- Usable by a wider array of USCG analysts

Cyber Decision Support Requirements

Congress passed the MTSA giving the USCG the authority to regulate security for vessels, facilities, and OCS facilities operating on or adjacent to the U.S. MTS. The USCG later promulgated MTSA's implementing regulations (33 CFR Parts 101-106). The key requirements for the different types of assets are addressed in the following parts:

- U.S. flagged vessels (33 CFR Part 104)
- Facilities (33 CFR Part 105)
- Offshore platforms (33 CFR Part 106)

There are numerous requirements described in these parts covering a wide array of security program facets (e.g., training, recordkeeping, incident reporting). Of particular interest to this research are the requirements mandating that a MTSA-regulated vessel/facility complete a VSA or FSA. The assessment must identify and evaluate critical assets, potential threats, and general security vulnerabilities. The vessel/facility must then develop and submit a VSP or FSP to the USCG that addresses the vulnerabilities identified in the VSA/FSA.

The MTSA regulations do not explicitly address cyber; so, to clarify, in July 2017, the USCG issued draft policy in Navigation and Vessel Inspection Circular (NVIC) 05-17, titled: *Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities.* The NVIC clarifies existing regulatory requirements in 33 CFR parts 105 and 106 to explicitly address cybersecurity measures in the facility security assessment and facility security plan.

In accordance with 33 CFR parts 105 and 106, MTSA-regulated facilities are instructed to analyze vulnerabilities with computer systems and networks in their FSA. This NVIC will assist FSOs in completing this requirement. Additionally, this NVIC provides guidance and recommended practices for MTSA regulated facilities to address cyber related vulnerabilities. Until specific cyber risk management regulations are promulgated, facility operators may use this document as guidance to develop and implement measures and activities for effective self-governance of cyber vulnerabilities.

The NVIC assists the owner/operator in identifying cyber systems that are related to MTSA regulatory functions, or whose failure or exploitation could cause or contribute to a Transportation Security Incident (TSI). A TSI is defined as: a security incident resulting in a significant loss of life, environmental damage, transportation system or economic disruption. The traditional emphasis of cybersecurity is the prevention of information theft and ensuring the integrity of business systems (e.g., corporate Websites, accounting systems) where TSIs are focused on scenarios that could result in or contribute to physical consequences or port disruptions.

While the NVIC is focused on shore side and OCS facilities, the USCG is working in coordination with the IMO to address cybersecurity for vessels as well. IMO has given vessel owners/operators until January 1, 2021 to incorporate cyber risk management into their safety management systems.

So, the NVIC cements the USCG's role in cybersecurity is one of regulatory oversight for assets that operate in the U.S. MTS to ensure that owner/operator of these assets have identified and addressed vulnerabilities that could cause or contribute to a TSI.

The question going forward is how can USCG offices responsible for development of cybersecurity policies (and potentially regulations) develop strategies that best reduce maritime cybersecurity risk while balancing cost of implementation.

These offices need the ability to (1) understand the relative risk priorities of potential cybersecurity scenarios, (2) contextualize and prioritize the risk of cybersecurity within the USCG's PWCS mission and ultimately within the enterprise risk portfolio which spans the 11 statutory missions, and (3) assess the impact of potential deterrent strategies on the cybersecurity risk profile.

While qualitative information can help guide policy and regulatory decisions, quantitative results are preferable, and ultimately required, if the USCG wishes to promulgate new cybersecurity regulations. To date, there has not been a cyber-initiated TSI in the U.S.; so, the USCG lacks sufficient data on which to make these decisions. So, a strategic model is needed. One that rises above the assessment of risk for individual assets or even fleets to considering cybersecurity risk in the entire U.S. maritime domain.

Needed Information

Decision makers need a cyber risk model that generates results with the following attributes:

- **Quantified.** Cyber risk must be quantified to enable comparison with other security and non- security incidents in the USCG (and DHS) mission space. Risk expressed as an absolute expected annual loss is an ideal metric to enable comparison with other security and non-security missions. Relative risk metrics can also be useful for establishing policy that targets certain asset types.
- **Consequence-informed.** The relative risks generated by the model described earlier in this document are useful for prioritization of similar assets for inspection and/or mitigation, but a quantification of consequence potential is needed to prioritize across asset types. For example, failure of a cargo management system can result in very different consequences for a chemical tanker vs. an oil tanker.

- **Security and Safety.** The model must consider both intentional (e.g., cybersecurity) and accidental (e.g., cyber safety) events
- **Residual Risk and Risk Reduction.** The model must characterize owner/operator risk reduction as well as residual risk.
- **Asset Classes and Functions.** The risk profiles must be able to be viewed by asset and function to develop and prioritize strategy alternatives.
- **Impact of alternative strategies.** Methodology must support characterizing the impact (in terms of risk reduction) of alternative strategies to help decision makers choose those with the best return-on-investment potential
    - Ideally, show **X** amount of residual risk in the mission set.
    - Option 1: risk is reduced by **Y** amount
    - Option 2: risk is reduced by **Z** amount

Application

The development and steady evolution of the risk models described in Section 2.2.4, under USCG Risk Assessment Models provides a blueprint that could be employed to establish and steadily improve the USCG's understanding of cybersecurity risk as well. The model presented in the following sections build off of the functions-connections- identities (FCI) concepts presented in the Framework for Point of Failure Detection Methodology, discussed in the Center's Year 3 report, and in the Critical Points of Failure section (Section 2.2.2) of this report to a higher level of abstraction.

The relative risk index presented in Section 2.2.2 is analogous to PSRAT and its successor MSRAM which focus on individual assets. The model presented in this section is a method for a national, strategic assessment analogous to the L-ROI and PWCS Risk-Based Performance Model and ultimately, the NMSRA.

Model

The strategic model described in this section follow the approach and evolution of the physical security models by estimating risk for asset classes vs. individual assets. The model employs a stochastic approach to account for the wide variability in expected outcomes. By representing different potential random outcomes using probability distributions, model results better account for the fact that various real-world situations are rarely the same. By running a model over a large number of iterations with each iteration drawing different results from defined probability distributions allows a user to better understand trends and expected outcomes over time.

Stochastic modeling is particularly relevant when multiple factors exhibit variability and there is a desire to understand how these fluctuations interact to produce results. As an example, in the instance of cyber modeling, probability distributions may represent observed differences in connectedness within an asset class as well as the distribution of different consequences should a cyber incident occur. Repeatedly running the model, taking into account the "dice roll" results for each probability distribution, and then consolidating the final results provides the analyst with a sense of “spread” for those results and allows use of statistical techniques (e.g. mean, median, standard deviation) to interpret the modeling outputs.

The model includes threat, vulnerability, and consequence (TVC) risk factors aligned to the FCI elements. The various nuances of maritime cyber risk require the designation of several sub-factors for threat, vulnerability, and consequence. Each sub-factor has a distribution of values associated with it. In early iterations, the distributions should be representative of experts understanding of the current state of maritime industry based on experience reviewing and assessing maritime assets. Over time, these distributions could be developed based on data collected from assessment of individual assets using the model from the Critical Points of Failure section mentioned earlier.

Scenarios

In the model, scenarios should be defined as exploitation of safety-critical functions that could credibly lead to a TSI. Table 2 lists the scenario set based on the team’s identification of the common functions of various vessel and facility asset classes. Scenarios are defined as combinations of the first two columns, for example:

- Exploitation of Propulsion System/Freight Ship
- Exploitation of Cargo Management System/Tank Ship
- Exploitation of ICS/Waterfront Facility

Table 2. Cyber Scenario Framework

Asset Classes	Incidents: Safety-critical Function Exploitation	Event	Potential Consequences
Commercial Vessel Communities: *Systems found on most commercial vessels* • Freight Ship • Industrial Vessel • Mobile Offshore Drilling Unit • Offshore Supply Vessel • Passenger (More Than 6) • Public Tankship/Barge • Public Vessel, Unclassified • Research Vessel • School Ship • Tank Ship • Towing Vessel	**Propulsion System:** Increase or decrease speed at critical moments during port transit or extreme weather at sea **Steering/Maneuvering Control System:** Take vessel off course at critical moments during port transit or extreme weather at sea **Navigation Systems:** Take vessel off course at critical moments during port transit **Power Management System:** Lose power or overpower vessel at critical moments during port transit or extreme weather at sea **Ballast Control System:** Facilitate improper loading, causing listing or potentially exceeding hull loading limits	• Grounding • Collision/Allision • Flooding/Sinking	• Loss of life/injuries to crew and passengers • Vessel damage • Spill of fuel oil • Channel blockage
Tank Ship	**Cargo Management System:** Open valves to release of oil, refined product, or certain dangerous cargo (CDC) during port transit	• Oil, refined product, or CDC spill	• Spill of oil, refined product, or CDC • Navigation restriction • Loss of life to crew and

Mobile Offshore Drilling Unit	**Dynamic Positioning System**: Take MODU off station at critical moments during drilling operations **Drilling Control System:** Affect drilling system performance at critical moments during drilling operations **Vessel Management System:** Effect MODU ballast, causing vessel to go off station at critical moments during drilling operations	• Emergency disconnects • Loss of well control	• Spill of oil and drilling mud in the riser • Navigation restriction • Loss of life/injuries to crew
Waterfront Facility (Bulk Liquid)	**ICS:** Open valves to release oil, refined product, or CDC from facility's processing or storage equipment	• Oil, refined product, or CDC spill	• Spill of oil, refined product, or CDC • Navigation re-
Waterfront Facility (Container Terminal)	Crane Control System: Affect crane system performance at critical moments during container loading/unloading operations	• Container drop • Crane damage	• Loss of life/injuries to workers • Crane damage, resulting in re-
	Terminal Operating System: Unavailability of terminal operating system or corruption of data. Improper loading of container, affecting ship stability	• Inability to load or unload cargo	• Port disruption

Threat

To model and quantify threat, the research team chose four sub-factors shown in Figure 20 and described below.

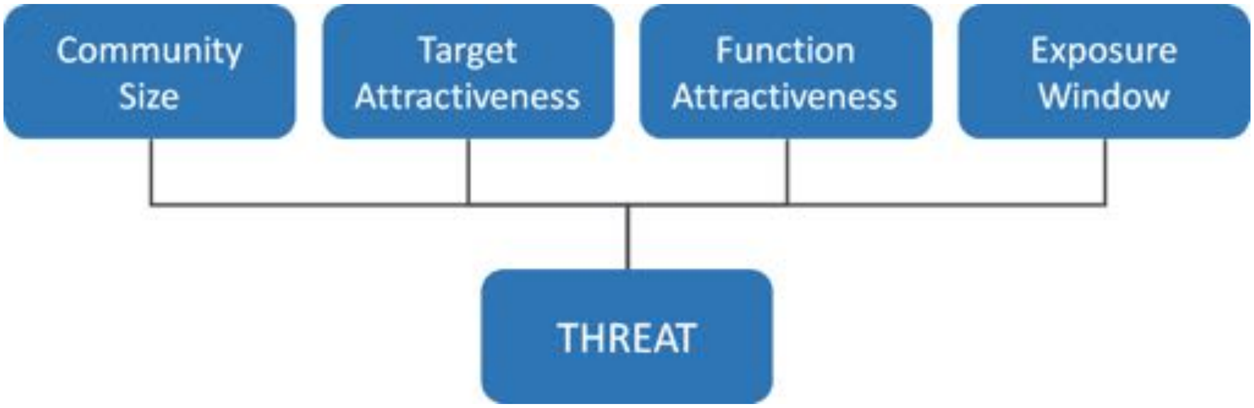


Figure 20. Threat Sub-factors

Asset Class Size

Asset Class size is a scaling sub-factor designed to account for the estimated number of assets in a given class. This represents the number of opportunities for system exploitation, commensurate with a class's size. For example, with all factors being equal, if there are many more tank ships than MODUs, then a safety-critical functional failure is more likely to occur on a tank ship as opposed to a MODU because there are more opportunities. This value is the count of assets in a class divided by the total number of assets across all asset classes. Class data can be derived from a number of authoritative government data sources:

- USCG MISLE vessel registries for domestic vessels
- USCG Ship Arrival Notification System for foreign vessels
- MSRAM for waterfront facilities
- BSEE platform structures for platforms and mobile offshore drilling units

Target Attractiveness

The target attractiveness sub-factor is designed to capture attacker preference's for attacking certain asset classes. This sub-factor applies values ranging from zero to one providing relative measure for how likely an adversary is to target an asset class. This can be assigned based on specific threat data, if available.

Function Attractiveness

Function attractiveness is designed to quantify and capture the adversarial capability to exploit a given safety-critical function; that is, the capability required to successfully cause a functional failure for a given class via digital attack vectors. This value is function-specific and uses a zero to one scale to account for the relative attractiveness of each function to an adversarial.

For example, if a terminal operating system requires less technical expertise to exploit than a drilling control system, attackers may be more likely to attempt an attack on a terminal operating system. It is important to note that the research team has not yet found a reliable data source for this value; it may be an area for future data exploration in future iterations of the model.

Exposure Window

To achieve a TSI-level of consequences for a particular scenario, most attacks must occur within a time- sensitive window. For example, if a navigation function is compromised, an incident such as a grounding or collision will be more likely to occur, and with greater consequences, in restricted waters as opposed to open ocean.[2]

[2] The exposure window conceptual framework was developed through interviews with industry and input from ABS SMEs who have performed many cyber assessments on a wide range of maritime assets.

The model should assign an exposure window category or distribution to each asset class/safety-critical function pair. Consider the simple example below, where exposure windows are defined in three categories:

High (90%): attack does not require precise attack timing or systems are susceptible to TSI consequences with passive corruption
Medium (50%): attack requires specific attack timing
Low (10%): attack requires precise attack timing or requires persistent remote connection

Table 3 provides example exposure window assignments for several asset class/safety-critical function pairs:

Table 3. Example Exposure Window Assignments

Function	Asset Class	Exposure Window
Propulsion	Freight Ship	Low
Steering	Freight Ship	Low
Navigation	Freight Ship	Low
Propulsion	Passenger (more than 6)	Medium
Steering	Passenger (more than 6)	Medium
Navigation	Passenger (more than 6)	Medium
Terminal Operating	Waterfront Facility	High
ICS	Waterfront Facility	Medium
Drilling	MODU	Medium

Threat Results

The model selects a value for target attractiveness and function attractiveness, each of which are fixed between zero and one, and then multiplies the selected values by the asset class size and exposure window values, which are scenario-specific, in order to arrive at the threat value. This random-value selection and calculation process is repeated a number of times to arrive at a predicted threat value for the final risk calculation.

Vulnerability

Vulnerability assessment accounts for two primary sub-factors: system connectedness and non-cyber mitigating factors, as shown in Figure 21.

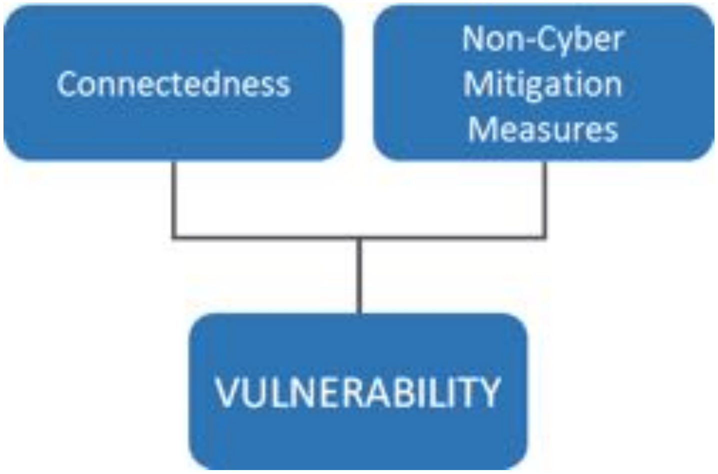


Figure 21. Vulnerability Components

Connectedness

Connectedness captures the risk posed by the degree to which digital systems – especially those that govern safety-critical functions – are linked. Each safety-critical function is enabled by a system or set of systems. These systems exhibit varying degrees of connectedness. Generally, the more connected a system is, the higher the vulnerability. The model uses four connectedness categories:

1. **Discrete** – A single (1:1) digital connection only between a single equipment controller and a single piece of controlled equipment
2. **Simple** – More than one connection between a single equipment controller and more than one other equipment controllers, but not through a network
3. **Complex** – More than one digital connection to a network linking only equipment controllers and associated interfaces
4. **VLN** – Any of the above type connections that are also connected to the Internet or any potentially accessible proprietary wireless connection

Table 4 provides several examples of connectedness assignments for asset class/ function pairs based on input from ABS maritime cybersecurity assessors:

Table 4. ***Connectedness Assignments by Asset Class and Function***

Asset Class	Function	Simple	Discrete	Complex	VLN
Freight Ship	Propulsion	80%	19%	1%	0%
Mobile Offshore Drilling Unit	Propulsion	5%	70%	23%	2%
Offshore Supply Vessel	Propulsion	60%	35%	5%	0%
Passenger (More Than 6): Cruise	Propulsion	5%	20%	40%	35%
Tank Ship	Propulsion	80%	19%	1%	0%
Freight Ship	Steering/Maneuvering	5%	70%	25%	0%
Tank Ship	Steering/Maneuvering	15%	60%	25%	0%
Towing Vessel	Steering/Maneuvering	45%	50%	5%	0%
Freight Ship	Navigation	5%	60%	33%	2%
Passenger (More Than 6): Cruise	Navigation	0%	10%	70%	2%
Tank Ship	Navigation	5%	60%	33%	2%
Freight Ship	Power Management	60%	30%	5%	5%
Mobile Offshore Drilling Unit	Power Management	10%	30%	55%	5%
Passenger (More Than 6): Cruise	Power Management	0%	30%	65%	5%
Tank Ship	Power Management	60%	30%	5%	5%
Freight Ship	Ballast Control	5%	50%	45%	0%
Mobile Offshore Drilling Unit	Ballast Control	5%	40%	55%	0%
Passenger (More Than 6): Cruise	Ballast Control	0%	45%	45%	10%
Tank Ship	Ballast Control	5%	50%	45%	0%
Tank Ship	Cargo Management	5%	75%	20%	0%
Freight Ship	Cargo Management	5%	75%	20%	0%
Mobile Offshore Drilling Unit	Dynamic Positioning	0%	0%	95%	5%
Mobile Offshore Drilling Unit	Drilling Control	0%	10%	70%	20%
Waterfront Facility: Bulk Liquid	Industrial Control	20%	70%	10%	0%
Container Terminal	Terminal Operating	0%	0%	0%	100
Container Terminal	Crane control	90%	8%	2%	0%
Industrial Vessel	Dynamic Positioning	0%	40%	60%	0%
Offshore Supply Vessel	Dynamic Positioning	0%	60%	40%	0%

Passenger (More Than 6): Cruise	Dynamic Positioning	0%	0%	80%	20%
Research Vessel	Dynamic Positioning	0%	60%	40%	0%

Non-Cyber Mitigation Measures

If an asset’s vulnerabilities are exploited, there are often actions that personnel may take to compensate for the loss of automated functions to avoid an incident or mitigate consequences upon discovery of a problem. These capabilities are often highly effective at mitigating a successful system exploitation or functional compromise. Examples of these capabilities include:

- **Ship Handling Functions** involve humans-in-the-loop, and there are manual overrides for critical vessel functions on the bridge, in the engine room, or in the steering compartment. The crew can switch automated functions to manual mode to pilot the vessel to safety.
- **Local Pilots** are aboard foreign commercial vessels when navigating U.S. ports. These pilots are intimately familiar with their port environments making them far more likely to recognize anomalies in the vessel’s navigation system due to cyber exploitation.
- **Material Transfer Operations** to/from vessels are required by USCG regulations to involve persistent oversight by a facility and a vessel person-in-charge (PIC). The PICs each monitor their systems and coordinate actions throughout the transfer process via handheld radio. Often facilities will have another operator in the field monitoring tank level (e.g., local tank level indicators) and flow rates.

The model should assign a category or distribution to each asset class/safety-critical function pair. Consider the simple example below, where non-cyber mitigation capability is defined in three categories:

- **High (10%):** Ample time to recognize functional failures and capability to manually perform automated functions or place asset in a safe status
- **Medium (50%):** Limited capability to recognize functional failures with some capability to manually perform automated functions or place asset in a safe status
- **Low (90%):** Limited/no capability to manually perform automated functions or place asset in a safe status

Table 5 provides example assignments for several function/asset class pairs:

Table 5. Example Non-Cyber Mitigation Assignment

Function	Asset Class	Non-Cyber Mitigation
Propulsion	Freight Ship	High
Steering	Freight Ship	High
Navigation	Freight Ship	Medium
Terminal Operating	Waterfront Facility	Low
ICS	Waterfront Facility	High
Drilling	MODU	Medium

Consequences

Since few cyber-initiated events have significantly impacted U.S. maritime assets at the time of writing, the research team applied consequence assessments based on the results of historical non-cyber incidents relating to each asset class and function pairing.

The USCG's MISLE system documents incident data going back for decades which informs the frequency
and magnitude of consequences that could result from successful cyber attacks.

MISLE incident investigation data can be used to construct consequence distributions for the set of scenarios. This data is gathered after a marine incident and documented the amount of oil and/or chemicals spilled, the estimated property damaged resulting from the incident, and the number of people injured, missing, or dead.

To capture the effect of obstructed or closed waterways as the result of an incident, data can be applied from the USCG's Common Assessment and Reporting Tool (CART) system, which is used to manage incidents impacting the MTS. CART data provides a historical record allowing capture of the cause, severity, and duration of waterway closures.

Types of Consequences & Results

The model includes assessments for the following consequences caused by TSI:

- **Environmental consequences** – oil and/or chemicals spilled, in gallons
- **Economic consequences** – property damage, in dollars
- **Death and Injury consequences** – the number of people injured, missing, or dead
- **Mobility consequences** – disruption to waterway traffic

Each set of consequence evaluations is measured using consequence points based on the USCG Consequence Equivalency Matrix (CEM). The consequence scores are then summed across impact types to arrive at a total consequence vale for the risk calculation, as outlined in Figure 22.

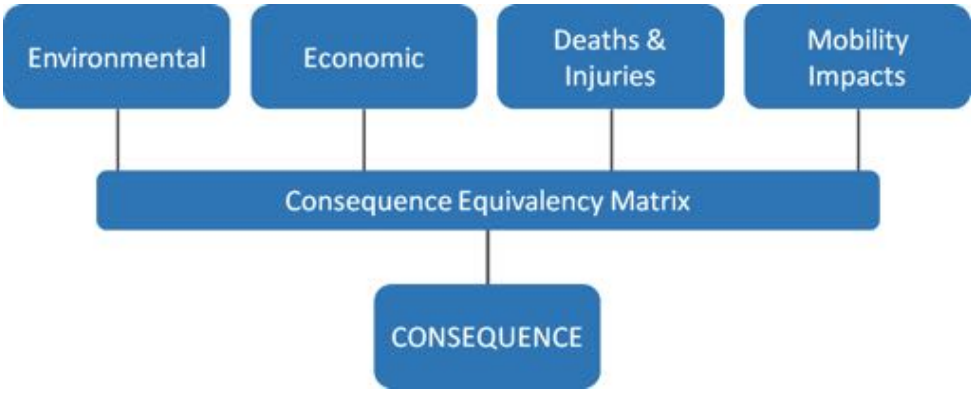


Figure 22. Consequence Components

The consequence values for the four consequence types are determined by randomly selecting a value from a Poisson (P(λ)) distribution, where the input λ is the mean value from the comparable scenario set of MISLE incident data. That is, the team calculated the λ-value for the Poisson distribution by taking the weighted average of the number of gallons of oil/chemicals spilled, the amount of property damage caused, the number of people killed or injured, and the level of waterway impacts resulting from a navigational failure aboard an OSV; each time the model runs, it randomly selects a value in the distribution determined by P(λ). The idea is that since the model runs and performs these selections many times (1000 times), the resulting modeled consequences will approach a “true” value.

Outputs and Results

The model output includes exceedance probability (EP) curves for each scenario. An EP curve describes the probability that various levels of loss will be exceeded. This is consistent with the USCG’s multi- mission risk analysis approach. Figure 23 provides an example exceedance probability curve result.

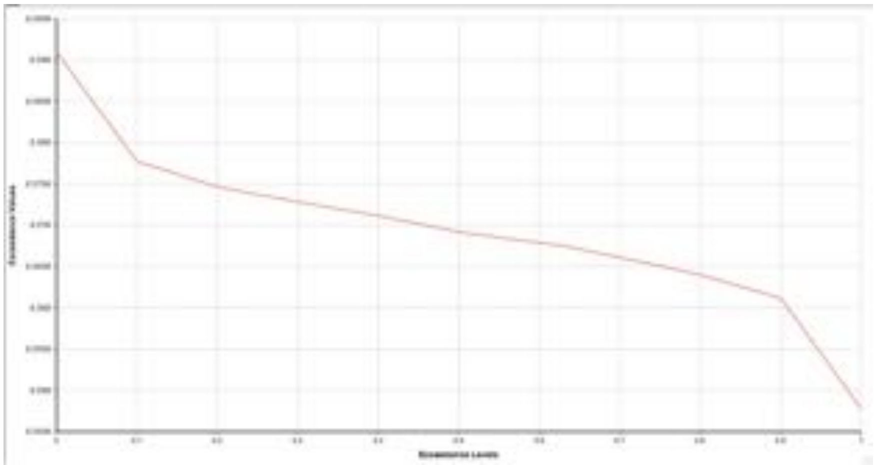


Figure 23. Exceedance Probability Curve Example

Average Annual Loss

Average Annual Loss (AAL) is the mean value of an EP curve, and represents the expected loss per year, as assessed over the outputs of many model iterations. This value gives an idea of the absolute “riskiness” of cyber given the modeled asset classes, functions, and related system factors. The set of EP curves aims to provide insight as to what is driving risk to the given asset class. Figure 24 provides an example AAL result.

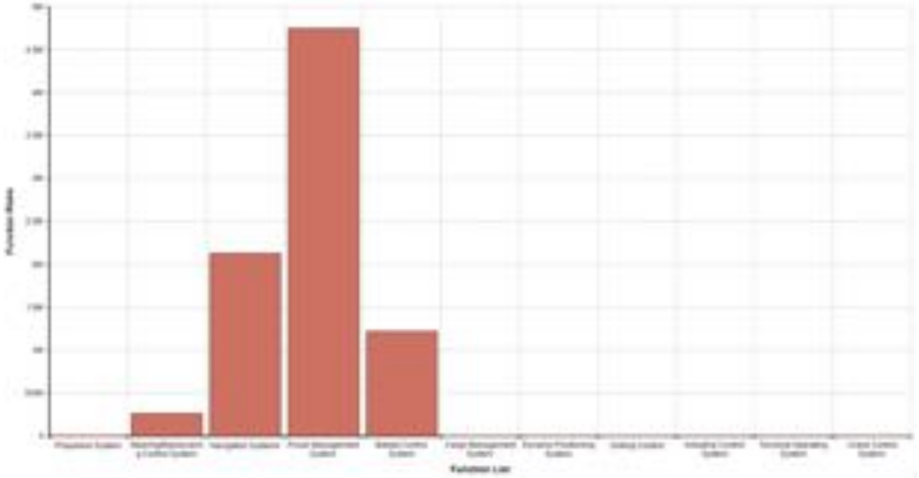


Figure 24. AAL Example

Cyber Deterrent Strategy Development

The baseline risk profile generated by the model provides USCG policy makers with a portfolio-level view of cybersecurity risk. By exploring this profile, analysts can identify high risk segments to develop cyber deterrent strategy options. The model sub-factors and distributions can be adjusted by analysts to reflect the impact of various policy options. This adjustment could be performed at any level of detail. For example, policies or regulations may focus primarily on select asset classes or specific safety-critical functions. So, analysts could make adjustments to the distributions and re-run the model to generate risk results for each option, which could be compared to the baseline profile to characterize the potential risk reduction.

Risk reduction estimates combined with implementation cost estimates are essential for the development and selection of new regulations and policies.

2.3. VTS Radar Project

2.3.1. Introduction

The U.S. Coast Guard uses a Vessel Traffic Service (VTS) system to collect, process, and disseminate information on the marine operating environment and maritime vessel traffic in major U.S. ports and waterways. The PAWSS (Ports And Waterways Safety System) VTS mission is to monitor and assess vessel movements within a VTS Area, exchange vessel movement data with vessel and shore-based personnel, and provide advisories to vessel masters.

The VTS system at each port has a Vessel Traffic Center that receives vessel movement data from the Automatic Identification System (AIS), surveillance sensors, other sources, or directly from vessels. AIS technology relies upon global navigational positioning systems (GPS), navigation sensors, and digital communication equipment operating according to standardized protocols (AIS transponders) that permit the exchange of navigation information between vessels and shore-side vessel traffic centers. AIS transponders can broadcast vessel information such as name or call sign, dimensions, type, GPS position, course, speed, and navigation status.

While AIS is helpful, not all vessels are required to use AIS (only certain vessels that fall under certain categories for gross tonnage, passenger capacity, length, and function are required to carry and use AIS). Also, the majority of currently installed radars detect vessels with a minimum size where smaller vessels and other objects that have too small of a Radar Cross Section are not seen in the background of clutter. Therefore, a means is needed to detect these small and large vessel targets that are either not required to carry AIS or not cooperative (i.e., they do not comply with AIS required use or spoof AIS information).

2.3.2. Research Objectives

The objective of this research is to enhance the operational capabilities and missions of DHS stakeholders (USCG, CBP, ICE, and others) to identify suspicious small vessels that may be present in a harbor or port. It addresses one of the Secure Borders Integrated Product Team (IPT) gaps as well as questions posed for the Maritime Security Center by DHS. Specifically, these questions are:

1. What new technologies can be developed and applied to effectively improve surveillance, detection, classification, and identification of vessels, suspicious materials, and persons in the maritime domain both on and below the water?

2. What new technologies, including technologies combined with new non-technological inspection methods and tools, can effectively improve a user’s ability to screen, detect, and mitigate threats?

2.3.3. Methodology

The deployment of new radar systems into an operational environment is a difficult process. In addition to the technical and training aspects, there are also space and structural limitation concerns. The USCG has invested in many VTS/PAWSS installations around the US ports. Although their objective is to detect large vessels using commercially available radars for such applications (e.g., the TERMA Scanter), the raw radar data could contain detections of small vessels as well. Therefore, to avoid deploying additional radars that are capable of detecting smaller targets, we proposed that the information already collected by VTS radars be exploited to identify the small targets. The radar raw data contains all the detected information, including small targets. However, the small targets may be masked by the presence of reflections caused by unwanted clutter. Through special signal processing of the raw data, small vessel data may be extracted. There are several issues associated with acquiring and processing this raw data, or “radar video.” Among them, the video data is wideband compared to processed data. Therefore, appropriate wideband protocols need to be defined. Another issue is that video data is often not provided by radar vendors, as the processing of the video data is kept proprietary. Furthermore, innovative signal processing techniques to extract small boat signals from clutter need to be developed. These are the subjects of the project Milestones as described next.

2.3.4. Milestones

This project started in Year 3, but the scope was modified after the start date due the USCG being concerned with the nature and sensitivity of data that needs to be collected and analyzed. Therefore, the project results with the following milestones are being reported in this annual report.

Milestone	Description	Status
1	Kick-off meeting with key stakeholders from DHS, CBP, and USCG.	Complete. Kick off meeting was held on March 20, 2017. Meeting notes prepared and shared with PM and stakeholders.
2	Survey of software standards, integration patterns, and security requirements.	Complete. A summary report of software standard, integration patterns and security requirements were prepared and can be found in the final project report.

3	Investigation of the application of NMEA OneNet, Asterix formats, and other National Marine Electronics Association (NMEA) communications protocols for organizing the radar network and for data fusion with information from other sensors (like AIS and Maritime CCTV surveillance).	Complete. An analysis and summary report were completed and can be found in the final project report.
4	Investigation of existing commercially viable systems for clutter suppression methods for improving radar performance through open source information.	Complete. An analysis of commercially available systems was conducted. The results were provided in the final report.
5	Investigation of new algorithms and known signal processing algorithms and sea clutter suppression methods that can provide longer range of small boat detection.	Complete. Signal processing algorithms were analyzed and were completed and provided in the final report.
6	Documentation of all findings.	Complete. Final Summary Report was provided at the end of the project.

The following milestones were the output of this project as follows:

Milestone 1: Project kick-off meeting to describe the project goals and output with DHS Stakeholders.

Milestone 2: A survey of software standards, integration patterns, and security requirements.

Milestone 3: An investigation of the application of National Marine Electronics Association (NMEA) OneNet, All-purpose Structured EUROCONTROL Surveillance Information EXchange (ASTERIX), and other NMEA communications protocols for organizing the radar network, and for data fusion with other sensors (such as AIS and Maritime CCTV surveillance).

These milestones surveyed software standards for rotating radars and investigated how these standards can be applied to the VTS radar network. A description of the NMEA, and the ASTERIX formats were described. Current NMEA standards do not support wideband communications, although a wideband version is underway (NMEA OneNet).

A version of ASTERIX that can also be used for radar video architecture was discussed. Most utilize proprietary signal processing techniques, although Kelvin Hughes and Cambridge Pixel systems utilize an open architecture.

Milestone 4: An investigation of existing commercially viable systems for clutter suppression methods for improving radar performance through open source information.

The specifications for several important radar systems were given, including TERMA and Gem systems. In terms of quantitative information, what is available is basically specifications, such as bandwidth, power consumption, etc. In terms of performance information, including performance validation, quantitative data is generally unavailable. Performance claims are given in qualitative terminology. This is a key shortcoming, particularly if a key dimension, such as clutter suppression performance, is necessary for an acquisition decision. Hence the determination of availability of COTS clutter suppression systems requires a more in-depth analysis.

Milestone 5: Investigation of new algorithms and known signal processing algorithms and sea clutter suppression.

The central focus of this project was to improve the ability to detect small boats by the use of advanced signal processing techniques to existing radar video. Previous milestones have discussed possible availability of radar video in existing radar systems, for the purpose of applying advanced signal processing techniques to the video and reduce clutter. Two tracks were pursued for this milestone. The first was to review high resolution sea clutter models. Several high-resolution models were described, and it was reported that high resolution sea clutter is globally non-Gaussian, which adds complexity to the modeling. The second part of this milestone reviewed advanced detection techniques to apply to the detection of small targets. A promising technique for detection in globally non-homogeneous clutter (i.e. where clutter varies from cell to cell) referred to as the “Parametric Generalized Likelihood Ratio Test (Parametric GLRT)” detector, which requires minimal training data was identified.

2.3.5. Future Work

This project focused on the objective of improving existing maritime radar detection of small targets by using advanced signal processing techniques to reduce sea clutter. This, in turn, requires access to the radar video, which is often not readily available. This report begins with the analysis of communications protocols that would apply to the wideband signals characteristic of radar video. This was followed by a survey of existing systems that use an open architecture that could operate over these protocols. Then, existing systems were reviewed to determine their operating specifications and performance. It was difficult, however, to determine quantitatively which system has the best clutter suppression performance. Finally, a review of advanced target detection techniques was provided. A promising technique is the Parametric GLRT, especially in view of its low requirement for training data.

A next step for this effort would be to acquire operational radar video (raw data) and apply the most promising signal processing and detection techniques, improve these techniques, test them to determine the probability of detection improvements for small targets at sea, and develop recommendations for implementing this capability on existing VTS radars.

3. Education and Outreach

3.1. Overview

MSC has established a robust portfolio of high-impact educational programs designed to provide hands-on, research-based learning opportunities for aspiring homeland security professionals. The Center's educational programs leverage the subject matter expertise and research capabilities of its academic partners to provide relevant programs for a broad audience of college-level students, professionals, and stakeholders. During Year 4, MSC offered the following homeland security-focused educational programs:

- Summer Research Institute
- Maritime Security Graduate Fellowship and Research Assistantship Programs
- MSI STEM Educators Workshop

MSC's educational programs are offered in collaboration with the Center's network of stakeholders. MSC stakeholders include the U.S. Coast Guard, Customs and Border Protection, National Urban Security Technology Laboratory (NUSTL), Port Authority of New York and New Jersey (PANYNJ), and DHS S&T Office of Intelligence and Analysis (I&A) to name a few. These stakeholders have contributed to the Center's educational programs by hosting field-visits, providing feedback on program content and curriculum, input on student research projects, and employment opportunities.

This section of the report provides a summary of MSC's education milestones, followed by a detailed account of the MSC's educational programs and outreach activities during Year 4.

3.2. Summary of Education Milestones

3.2.1. Doctoral Fellowships (Homeland Security and Mechanical Engineering Doctoral Fellowship)

Mr. John Martin completed his third year in the Mechanical Engineering & Homeland Security Doctoral Fellowship. During the 2017/2018 academic year, he completed 24 additional credits towards his doctoral degree program, presented two research posters and submitted two conference papers.

3.2.2. Maritime Systems Master's Degree (CDG) Fellowship Program (Maritime Security Master's Degree Fellowship)

Funds remaining from the Center's 2012 DHS CDG award were used to provide a one-year fellowship to Luciano Triolo, a graduate-level student in the Stevens Maritime System program. During Year 4, he completed a Master thesis titled "*Guidelines for a Remote Multi-spectral Emissions Monitoring System.*" Following his graduation in May 2018, he was hired by the Port Authority of New York/New Jersey as an Engineering Associate.

3.2.3. Undergraduate and Graduate-level Research Assistantships

MSC supported two students in Research Assistantships at Stevens Institute of Technology during Year 4. The students conducted research in the areas of mobile/modular maritime domain awareness and underwater robotics. The students were each enrolled full-time and maintained above a 3.30 cumulative GPA. In May 2018, Erik Pearson, doctoral research assistant presented his research in the form of a poster at the COE Summit, and undergraduate research assistant Dmitriy Savinsky completed his Bachelor of Engineering in Electrical Engineering and was hired as a Software Engineer at LGS Innovations.

3.2.4. MSI Outreach and Engagement in Research

MSC in conjunction with the U.S. Coast Guard Sector New York and faculty members from Stevens Institute of Technology developed and delivered an Environmental Data Collection and STEM Education workshop tailored to educators from Minority Serving Institutions and underserved communities. The workshop focused on the Coast Guard's use of weather forecasts and oceanic data to guide its operations and included hands-on activities and curriculum materials that can be used in higher education and K-12 classrooms to engage students in the collection, monitoring and visualization of environmental data.

3.3. College-Level Experiential Learning and Research-Based Programs

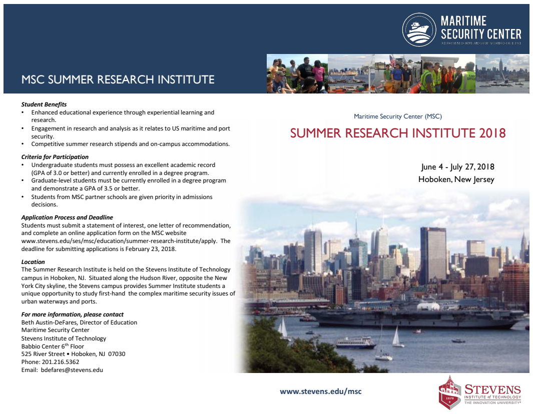
3.3.1. The 2018 Summer Research Institute

Milestones	Performance Metrics	Status/Discussion
1. Featured lectures by MSC researchers and invited guests. (Weeks One – Eight) (6/4/18 – 7/27/18)	- A minimum of four faculty lectures will be provided during the eight-week program. -A minimum of three homeland security/maritime industry guest speakers will be hosted during the summer research program. -The quality of and knowledge learned from the lectures will be assessed through a post- program student survey.	Complete: Four faculty lectures were held during the first week of the SRI. Complete: MSC hosted one guest speaker on-campus from DHS I&A, however, the students attended additional briefings provided by CBP, NUSTL, PANYNJ, and Rutgers as part of the Center's coordinated field-visits. A decision to limit the number of on-campus speakers was made to accommodate the number of field-visit opportunities. A post-program survey was distributed to the SRI student participants.

2. Field-visits and field-based activities. (Weeks One – Seven) (6/4/18 – 7/20/18)	-SRI students will engage in a minimum of two field-visits per summer research program. -MSC will facilitate a minimum of one field-based activity (meeting with stakeholders, research experiments/deployments, attendance at a workshop) during the program. -The impacts of the field-visits and field-based activities on student professional development and networking skills will be assessed through a post-program student survey.	Completed: Four field-visits were facilitated this summer. (CBP, NUSTL, PANY/NJ, NY Waterways lower Manhattan and Staten Island ferries, and Rutgers Center for Ocean Observation Leadership. Completed: Students participated in multiple experiments, including the deployment of an ROV in the Davidson Laboratory Tow Tank, and the hacking of an underwater glider at Rutgers, and engaged in conference call meetings with industry representatives from InSitu, SeaRobotics, and Schlumberger. Completed: A student survey was administered and completed by 21 of the 24 participants.
3. Diversity of student participants. (6/4/18 – 7/27/18)	-Diversity will be measured according to the range of engineering and science majors represented in the program. A minimum of four different disciplines will be represented per SRI program. - Student diversity will be measured by the percentage of women and minority students participating in the program each summer. A diverse student population will include a minimum of 50% women and/or minority students.	Completed: The SRI 2018 student cohort included students from 11 academic disciplines. Incomplete: MSC did not achieve its diversity goal of 50%, however, 42% of the students who accepted the Center's SRI offer of admission and who attended, were from underrepresented communities. (women and minority students).
4. Research Reports, Presentations and Posters.	-A minimum of two student research team reports will be prepared at the end of each SRI program.	Completed: Five student research reports were completed. Each of the

. (Week Eight) (7/23/18 – 7/27/18)	-A minimum of two student research team posters will be prepared at the end of each SRI program. -Students will engage in weekly status update presentations during weeks three – seven. -Stakeholder engagement will be assessed by representation of MSC stakeholders attending the final student team presentations. -Quality of SRI research outcomes will be assessed by MSC research mentor feedback and the number of projects selected for presentation at conferences and/or for publication. -Program impacts, e.g., professional development, technical skills learned, student interest in advanced academic study or careers in homeland security will be assessed by a post-program student survey.	student teams also prepared final presentation slides and research posters. Completed: The student teams each presented their research progress during weeks 3 – 7. Completed: Representatives from NUSTL, CBP and PANYNJ attended the SRI final research presentations. SRI survey showed that students significantly improved their skills in several skill areas. 86% of the students reported that the SRI had enhanced their interest in careers in HS.
5. Post-Program and SRI alumni survey. Post-program surveys to be conducted (Week Eight) (7/23/18 – 7/27/18)	-A minimum of one student survey will be conducted at the end of each summer research program. The survey will be used to measure the strengths and weakness of the program, the program's impacts on student interest and skills development, and to gather feedback to enhance the future delivery of the program.	Completed: A student survey was completed by the program participants and assessed by the MSC.

MSC held its 9th Annual Summer Research Institute from June 4 – July 27, 2018, at the Stevens Institute of Technology campus in Hoboken, NJ. Since the Summer Research Institute's inception in 2010, 162 students have conducted research in conjunction with MSC research PIs, stakeholders and Stevens' faculty members. Each year, the Center identifies a set of student research projects based on conversations and interactions with its stakeholders and takes into consideration the Center's ongoing and emerging areas of research. The SRI student research projects are purposely designed to expose students to critical issues in the maritime domain and to challenge them to find innovative and technological approaches to address them.



MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

MSC SUMMER RESEARCH INSTITUTE

Student Benefits

- Enhanced educational experience through experiential learning and research.
- Engagement in research and analysis as it relates to US maritime and port security.
- Competitive summer research stipends and on-campus accommodations.

Criteria for Participation

- Undergraduate students must possess an excellent academic record (GPA of 3.0 or better) and currently enrolled in a degree program.
- Graduate-level students must be currently enrolled in a degree program and demonstrate a GPA of 3.5 or better.
- Students from MSC partner schools are given priority in admissions decisions.

Application Process and Deadline

Students must submit a statement of interest, one letter of recommendation, and complete an online application form on the MSC website www.stevens.edu/ses/msc/education/summer-research-institute/apply. The deadline for submitting applications is February 23, 2018.

Location

The Summer Research Institute is held on the Stevens Institute of Technology campus in Hoboken, NJ. Situated along the Hudson River, opposite the New York City skyline, the Stevens campus provides Summer Institute students a unique opportunity to study first-hand the complex maritime security issues of urban waterways and ports.

For more information, please contact

Beth Austin-DeFares, Director of Education
Maritime Security Center
Stevens Institute of Technology
Babbio Center 6th Floor
525 River Street • Hoboken, NJ 07030
Phone: 201.216.5362
Email: bdefares@stevens.edu

Maritime Security Center (MSC)

SUMMER RESEARCH INSTITUTE 2018

June 4 - July 27, 2018
Hoboken, New Jersey

www.stevens.edu/msc

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Figure 1. SRI 2018 Program Brochure

During Year 4, the MSC hosted 24 student participants representing eight universities, including Cooper Union, Elizabeth City State University, Marist College, New Jersey Institute of Technology, Stevens Institute of Technology, Tiffin University, University of Alaska – Fairbanks, and the University of Hawaii. Out of the student cohort, 96% of the students were undergraduates and 42% were from underrepresented communities (e.g. women and minority students).

To support student participation in the 2018 summer research program (e.g., housing, stipend and travel), the Center leveraged existing Stevens Institute of Technology programs to recruit students who could attend the program fully-funded through external funding sources. Out of the 24 program participants, eleven students attended the program leveraging funding from Stevens' Pinnacle Scholars Program. Funding for the remaining 13 students was provided by the Maritime Security Center.

The MSC-funded students were selected through the Center's academic partnerships and through a competitive admission process. The students admitted into the program were endorsed by their academic professors and met or exceeded the Center's admission criteria. Figure 2 below shows the students on a field-visit to CBP Field Operations at the Port of New York/Newark. Table 2 identifies the participants and the funding sources leveraged to support their participation.

Figure 2. SRI 2018 student participants.

Table 2. Summer Research Institute 2018 Participants and Leveraged Funding

University	Student	Major	Funding Source
Cooper Union	Gregoire Caubel	Mechanical Engineering	MSC
Elizabeth City State University	Narendra Banerjee	Computer Science	MSC
Marist College	Chris Schlappich	Applied Mathematics	MSC
NJ Institute of Technology	Simone Coleman	Information Technology/Cybersecurity	MSC
Stevens Institute of Technology	Michael Alecci Domenico Albarella Allen Best Liam Brew Theo Cheevers Nicholas Duca Ameya Ivaturi Victoria Kapp Justin Sitler Asif Uddin Kurt von Autenried Herb Zieger Joshua Zietlinger	Mechanical Engineering Mechanical Engineering Software Engineering Software Engineering Environmental Engineering Finance Chemical Engineering Mechanical Engineering Mechanical Engineering Mechanical Engineering Software Engineering Software Engineering Computer Science	Stevens Scholar Stevens Scholar MSC MSC MSC Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar Stevens Scholar MSC Stevens Scholar
Tiffin University	Zoe Blough	Digital Forensics	MSC
Univ. of Alaska-Fairbanks	Naomi Kroyer	Electrical Engineering	MSC
Univ. of Hawaii	Makiko Kuwahara	Electrical Engineering	MSC

3.3.2. Student Qualifications and Documentation

Participation in the Summer Research Institute requires that students be actively enrolled in an undergraduate or graduate-level degree program at an accredited university. Undergraduate students must possess a minimum GPA of 3.0, and graduate-level (Masters and PhD) students are required to have a GPA of 3.5 or better. This past summer's participants were required to complete an online application form, write a personal statement of interest, submit letters of recommendation and transcripts upon request. In accordance with Stevens policy, visiting SRI students were also required to demonstrate proof of health insurance and submit immunization records.

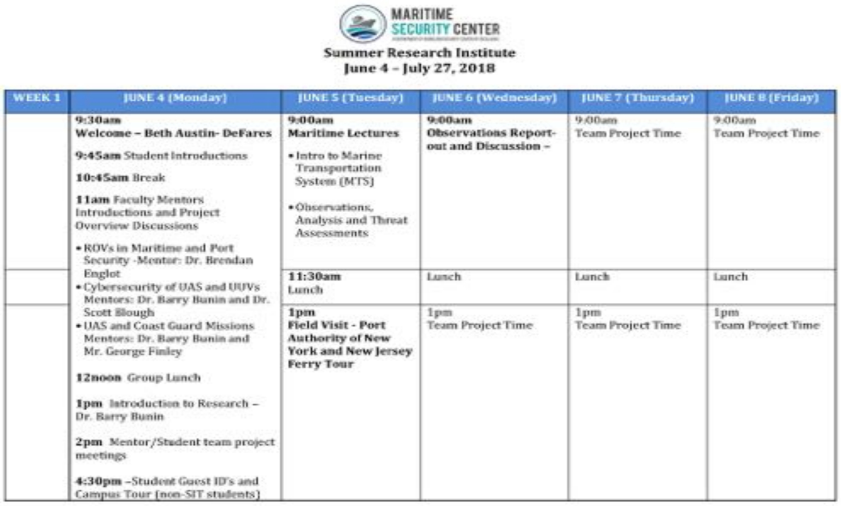
3.3.3. Summer Research Stipends and Housing

MSC funded students (13) received summer stipends of $4,000 and were provided with on-campus accommodations as needed. Travel reimbursements up to $1,000 were also made available for transportation to and from the start and end of the program for students residing outside the state of New Jersey.

3.3.4. Program Administration

The 9th annual SRI was organized and coordinated by MSC Director of Education, Beth Austin-DeFares, in conjunction with Dr. Barry Bunin (Director, Stevens Institute of Technology Maritime Security Program). Ms. Austin-DeFares served as the primary program facilitator, while Dr. Bunin participated as the lead faculty member and curriculum developer. He also served as the overall technical lead on the summer research projects and provided assistance to students in both theoretical and practical implementation of the projects. In addition to Dr. Bunin, SRI student team mentorship was provided by Mr. Scott Blough, Executive Director of the Center for Cyber Defense and Assistant Professor of Criminal Justice & Security Studies at Tiffin University, Dr. Brendan Englot, Director of the Robust Field Autonomy Laboratory and Assistant Professor in Mechanical Engineering at Stevens Institute of Technology, and Dr. Hugh Roarty, Research Project Manager at the Center for Ocean Observation Leadership at Rutgers University.

3.3.5. Program Format and Curriculum



MARITIME SECURITY CENTER

Summer Research Institute
June 4 – July 27, 2018

WEEK 1	JUNE 4 (Monday)	JUNE 5 (Tuesday)	JUNE 6 (Wednesday)	JUNE 7 (Thursday)	JUNE 8 (Friday)
	9:30am **Welcome – Beth Austin- DeFares** **9:45am** Student Introductions **10:45am** Break **11am** Faculty Mentors Introductions and Project Overview Discussions • ROVs in Maritime and Port Security -Mentor: Dr. Brendan Englot • Cybersecurity of UAS and UUVs Mentors: Dr. Barry Bunin and Dr. Scott Blough • UAS and Coast Guard Missions Mentors: Dr. Barry Bunin and Mr. George Finley **12noon** Group Lunch **1pm** Introduction to Research – Dr. Barry Bunin **2pm** Mentor/Student team project meetings **4:30pm** –Student Guest ID's and Campus Tour (non-SIT students)	**9:00am** **Maritime Lectures** • Intro to Marine Transportation System (MTS) • Observations, Analysis and Threat Assessments	**9:00am** **Observations Report-out and Discussion –**	9:00am Team Project Time	9:00am Team Project Time
		11:30am Lunch	Lunch	Lunch	Lunch
		1pm **Field Visit - Port Authority of New York and New Jersey Ferry Tour**	1pm Team Project Time	1pm Team Project Time	1pm Team Project Time

Figure 3. Schedule for Week One of the 2018 SRI.

The eight-week program includes in-class lectures, student team research projects, professional development activities, and field-visits to DHS operational environments. One week prior to the start of the program, the students were provided with pre-reading assignments and homework. During Week One, the assignments were reviewed and the student participants attended a sequence of maritime domain and homeland security focused lectures. The lectures, delivered by Dr. Barry Bunin, included talks on maritime security policies, maritime industry and government stakeholders, port facility infrastructure and operations, and current and emerging threats.

During Week One, the SRI student participants were also assigned into one of the following five project teams:

- Utilization of Unmanned Aerial Systems (UAS) in Law Enforcement, Safety and Security
- Cybersecurity of UAS and Unmanned Underwater Vehicles (UUVs)
- Remotely Operated Vehicle (ROV) Autonomy for Undersea Pipeline Inspection
- ROV Autonomy for Ship Hull Cleaning of Biofouling
- Wave Glider Design Optimization – Enhanced Persistence Surveillance

Starting Week Two, the program format shifted from time spent in the classroom to time spent engaging in team research projects, field-based visits and experiments, and meetings with maritime and homeland security practitioners. During the next five-week period, the student teams also began to provide status updates on their research in the form of weekly presentations. Each team was responsible for providing a fifteen to twenty-minute presentation discussing their research, field-based activities, and challenges and progress in their work. MSC also hosted a guest speaker from the DHS S&T Office of Intelligence and Analysis and facilitated field-visits to Customs and Border Protection Field Operations at Port NY/NJ, National Urban Security Technology Laboratory, Rutgers Center for Ocean Observing Leadership, and security observations on the NY Waterways and Staten Island Ferries. Details regarding the guest speaker and field-visits are provided later in this report.

In Week Seven, the student teams synthesized their research outcomes and started to compile their final reports, presentations and research posters. In Week Eight, the last week of the summer research program, students presented their research to an audience of academic researchers (MSC, Stevens, Rutgers, Tiffin University) and representatives from the DHS S&T network (NUSTL) and the cybersecurity intel firm Flashpoint, Inc.

Tables 3 and 4 below illustrate the program activities and guest speakers for each week of the 2018 summer research program.

Table 3. SRI 2018 Program Activities Weeks One to Eight

Schedule	Topic	Faculty /Guest Speakers	SRI 2018 Activities
Week One June 4 – 8	Orientation - MTS and Maritime Security Overview	Faculty: Dr. Barry Bunin	Discussions/lectures on maritime security and vulnerabilities. Field visits: PANY/NJ / NYC ferry terminals.

Week Two June 11 - 15	Team Research Projects		Field-visit: NUSTL and CBP Field Operations at the Port of NY/Newark. Experiment: UAS calibration
Week Three June 18 - 22	Team Research Projects	Guest Speaker: DHS S&T Office of Intelligence and Analysis	Status Update Presentations
Week Four June 25 – 29	Team Research Projects		Status Update Presentations
*Note that activities after July 1 for the SRI are considered planned activities for Year 5, but are reported here for consistency and program continuity.)			
Week Five July 2 – July 6	Team Research Projects		Status Updates with faculty mentors
Week Six July 9 – 13	Team Research Projects		Experiment: ROV Deployment Davidson Lab -Status Update Presentations
Week Seven July 16 - 20	Research Synthesis		Report writing, presentation slide preparation and research posters. –Status Update Presentations and Rehearsals
Week Eight July 23 – 27	Research Outcome Presentations and Reports	MSC and academic partner representatives, invited DHS S&T stakeholders & industry guests	Final presentation on research outcomes, reports and posters

Table 4. SRI 2017 Guest Speakers

Guest Speaker	Organization	Lecture Topic
Luis Feliciano	Office of Intelligence and Analysis (I&A)	DHS I&A Mission Briefing
Supervisor Noel Moloney	CBP Field Operations Port of NY/Newark	CBP Mission Briefing (Field-visit)
Dr. Adam Hutter, Director	National Urban Security Technology Lab (NUSTL)	DHS S&T NUSTL Mission Briefing and Test and Evaluation Overviews of First Responder Technologies
Dr. Hugh Roarty, Research Project Manager	Center for Ocean Observation Leadership, Rutgers	Briefing on Slocum Glider operations, including information technology and operational systems.

3.3.6. Field Visits and Meetings with Practitioners

Field-visits to ports and homeland security facilities are a key component of the Summer Research Institute. Field-visits provide a first-hand opportunity for students to observe the operational activities and responsibilities of homeland security professionals in the field (see Figure 4 below).

Figure 4. SRI 2018 participants receive a security briefing at the Waterways Ferry Terminal in lower Manhattan, NYC.

This summer's program featured field-visits and coordinated activities with representatives from the following organizations:

- Customs and Border Protection (CBP) Field Operations Division - Port of New York/Newark (Field-visit and briefing)
- National Urban Security Technology Laboratory (NUSTL) (Field-visit and technology briefings)
- Port Authority of NY and NJ (PANYNJ) – NY Waterways lower Manhattan and Staten Island Ferry (Briefing and Security Observation Exercise)
- Center for Ocean Observation Leadership, Rutgers University (Field-visit and cybersecurity hacking experiment.)

This was the Center's seventh annual student field-visit to CBP at the Port of NY/Newark and its second visit to NUSTL. The visit to CBP included observations of radiation portal monitors in use, high-energy mobile non-intrusive inspection (NII) equipment scanning cargo containers, and a tour of a Centralized Examination Station warehouse where cargo is physically inspected and analyzed.

The visit to NUSTL included a discussion with Dr. Adam Hutter, Director, as well as a sequence of demonstrations and briefings by NUSTL's team of engineers and scientists. Among the presenters were three of MSC's former DHS CDG Fellows, Blaise Linn, Tyler Mackanin and Chris Polacco, who are employed as Junior Engineers with the Laboratory.

3.3.7. Student Research Projects

The SRI 2018 student research projects were developed in conjunction with MSC's academic partners from Stevens Institute of Technology and Tiffin University and were intended to support the Center's on-going research in the areas of unmanned systems and maritime cybersecurity. The summer research projects and student team assignments are described below.

Research Team/Project: ***Utilization of Unmanned Aerial Systems (UAS) in Law Enforcement, Safety and Security***

Figure 5: Students on the UAS team have submitted an invention disclosure for work they completed during the 2018 Summer Research Institute.

The original objective of the UAS in Law Enforcement, Safety and Security team, also known as the UAS Buoy team, was to assess the utilization of drone technology to support U.S. Coast Guard mission areas, namely search and rescue operations, drug interdiction and illegal immigration and illegal fishing. Through the team's research and correspondence with the USCG Research and Development Center and conversations with representatives from Insitu Inc., a subsidiary of Boeing that focuses specifically on drone applications in security and defense, the team learned that these systems are already beginning to be utilized to support Coast Guard operations.

In an effort to refocus their project, the team identified a new application where UASs can be utilized to deploy Self-Locating Datum Marker Buoys (SLDMB) used during search and rescue missions and in the collection of oceanic data. Originally designed for deployment by Coast Guard vessels, the tracker buoys are equipped with GPS and upon deployment in the water can transmit their location while afloat in changing currents and weather conditions.

After researching the payload limitations of commercial drone systems, the multidisciplinary student team set out to design a lightweight modular buoy system that be deployed by drone and equipped with a sensor suite capable of transmitting not only the buoys location, but relay critical oceanic and environmental data. Such information could be utilized to assist the Coast Guards rapid response during environmental disasters and search and rescue operations, and in improving the resolution of weather forecasting ocean models. The team's UAS Buoy System design includes a streamlined release mechanism, a lightweight SLDMB with modular sensor suites, and software to calculate the trajectory and release GPS coordinates.

Given the potential utility and novelty of the team's design, MSC administrators contacted Stevens Institute of Technology's Office of Technology Commercialization to assess the feasibility of the team's work to be patented. After a brief prior review, the team was encouraged to submit an invention disclosure through the university and are currently working on developing a prototype and filing for a provisional patent. The Center will continue to mentor and assist the student research team throughout the patent process.

Details regarding the team's research methodology and project outcomes can be found in their final research report, presentation slides and research poster located on the MSC website at: *https://www.stevens.edu/SummerResearchInstitute*. Table 6 below identifies the student team members, their academic disciplines and their university affiliation.

Table 6. UAS Buoy Student Research Team

Student	**Academic Discipline**	**School**
Domenico Albarella	Mechanical Engineering	Stevens Institute
Theodore Cheevers	Environmental Engineering	Stevens Institute
Eric Fernandes	Software Engineering	Stevens Institute
Makiko Kuwahara	Electrical Engineering	University of Hawaii
Herb Zieger	Software Engineering	Stevens Institute
Faculty Mentor: Dr. Barry Bunin, Stevens Institute		

Research Team/Project: ***Cybersecurity of UAS and Unmanned Underwater Vehicles (UUVs)***

Figure 6. The largest of the five SRI 2018 student research teams, the Cybersecurity team included students from Elizabeth City State University, Stevens Institute and Tiffin University.

.
The Cybersecurity research team included a diverse team of students representing seven academic disciplines and three universities. Led by faculty mentors Scott Blough, Executive Director for the Center of Cyber Defense at Tiffin University and the chair of the 2017 U.S. Coast Guard Maritime Risk Symposium and Barry Bunin, Chief Architect, Maritime Security Laboratory at Stevens Institute, the team aimed to enhance the security of select UAS and Unmanned Underwater Vehicles (UUVs) from cyber hacking and attack. The team's objectives were to accomplish the following tasks:

- Learn the systems architecture and communications capabilities of off-the-shelf, commercially available UAS, in addition to UUVs.
- Develop a detailed understanding of how the communications links could be hacked.
- Determine the best way to attack a UAS, UUV or Unmanned Surface Vehical (USV).
- Build a simulated attack scenario for demonstration, using available off-the-shelf MSC and Tiffin University hardware.

The team prepared the following abstract describing their work: "The United States government does not have the proper protocols set in place when dealing with a security breach via Unmanned Aerial Systems (UAS). The Cybersecurity student research team at the Maritime Security Center researched how current cybersecurity measures apply to counter hostile UAS. To combat this security concern, the team came up with the No Drone Zone system which creates an area that identifies and takes control of drones that enter a high-risk site. This system targets both WiFi controlled and radio-controlled drones. The team utilized a Raspberry Pi, Software Defined Radio (HackRF), and Python and Bash scripts to create components of the No Drone Zone system. As it stands, this system can effectively identify and hack a Wifi controlled drone, and successfully identify a radio-controlled drone. In the future, the neutralization of a Wifi controlled drone will need updates as the security protocols become advanced. Neutralizing a radio-controlled drone will need updates as the security protocols become advanced. Neutralizing a radio-controlled drone will need more advanced equipment to implement an attack that will hijack the malicious drone."

While conducting their research, the team also met with researchers from the Center for Ocean Observation Leadership at Rutgers University who discussed the cybersecurity of its fleet of unmanned underwater ocean gliders used for oceanic research. Following a briefing on the glider's information and operational technologies (IT/OT), the team worked to hack the system and subsequently prepared a comprehensive overview of the systems' cyber vulnerabilities. The team also offered recommendations and outlined steps that the Rutgers research team can take to enhance the cybersecurity of fleets IT systems.

At the culmination of the eight-week program, the team developed a concept for a "No Drone Zone" application that can be used abroad vessels (cargo ships, cruise ships, etc.) to thwart drone incursions while transiting through waters known to be frequented by pirates and hostile actors. (e.g. Straits of Malacca, Horn of Africa, and the Coast of Somalia, etc.).

A copy of the team's final report, presentation slides and research poster can be found on the Center's website at: *https://www.stevens.edu/SummerResearchInstitute*. Table 5 below identifies the student team members, their academic disciplines and their university affiliation.

Table 5. Cybersecurity – Student Team

Student	**Academic Discipline**	**School**
Michael Alecci	Mechanical Engineering	Stevens Institute
Narendra Banerjee	Engineering Technology	Elizabeth City State University
Allen Best	Software Engineering	Stevens Institute
Liam Brew	Software Engineering	Stevens Institute
Zoë Blough	Digital Forensics	Tiffin University
Simone Coleman	Information Technology	NJ Institute of Technology
Nick Duca	Business Management	Stevens Institute
Ameya Ivaturi	Chemical Engineering	Stevens Institute
Joe Sette	Mechanical Engineering	Stevens Institute
Kurt von Autenreid	Software Engineering	Stevens Institute
Angelina Zaccaria	Computer Engineering	Stevens Institute
Faculty Mentors: Scott Blough, Tiffin University and Dr. Barry Bunin, Stevens Institute		

Figure 7. Dr. Brendan Englot, Director of the Robust Field Autonomy Lab at Stevens Institute of Technology (pictured back row far right) mentored a collection of three student teams, each focused on ROV research.

Research Team/Project: *ROV Autonomy for Undersea Pipeline Inspection (BlueROV2)*

The Summer Research Institute BlueROV team conducted a series of experiments to demonstrate the autonomous detection, tracking and mapping of subsea pipeline in the Stevens Davidson Lab tow tank. The team assisted in the tasking and control of the ROV and in the analysis of its multi-beam sonar system. The team's work emphasized the need to enhance the safety and security of homeland security professionals in missions that maybe related to underwater environmental disasters (e.g., Deepwater Horizon), or in emerging applications in the Arctic region.

The team prepared the following abstract to discuss their research project: "The research involves discovering the optimal way to detect, track, and map a subsea pipeline using a sonar equipped remotely operated vehicle, BlueROV2. The principal goal was to take a two-dimensional image and pinpoint the location of an oil pipe with high accuracy. The data for the image was gathered by the Oculus 750d sonar sensor after analyzing a subsea pipe mockup. Another challenge addressed was finding a way to integrate additional sensors onto the vehicle. The findings of this research would be useful in mitigating environmental disasters by inspecting underwater settings and locating abnormalities."

The team's work will continue to be utilized by graduate students and faculty members working within the Robust Field Autonomy Lab at Stevens. The team's research methodology and project results can be found in their final research report, presentation slides and research poster located on the MSC website at *https://www.stevens.edu/SummerResearchInstitute*. Table 7 below identifies the BlueROV team members, their academic disciplines of study and their university affiliation.

Table 7. BlueROV – Student Research Team

Student	Academic Discipline	School
Victoria Kapp	Mechanical Engineering	Stevens Institute
Naomi Kroyer	Electrical Engineering	Univ. of Alaska-Fairbanks
Asif Uddin	Mechanical Engineering	Stevens Institute
Joshua Zietlinger	Computer Science	Stevens Institute
Faculty Mentor: Dr. Brendan Englot, Stevens Institute		

Research Team/Project: *Wave Glider Design Optimization*

The Wave Glider team's work aimed to increase the understanding of how low profile, unmanned surface vessels can best harvest wave energy to maximize its forward velocity. Unmanned surface vessels, like the Wave Glider, are being used for maritime security purposes in coastal waters and open ocean environments. The low-cost, mobile platforms can be equipped with a range of sensors to provide persistent surveillance and situation awareness capabilities for the U.S. Coast Guard and other maritime and homeland security related organizations.

The principal objective of the student team's research was to conduct a paper study and to develop models to test assumptions regarding the propulsion design of surface vessels in ocean currents. By understanding how the system components work together (e.g. the float, glider, umbilical tether and hydrofoils) and the physics that govern the forward motion of the glider, the team worked to create a dynamic model and to simulate a variety of physical parameters that would test the velocity and forward propulsion of the glider.

The team prepared the following abstract to describe their research: "In order to optimize the parameters of the Wave Glider system, we started by trying to develop an accurate dynamical model of the three-part system. The first step in this process was validating or debunking existing dynamical models. From there, we gathered assumptions and key components from the existing dynamical models to create our own dynamical model. One key assumption is that the glider and the float are rigidly attached by the umbilical. This means the vertical motion of the glider is known because it is forced by the wave motion. Another key assumption is that the hydrofoils on the glider can be treated as flat plates and that their geometry is essentially insignificant. The final key assumption is that the motion of the hydrofoils is actually a square wave instead of a sinusoidal wave. The time that the hydrofoils spend in the transient phase in negligible and can be treated as such. Our dynamical model runs in Simulink and pulls drag coefficients from SolidWorks. Treating the hydrofoils on the glider as generic plates, we simulated the liquid flow around a plate at different velocities. We solved for the drag coefficients from there. Then, we took physical specifications about the Wave Glider such as mass, lengths, widths, etc. from existing papers to create our own dynamical model. Using our dynamical model, the Wave Glider will reach a terminal velocity of around 1.3 meters per second or 2.53 knots. Employing a constant force instead of a time-dependent sinusoidal force will eliminate the oscillatory behavior about the terminal velocity."

The team's research determined that neural networks can be used to test combinations of parameters to obtain optimal steady state velocity.

The team's research methodology and project results can be found in their final research report, presentation slides and research poster located on the MSC website at *https://www.stevens.edu/SummerResearchInstitute.* Table 8 below identifies the Wave Glider Optimization team members, their academic disciplines of study and their university affiliation.

Table 8. Wave Glider – Student Team

Student	Academic Discipline	School
Chris Schlappich	Applied Mathematics	Marist College
Justin Sitler	Mechanical Engineering	Stevens Institute

Faculty Mentor: Dr. Brendan Englot, Stevens Institute of Technology

Research Team/Project: ROV Autonomy for Ship Hull Cleaning of Biofouling - HullBug

The U.S. military spends in excess of one billion dollars each year to fuel its fleet of vessels. One method for enhancing the fuel efficiency of military and commercial maritime industry ships, is to reduce the frictional drag caused by biofouling (e.g. barnacles and algae) that attach and buildup on ship hulls. With the routine use of hull cleaning systems, such as SeaRobotics' HullBug ROV, it has been estimated that the U.S. military can save roughly 15% or $300 million dollars each year in fuel expenditures. The use of these systems however, is timely and requires trained personnel to methodically maneuver the underwater robots.

The students on the ROV Autonomy team sought to improve the HullBug ROV, by advancing its performance and navigational autonomy, and making it more efficient and less dependent on human interaction when performing routine cleanings. With enhanced autonomy, the team believed that the hull cleaning robot would have greater potential to further reduce fuel consumption and carbon emissions of the U.S. military's vessels, as well as those for the private maritime industry. (e.g. cargo and cruise ships)

The team's research included an assessment of commercially available off-the-shelf sensors. Taking into consideration the size, cost and performance of the sensors, the team selected a suite of three sensors to assist with the path finding capabilities and stability of the ROV system. Using MATLAB models and simulations, the team was able to validate the accuracy and reliability of the sensor suite. Working in conjunction with SeaRobotics, the makers of the ROV, the team recommended that the HullBug incorporate an Oculus 750d Multibeam Sonar for underwater imaging, a KVH1750 Fiber Optic Gyro for sensing changes in the ROVs orientation, and a Nortek DVL1000 for underwater navigation and positioning.

The team's research will continue beyond the MSC summer research program, and will include a field-based testing and evaluation of the sensor suite by the Robust Field Autonomy Laboratory at Stevens Institute of Technology during the 2018/2019 academic year.

An abstract for the team's project is provided below:

Project Abstract: "The research performed during the SRI leverages a Stevens Institute of Technology project being conducted in collaboration with SeaRobotics. The goal of the project was to determine a suite of sensors with which the HullBug, an unmanned underwater vehicle, can be adapted for enhanced autonomy and ship hull grooming capabilities. Currently available on the market, the HullBug is used for removing biofouling from the hulls of ships. With enhanced autonomy however, the hull cleaning robot has immense potential to drastically reduce the fuel consumption and carbon emissions of the U.S. military's fleet of vessels (e.g., Navy, Coast Guard), as well as those for the private maritime industry (e.g., cargo ships, cruise ships).

The sensors reviewed by the student team were chosen for a variety of reasons, including size, cost, and their given performance. Decisions to implement the sensors were made using a state-space representation of the HullBug to determine the overall random walk that the robot would experience based on the drift rates of its sensors, as well as from a thorough review of peer reviewed research papers on autonomous robotics."

The team's research methodology and project results can be found in their final research report and presentation slides on the MSC website at *https://www.stevens.edu/SummerResearchInstitute*. Table 9 below identifies the student team, their academic majors and their university affiliation.

Table 9. HullBug ROV - Student Research Team

Student	**Academic Discipline**	**School**
Gregoire Caubel	Mechanical Engineering	Cooper Union
Anthony Donatelli	Computer Engineering	Stevens Institute
Faculty Mentor: Dr. Brendan Englot, Stevens Institute of Technology		

3.3.8. SRI 2018 Student Survey

An assessment of the summer research program was conducted via a student survey (see Appendix E-2 for a copy of the student survey questions and format). Student participants were each asked to complete an online survey and to provide feedback on the program, the student's learning gains, areas for program improvement and program impacts on student interest in advanced study and/or careers in homeland security. 21 students out of the 24 participants completed the program survey.

A majority of the student respondents rated the SRI Very Good to Excellent in the following categories:

- Field-visits and Stakeholder Engagement (95%)
- Program Coordination/Administration (90%)
- Teamwork/Collaboration (90%)
- Research Project Outcomes (90%)
- Faculty and Guest Lectures (81%)
- Program Format and Curriculum (81%)
- Faculty Mentorship and Guidance (71%)

86% of the survey respondents said that the SRI enhanced their interest in advanced academic study and careers in the homeland security domain, and 100% of the students reported that they would recommend the program to their peers and colleagues at their respective schools.

When asked to what extent the SRI enhanced or improved their skills, a majority of the students reported "Significant Improvement" in the following areas:

- Networking (65%)
- Teamwork/Collaboration (48%)
- Ability to Conduct Research (43%)

When asked to identify their “top takeaways” from the program, the students commonly mentioned the following:

- Teamwork and collaboration.
- Networking with stakeholders and field-visits.

The students worked in collaboration with assigned researcher mentors and had the unique opportunity to interact and engage with homeland security practitioners.   Through their experience in the summer research program, students gained a greater awareness of maritime and homeland security issues. Student survey responses show that participation in the SRI has effectively inspired student interest to pursue careers and academic study in the homeland security domain. Collectively, the SRI was effective in achieving the following outcomes:

- Student presentations and research reports demonstrated the students gained knowledge and understanding of the maritime security domain and their respective research projects. 57% of the students stated that their understanding of their assigned research area improved sufficiently and they could apply what they learned, whereas 38% said that they had gained advanced knowledge and confidence in the research area.
- A majority of the students (86%) expressed enhanced interest in pursuing careers and/or advanced academic study in maritime/homeland security as a result of their participation in the SRI.

3.3.9. SRI Lessons Learned

MSC continuously strives to enhance the learning experiences of its students by modifying and tailoring the SRI program format according to the survey feedback. For this year’s program, the Center continued to limit the number of in-class faculty and guest lectures in lieu of more time for the students to conduct their research. The program administrators also leveraged broader research engagement across its academic network, to include faculty participation from Tiffin University, experts in the field of Cybersecurity and Digital Forensics, and from Rutgers Center for Ocean Observation Leadership who provided access to their fleet of underwater gliders and input on drifter buoys.

3.4. Fellowship and Research Assistantship Programs

Milestones	Performance Metrics	Status/Discussion
1. Homeland Security Research Assistantships. 7/1/17 – 6/30/18	Confer a minimum of one Assistantship.	Completed: Leveraging funds remaining in the Center’s 2012 CDG, MSC supported one student through the completion of his Master’s degree in Maritime Systems with a concentration in Maritime Security, and one undergraduate degree student in Electrical Engineering.

3.4.1. MSC Supported Students (2017-2018)

The following students were supported by the MSC during Year 4.

Student	Award / Program	Research / Activities
Dmitriy Savinsky	Undergraduate Research Assistantship / Electrical Engineering	Conducted research focused on Mobile, Modular Sensor Platforms. Completed B.Eng degree. Employed by LGS Innovations
Luciano Triolo	Master's Degree Fellowship / Maritime Systems and Security	Conducted research on the multispectral imaging of vessel emissions. Completed a thesis and MS degree. Presented research poster at the COE Summit. Employed by Port Authority of NY/NJ.
Erik Pearson	Graduate Research Assistantship / Mechanical Engineering Doctoral Program	Conducted research focused on the use of a heterogeneous team of mobile robots for port and harbor security. Presented research poster at COE Summit.
John Martin	Homeland Security and Mechanical Engineering Fellowship / Mechanical Engineering Doctoral Program	Conducted research focused on enabling robust robot intelligence for underwater surveillance. Completed coursework/research towards a doctoral degree in Mechanical Engineering. Submitted two conference papers and presented research posters, including at the COE Summit.

During the 2017 / 2018 academic year MSC continued to support the Undergraduate Research Assistantship for Electrical Engineering student Dmitriy Savinsky. Throughout his two-year assistantship, Dmitriy provided research support on projects related to mobile, modular sensor platforms that can be used to bolster Maritime Domain Awareness (MDA) for the U.S. Coast Guard and other DHS component agencies. At the Center's 2017 annual meeting, Dmitriy also presented independent research that he had conducted in the area of AIS fraud detection.

In May 2018, he completed his degree requirements to receive a Bachelor of Engineering degree in Electrical Engineering from Stevens Institute of Technology and is now employed as a Software Engineer with LGS Innovations, a technology development company that provides support to the DHS and DOD.

In the spring of 2018, the Center also provided funding support to Erik Pearson, Mechanical Engineering Doctoral Candidate. Throughout the spring semester, Erik conducted research aimed at enhancing the autonomy of underwater remotely operated vehicles (ROV) for enhanced maritime security operations. Erik's work was presented in the form of a research poster at the DHS S&T COE Summit in Arlington, VA. An abstract describing his work is provided below:

"Exploring the Unknown for High Resolution Imaging - Large unknown spaces often create a massive amount of data points that inhibits quick processing, which is required for exploration. The data size can be subsidized by using a quadtree format such as an Octomap. However, most search algorithms today have a low-resolution minimum for detailing physical objects when exploring large spaces, caused by the number of data points constraint. My research focuses on scanning physical objects to get a high-resolution image of physical structures in large, open areas such as underwater or in the air, without vastly increasing the number of data points. The algorithm can also take into account initial conditions. These conditions can define a volumetric box as a search boundary as well as any expected points of interest. Due to the two parts of the algorithm, the processing can be split between a server and a local robot. This decentralized nature of the exploration algorithm can be used with a swarm of robots with one main hub, or mothership. The Robust Field Autonomy Lab at Stevens has access to a WAM-V unmanned surface vessel, and Videoray ROV which will be used to do preliminary testing of multi-robot underwater exploration utilizing this algorithm."

3.4.2. Mechanical Engineering and Homeland Security Doctoral Fellowship – DHS Career Development 2015 Supplement Award

Mr. John Martin was selected to receive the Center's Mechanical Engineering and Homeland Security Doctoral Fellowship in the fall of 2015. In May 2018, he completed his third year in the Mechanical Engineering Doctoral program, where he is conducting research in conjunction with his dissertation advisor, Dr. Brendan Englot, Assistant Professor, Mechanical Engineering. During the 2017/2018 academic year, John completed 24 additional credits towards his PhD requirements and engaged in the following courses and fellowship activities:

Semester	Courses/Activities	Credits
Spring 2018	MA612 Mathematical Statistics	3
Spring 2018	ME960: Mechanical Engineering Doctoral Research	6
Spring 2018	FE542: Time Series Analysis	3
Fall 2017	ME960: Mechanical Engineering Doctoral Research	3
Fall 2017	MA611: Introduction to Probability and Measure	3
Fall 2017	FE541: Applied Statistics with Applications to Finance	3

John's fellowship and research activities during Year 4 included the following:

- MSC Annual Review Meeting (October 2017) Presented research titled *Enabling Robust Robot Intelligence*
- New York Academy of Sciences – Machine Learning Symposium (March 2018 Presented poster: *Actor-critic Methods using Distributed Gaussian Process Temporal Differences*
- Robotic Science and Systems (Feb 2018). Submitted conference paper: *Temporal Difference Learning with Sparse Gaussian Processes for Robot Control*
- Robot Mechanical Engineering Graduate Seminar Series (March 2018). Presented 20min presentation: *Temporal Difference Learning with Parse Gaussian Processes for Robot Control*
- DHS 2018 COE Summit (May 2018). Presented poster: *Distributed Gaussian Process Regression for Efficient Robot Learning*
- Conference on Robot Learning (June 2018). Submitted conference paper: *Sparse Gaussian Process Temporal Difference Learning for Marine Robot Navigation*

Over the coming academic year, John will complete his doctoral studies and defend his dissertation. MSC will continue to provide funding support for John throughout the 2018/2019 academic year.

3.4.3. Maritime Security Doctoral Fellowship - DHS Career Development 2013 Supplement Award

Alex Pollara successfully defended his doctoral dissertation titled *Characterization of Small Vessels from Acoustical Signatures* in August 2017 to receive his Doctorate in Ocean Engineering with a focus on Maritime Security. He is now employed as a Data Scientist at UBS, where he develops natural language and machine learning models to flag communications for language that suggests illegal or unethical behavior, including the violation of funds being transferred to U.S. sanctioned countries and other nefarious financial activities that negatively impact U.S. financial compliance regulations.

.

3.4.4. DHS Career Development Grant Master's Degree Fellowship – 2012 Award

In Year 4, MSC awarded Luciano Triolo a one-year Fellowship leveraging funds remaining in the Center's 2012 Career Development Grant Award. The Fellowship provided Luciano with the opportunity to conduct research in the area of multispectral imaging of vessel emissions and to complete coursework leading towards his Master degree in Maritime Systems at Stevens Institute of Technology.

In May 2018, Luciano defended his Master thesis titled "*Guidelines for a Remote Multispectral Emissions Monitoring System"* to receive his Master of Science degree in Maritime Systems with a Graduate Certificate in Maritime Security.

His fellowship and research activities during the fall and spring semesters included the following:

- Completed and defended Master thesis. (May 2018)
- Provided research support on MSC research projects related to Maritime Domain Awareness.
- Attended the MSC's Annual Review Meeting in Washington, DC. (Oct. 2017)

Upon graduation from the Maritime Security program, Luciano was hired as an Engineering Associate within the Program Management Division with the Port Authority of New York/New Jersey.

3.4.5. Maritime Systems Master's Degree Fellowship and Assistantship – Alumni Career Placement 2017-2018

In Year 4, Blaise Linn, MSC Research Assistant (2015 – 2017) and Tyler Mackanin former MSC CDG Fellow (2015 – 2017), assumed engineering positions with the Logistics Management Institute (LMI), a Federally Funded Research and Development Center (FFRDC) providing support to the National Urban Security Technology Laboratory (NUSTL) in New York City.

In their positions as Junior Engineers, Blaise and Tyler provide support to NUSTL's Testing and Evaluation Division. They assist with planning, execution, and reporting on various NUSTL tests to include operational field assessments and urban operational experiments. They also draft test plans and protocols, perform data collection and analysis, and prepare draft assessment reports. Since 2016, the Center has placed two other students in positions with the DHS S&T National Lab.

3.5. MSI Engagement - STEM Education Workshop and SRTP Follow-on Funding

Milestone	Performance Metrics	Status / Discussion
1. Minority and women student participation in the Center's annual Summer Research Institute. SRI 2018 – outreach and recruitment (9/1/17 – 2/16/18)	Diversity in the SRI program will reflect a minimum of 50% of students from underrepresented communities. (e.g. minority students, women and MSI enrolled students.)	Incomplete: The demographics for the 2018 SRI included 42% students from underrepresented communities and students from two MSIs.
2. MSI participation in MSC research activities/programs. Summer Research Team program YR 4 (6/4/18 – 8/10/18)	MSC will host a minimum of one MSI SRT team per summer. - Outreach efforts to recruit MSI SRT participation will be measured by the number of targeted email distributions and personal conversations had with MSI representatives.	Incomplete: Although effort was made across the MSC network to recruit MSI SRTP participants, the project proposals received for the program were not in alignment with the Center's current research projects. Complete: Follow-on funding of $50k was successfully applied for and awarded to the Center's 2017 MSI summer re-

		search team from University of Texas-Rio Grande Valley.
3. MSI Workshop	MSC will host a STEM-focused workshop tailored to MSI faculty and educators from underserved communities.	Completed: MSC developed and delivered an Environmental Data Collection and STEM Education workshop on June 8, 2018 in conjunction with Stevens faculty and the USCG Sector NY.

3.5.1. MSI Environmental Data Collection and STEM Education Workshop

Figure 8. Dr. Gregg Vesonder provides instruction on how to build intelligent sensor boards during MSC's Environmental Data Collection and STEM Education Workshop.

MSC developed and delivered a one-day multidisciplinary workshop focused on the impacts of extreme weather events on urban coastal communities and homeland security through the perspective of the U.S. Coast Guard. The workshop aimed to provide methods in which the workshop participants can engage their students in activities to track and report the daily environmental conditions of their communities. The teach-the-teacher event included faculty members from higher education Minority Serving Institutions (MSIs) and educators from underserved communities (K-12) to assist in the development of their STEM-based curriculum efforts.

The agenda for the workshop included the following activities:

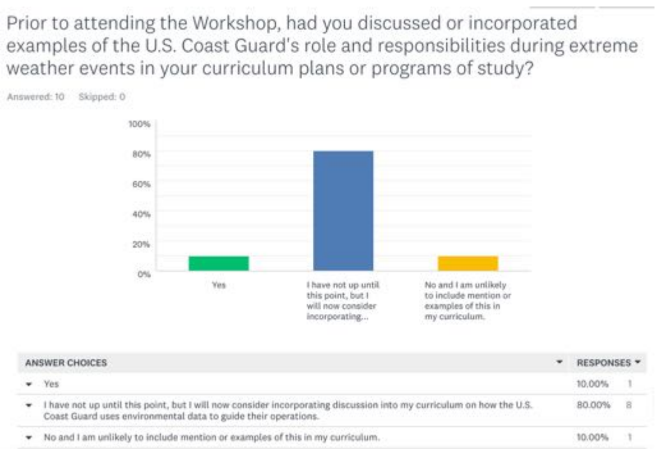
- MSC overview (Beth Austin-DeFares, MSC)
- Extreme Weather Events in the NYC Metro Area and the Case with Hurricane Sandy (Dr. Philip Orton, Research Associate Professor, Stevens Institute)
- U.S. Coast Guard Perspective – Discussion on the USCG's Hurricane and Severe Weather Plan in the Port of NY/NJ (Mr. John Hillin, Division Chief, Safety and Security, USCG Sector NY)
- Using Extreme Weather and Disasters as Scenarios for Teaching Science – Roundtable Discussion

- Overview of Curriculum and Classroom Activities Centered Around Coastal/Urban Disasters and Climate (Dr. Philip Orton with support by Dr. Brian Vant-Hull, Research Scientist, City College of New York)
- Citizen Science, Sensors and Coding (Dr. Gregg Vesonder, Program Director, Software Engineering and Director, Altorfer Design Studio Lab Stevens Institute)
- Getting Comfortable with the Raspberry Pi, the Sensors and the Circuit Board
    - Basic Principles on Coding and Wiring
    - Connecting the Environmental Sensors – Data and More Data
    - Data Exploration
- Citizen Science - Building your Own Curriculum
- Group Discussion

Takeaways from the workshop included curriculum materials, intelligent sensors boards and a discussion on opportunities to engage in ongoing and future research projects with Stevens Institute of Technology. A repository of the workshop curriculum materials has been made available to the workshop participants via a dedicated Google Drive folder.

Twelve educators from the following institutions attended the one-day MSC event: Center for Innovation in Engineering and Science Education, City University of New York, New Jersey City University, New York City College of Technology, Norfolk State University, and from the Paterson and Toms River, NJ school districts.

To assess the effectiveness of the workshop in providing relevant and useable curriculum materials and to determine the likelihood in which the participants would now consider the perspective of U.S. Coast Guard in their lesson plans, the MSC prepared and disseminated a post-program survey. Results of the survey showed that while a majority of the workshop participants (80%) had not previously discussed how the Coast Guard uses environmental data in their classrooms, they would now consider incorporating Coast Guard examples into their lesson plans. Figure 9 below shows the question and responses by ten of the twelve workshop participants.


Prior to attending the Workshop, had you discussed or incorporated examples of the U.S. Coast Guard's role and responsibilities during extreme weather events in your curriculum plans or programs of study?

Answered: 10 Skipped: 0

100%
80%
60%
40%
20%
0%
Yes
I have not up until this point, but I will now consider incorporating...
No and I am unlikely to include mention or examples of this in my curriculum.

ANSWER CHOICES	RESPONSES	
Yes	10.00%	1
I have not up until this point, but I will now consider incorporating discussion into my curriculum on how the U.S. Coast Guard uses environmental data to guide their operations.	80.00%	8
No and I am unlikely to include mention or examples of this in my curriculum.	10.00%	1

Figure 9. MSC workshop inspired MSI STEM educators to incorporate USCG examples into their class activities.

Overall, a majority of the survey respondents rated the workshop excellent in the following areas:

- Quality of Workshop Curriculum (60%)
- Quality of Instruction (60%)
- Quality of Facilities (70%)
- Quality of Program Coordination/Administration (90%)

The top takeaways from the workshop included:

- Discussions and Networking (90%)
- Sensor Board Materials (80%)
- Inclusion of the U.S. Coast Guard (60%)
- Curriculum Materials (60%)

Please see Appendix E-2 for copy of the survey instrument.

3.5.2. MSI Summer Research Team Program

During the fall of 2017, the Center pursued its academic network to identify an MSI partner to collaborate with in the DHS MSI Summer Research Team Program (SRTP). The Center's goal was to recruit an MSI faculty and student team from a community college within the local NYC metropolitan area to conduct work in a mutual area of interest, however, the MSC was not able to identify a team in time for the MSI SRTP program deadline.

The Center did however receive two project proposals from Dillard University and Northern New Mexico College, but upon assessment by MSC administrators, the faculty research interests were not in align with the Center's research projects and the Center did not feel as though it had the appropriate faculty resources to adequately support either of the team's desired projects.

During Year 4 however, Dr. Alley Butler, Professor Manufacturing and Industrial Engineering at the University of Texas Rio Grande Valley (UTRGV) was awarded follow-on funding through the MSI SRTP program to continue research he and his team conducted during their 2017 summer research program with the MSC. During their twelve-week stay at the Center, the team assessed the use of Virtual Reality (VR) to enhance maritime domain awareness and the response capabilities of homeland security practitioners. The team completed a comprehensive literature review and collaborated with Stevens Institute of Technology faculty and MSC students to create VR environments leveraging imaging sonar data collected from a Remotely Operated Vehicle (ROV). The award will assist Dr. Butler and his team which now includes Dr. Emmett Tomai at UTRGV and Dr. Brendan Englot at Stevens to advance work to develop machine automated feature recognition capabilities in VR environments.

4. Other Related Activities

This section describes additional activities related to MSC that occurred during the reporting period. These include the Center's activities for soliciting projects, stakeholder engagement, communications and outreach, management, and guidelines and policies.

4.1. Project Solicitation

In August 2017, the MSC announced a Request for Proposals for Maritime Security Research. The RFP solicited projects that addressed IPT gaps and FOA research questions, and that corresponded to one or more of the following research theme areas:

- Theme Area 1: Maritime Risk, Threat Analysis, and Resilience
- Theme Area 2: Maritime Domain Awareness (MDA) Research
- Theme Area 3: Maritime Technology Research
- Theme Area 4: Integration of Science and Engineering with Maritime Security Governance and Policy Research

MSC leveraged the OUP and COE networks, as well as its own academic and industry contact list to distribute the RFP announcement as broadly as possible. Eligibility requirements stated that only proposals from accredited U.S. colleges and universities, for-profit organizations and organizations that met the definition of non-profit.

MSC planned to fund at least one award for 12 months, up to $300,000 per award. The anticipated performance period for the award was January 1, 2018 through December 31, 2018.

Collectively, the RFP solicitation resulted in the receipt of 16 high-quality submissions. Covering a broad range of topics, from Unattended Remote Sensing Applications to Piracy and Maritime Crime to Predictive Port Resilience Tools, the proposals addressed research themes and questions posed in the RFP. Each proposal underwent a two-part review, to include a Scientific Merit Review conducted by independent peer reviewers (a total of 32 reviewers) and then a comprehensive assessment by the DHS Office of University Programs for Mission Relevancy.

Following an extensive review that concluded in April 2018, the following two proposals were selected for funding by the DHS pending receipt and approval of their project workplans:

1. *Predictive Port Resilience Tool to Assess Regional Impact of Hurricanes,*
   Dr. Manhar Dhanak Florida Atlantic University (FAU)
   Project Champion: LCDR Rachel Stryker, CG-FAC-1

Abstract: The principal objective of this research is to develop a predictive resiliency-planning tool for ports that enhances regional community resiliency from hurricane events. This research seeks to expand understanding of port resiliency and enhance the knowledge in the development of a stakeholder-focused tool to improve regional resilience. Through use of knowledge, innovation, and education, as well as assessment of consequences of hurricane events, we seek to support and improve the regional preparedness of interconnected ports systems. Considerations will include network and inter-dependence of ports in a region. Fundamentally, ports cluster areas of the country, with multiple ports servicing the same region. Although these regions may be composed of separate local governmental jurisdictions, port clusters often share common historical, environmental, and topographic systems. Because of transportation linkages that connect the movement of people and freight, they also share close economic ties. These shared cultural and transportation ties also mean that they also often share similar hazards and threats. US ports and container/intermodal terminals are critical links in the marine transportation system. Disruption at series of ports can have crippling economic effect in the coastal zone as well as the rest of the nation. Ports are vulnerable to natural disasters since they are fixed, publicly accessible entities. Port stakeholders have a vested interest in the long-term function and viability of ports, but no standardized measures for performance or resilience exist for regional ports. An approach to measuring resilience must be adaptable to the specific needs of the community using it, which quickly renders a national-scale resilience metric nearly impossible. Driven by global economic forces, ports have unique needs that should inform indicators to assess resilience over time. Quantitative methods and tools, stemming from engineering science and vulnerability studies, provide quick assessments of "resilience" at broad spatial scales, but do not dip below the surface into local scale, place-based, community resilience. Qualitative methods, on the other hand, help answer research questions that cannot be addressed with numerical data and dive into questions of attitude, perception, and social interaction.

Given the nature of resilience as a dynamic process, we study and consider strategies for managing identified risk. We address and study how risks affect resilience in a network of ports/container terminals in the region and our approach will bridge the gap between developing tools to assess resilience and understanding the process of resilience at the ports and the intermodal facilities in the region.

2. *Social Media Analytics Research and Training for the US Coast Guard*,
   Dr. David S. Ebert, Purdue University
   Project Champion: Captain Howard Wright, USCG

Project Abstract: Several groups within the USCG utilized the Social Media Analytics and Reporting Toolkit (SMART) pilot software, developed at the VACCINE DHS COE, to harness crowdsourced information for improved on-the-ground situation awareness during the four 2017 hurricanes that impacted the U.S. Although the USCG gave initial positive feedback about the use of SMART, the software deployment to the dozen or so users at the USCG was ad hoc and without systematic training. The ad hoc deployment resulted in uncertainty whether each USCG user has a full understanding of the capabilities of social media analytics. Moreover, there was a lack of a feedback loop of how SMART is being used by a broad spectrum of USCG users. As a result, it is first unclear how (or if) increased social media analytics can lead to improved safety outcomes during a natural disaster and other emergency events. Second, the experiential knowledge gained during the use of social media analytics is not currently reintegrated into the training of future USCG end users.

Our research project will increase the understanding of information and intelligence integration within maritime operations, with a focus on advancements in technologies and command and control systems that utilize crowdsourced information. To accomplish this goal, we will first research the use of social media analytics by the USCG during the 2017 hurricanes through structured interviews, targeted questionnaires, and situation awareness measurement techniques. The user studies will be conducted with our extensive network of partners at the USCG. Second, we will use stakeholder feedback to develop and distribute online and physical training material for the USCG and FEMA in social media analytics. The training will utilize the infrastructure of the FEMA National Training and Education System to integrate social media analytics into national Emergency Management Higher Education Programs. Third, the findings from this research proposal will support the broader dissemination and use of the SMART software, which is currently supported and under development for the DHS S&T First Responder Group.

The scope of this project was later reduced to eliminate areas that were being addressed in other projects.

4.2. Stakeholder Engagement, Communications, and Outreach

MSC continued to engage visitors and partners from various key stakeholder organizations in a range of activities (e.g., Meetings, COE Summit, trainings and exercises). MSC personnel participated in various activities and has partnered with the USCG RDC, USCG Sector NY, DHS S&T Borders and Maritime Division, Customs and Border Protection, National Urban Security Technology Lab, the Office of Intelligence and Analysis, and others as described below.

USCG RDC

USCG RDC representatives were consulted on the development of an Unmanned Aerial System (UAS) project for the 2018 Summer Research Institute. In addition, RDC served as a trusted partner for discussing various Center projects (both existing and proposed) and their relevance to the Coast Guard. MSC supported the USCG in their CUAS testing activities and held various meetings with RDC personnel at Stevens, NUSTL, and RDC to discuss their test plans and participated in their field testing activities. In addition, MSC offered technical assistance to RDC personnel related to their systems of interest.

USCG Sector New York

Mr. John Hillin, Division Chief Safety and Security, USCG Sector New York, participated in the development and delivery of the MSC Environmental Data Collection and STEM Education Workshop. During the one-day venue, Mr. Hillin provided a lecture on the U.S. Coast Guard’s use of weather forecasts and oceanic data to guide the agency’s operations and provided case study information which can be utilized and incorporated into the workshop participants class room activities and lesson plans. Throughout Year 4, MSC’s Director of Education continued to serve as a co-Chair for the Sector NY Area Maritime Security Committee – Cybersecurity Subcommittee and provided feedback on the organizations Cyber Annex.

S&T Borders and Maritime Division

MSC PI and other researchers met with the Director of the S&T Borders and Maritime Division to solicit input from their interactions with the DHS components (USCG, CBP, and ICE) on their operational needs. These discussions include the IPT gaps, existing projects, as well as potential new projects that can quickly fill in gaps that need to be addressed. MSC research PIs had multiple interactions with S&T’s BMD Director as well as with Program Managers (Marilyn Rudzinsky and Shawn MacDonald) to discuss port resilience and maritime surveillance areas of interest to BMD, CBP, and USCG.

NUSTL

In 2017, the Center successfully placed two of its Center- supported students in Junior Engineering positions with the Logistics Management Institute (LMI), a Federally Funded Research and Development Center (FFRDC) providing support to the National Urban Security Technology Laboratory (NUSTL) in New York City. The students work within

NUSTL's Testing and Evaluation Division. They assist with planning, execution, and reporting on various NUSTL tests to include operational field assessments and urban operational experiments. This brings to a total four students that the MSC has placed at NUSTL over a two-year period.

NUSTL also facilitated a comprehensive field-visit and briefing to the Center's summer research students during the 2018 Summer Research Institute. In addition, NUSTL served as a Center partner engaging in numerous activities and conversations with the MSC regarding areas of mutual interest.

In addition, MSC PI participated in multiple meetings with NUSTL to discuss CUAS needs for the Coast Guard and other DHS stakeholders and assist them in formulating their test plans and reviewing requirements.

CBP

CBP's Office of Field Operations at the Port of NY/NJ hosted MSC students and faculty mentors from the 2018 Summer Research Institute for a tour of the agency's cargo scanning equipment and operational facilities. This trip marked the Center's seventh annual visit to CBP over the course of the summer research program.

MSC PIs also participated in meetings with CBP representatives to discuss their needs for port agricultural security and for using VTS radars to detect small vessels. In addition, assistance was provided on the capabilities and limitations of radar for maritime situation awareness.

PANYNJ

MSC fellowship student Luciano Triolo was hired by the Port Authority of New York/New Jersey (PANYNJ) as an Engineering Associate in the Program Management Division.

MSC and Stevens students participated in a full-scale emergency response exercise held at the George Washington Bridge. The exercise simulated an oil tanker explosion and was designed to test the bridge's emergency plan for mutual aid response, enabling bridge personnel and local emergency response organizations to train together and validate response procedures. The exercise included members of the Port Authority Police Department and Port Authority operations staff along with federal, state, and local emergency response partners.

The PANYNJ also facilitated a tour of the agency's ferry terminals and security operations as part of the MSC's 2018 Summer Research Institute.

Other Activities

In addition to the above activities, MSC conducted many targeted communications efforts. This included participation in the following events:

- MSC Annual Meeting – The MSC held its 3rd annual review meeting on October 10, 2017 at the U.S. Coast Guard Headquarters in Washington, DC. Stakeholders from the U.S. Coast Guard, Customs and Border Protection and DHS S&T Borders and Maritime Security Division joined MSC research investigators and DHS Office of University Programs administrators for a one-day meeting to review the Center's research projects and discuss strategies for transitioning the Center's work into operational environments.

  The meeting included an overview of the Center's project portfolio and operational activities by MSC's Director, and research and education project presentations related to the Center's work in the areas of Port Resiliency Planning and Assessment *(Florida Atlantic University)*, Maritime Cybersecurity *(American Bureau of Shipping)*, and Maritime Security Education and Professional Development programs *(MSC and Louisiana State University)*. The meeting also included presentations by MSC students who discussed their respective research in Underwater Robotics and Autonomous Navigation and AIS Fraud Detection.

- COE Summit, where all Centers of Excellence and representatives from DHS OUP, S&T Divisions, Customs and Border Protection, USCG, Immigration and Customs Enforcement, FEMA, and other stakeholders participated – Arlington, VA. On May 30-31, MSC administrators, researchers and students participated in the DHS S&T Centers of Excellence (COE) Summit held at George Mason University in Arlington, VA. The event brought together representatives from across the public and private homeland security enterprise with researchers and students to discuss technologies and new approaches to address security concerns. The Summit featured an Innovation Showcase where each of the COE's presented their respective knowledge products, tools and technologies, and a Student Poster Showcase that highlighted the talent and breadth of student research being conducted across the COE university network.

  The MSC Director served as a panelist on the Cross-Border Movement of People, Goods, Data and Capital panel. The Director of Education chaired the Student Activities and Poster Committee and three MSC funded graduate students presented their research as part of the poster showcase.

  During the Summit, MSC administrators met with representatives from the following organizations:

  DHS S&T divisions, component agencies and affiliate federal partners:

  - CBP, FEMA, ICE, National Geospatial Intelligence Agency, NPPD, Texas Department of Public Safety, Combating Terrorism Technical Support Office

  International Homeland Security partners:

  - Defence Research and Development Canada and Swedish Defence Research Agency

Commercial/private sector:

- Smiths Detection, ABS Group, Draper, Assett, Van Cleve & Associates

Academia and COE partners:

- Georgia Tech, Carnegie Mellon, CINA, CEEZAD

The Center also generated and distributed a quarterly newsletter distributed to the Center's contact database of over 700 stakeholders and other contacts. The newsletter contains relevant information regarding the Center's research, stakeholder engagements and student achievements. An archive of MSC's newsletters can be found on the Center's website at: https://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/center-newsletters.

4.3. Management Activities

The main COE management activities not discussed earlier in this report are summarized in this section. The Center Director worked with the COE's Principal Investigators (PIs) to develop project work plans and discussed project content that will benefit DHS and its stakeholders. The Director also worked closely with the DHS Program Manager and spoke with him on a weekly basis to understand DHS expectations from the Center and bring up any issues of concern and to adjust operations based on additional OUP COE requirements. Based on these discussions and meetings, the Director held frequent meetings with individual PIs as well as coordinated conference call meetings with the Center's PIs as needed. The purpose of these meetings was to ensure that the individual projects are progressing according to the work plans and continue to be aligned with DHS OUP's expectations.

Members the Center Science and Education Advisory Committee (SEAC) have been engaged periodically throughout the year and were kept informed of the Center activities through phone conversations, annual meeting, and Center email communications. In addition, they were invited to Center activities including the annual meeting (for which, two members of the Board attended) and to the Summer Research Institute.

In addition to the above activities, the Center Director continued to reach out to many DHS stakeholders at various levels and in different capacities to discuss their projects and how the Center can be a resource to them. These meetings included discussions with representatives from NUSTL and USCG RDC regarding research in the area of counter-UAS systems, such as developing requirements, testing, and quantifying their performance. The Director also discussed transition ideas with the USCG RDC and CBP Air and Marine personnel to understand their needs and their limitations in preparation for transitioning projects when they are ready. In particular, many discussions were held with CBP's Air and Marine Office and with the USCG RDC regarding current radars used in VTS applications and the steps needed to implement additional signal processing for detecting small vessels and eventually transition this capability to the field on already deployed radar systems.

As part of its transition efforts, the MSC management has continued to conduct project evaluations and tracking of post-project developments. Discussions and meetings were conducted with Mr. Jon McEntee, Mr. Shawn MacDonald, Ms. Marilyn Rudzinsky, and Mr. Doug Maughan on the Year 4 projects. MSC also connected with local Area Maritime Security Committees, including a Maritime Cyber Awareness webinar series that was delivered to AMSC members nationwide, and the Center's on-going collaboration with the Sector NY AMSC and their cybersecurity awareness initiatives.

MSC management conducted scientific discussions with various stakeholders. Discussions on VTS radar capabilities were conducted with CAPT Evans from RDC, on cyber research with Mr. Maughan from DHS S&T Cyber Division, and Mr. Steve Tucker from USCG HQ. As a result, we were invited to write a paper on the detection of illegal fishing activities that was published in the Spring 2018 USCG Proceedings. We also engaged a broad range of academic and private industry professionals to assess and review RFP project proposals for a comprehensive Scientific Merit Review.

In addition, MSC management formed new partnerships with ICE, DHS Intelligence and Analysis Directorate, and National Maritime Security Advisory Committee (NMSAC). With ICE, many discussions were conducted regarding the use of multiple sensors to protect the US Virgin Islands and Puerto Rico against illegal smuggling of humans and illicit material. With DHS I&A, we had a couple of meetings and are currently working with them to hold a symposium at Stevens that will host many of MSC stakeholders. Finally, MSC's Director was appointed by the DHS Secretary to serve on the NMSAC and will be using this opportunity to meet additional MSC stakeholders and better understand the USCG's emerging priority mission gaps.

To support these efforts, MSC's management travel budget was used to attend the stakeholder meetings described above, participate in the annual review meeting at the USCG HQ in Washington, DC, and participate at the COE Summit that was held in May 2018 at the George Mason University.

4.4. Center Guidelines and Policies

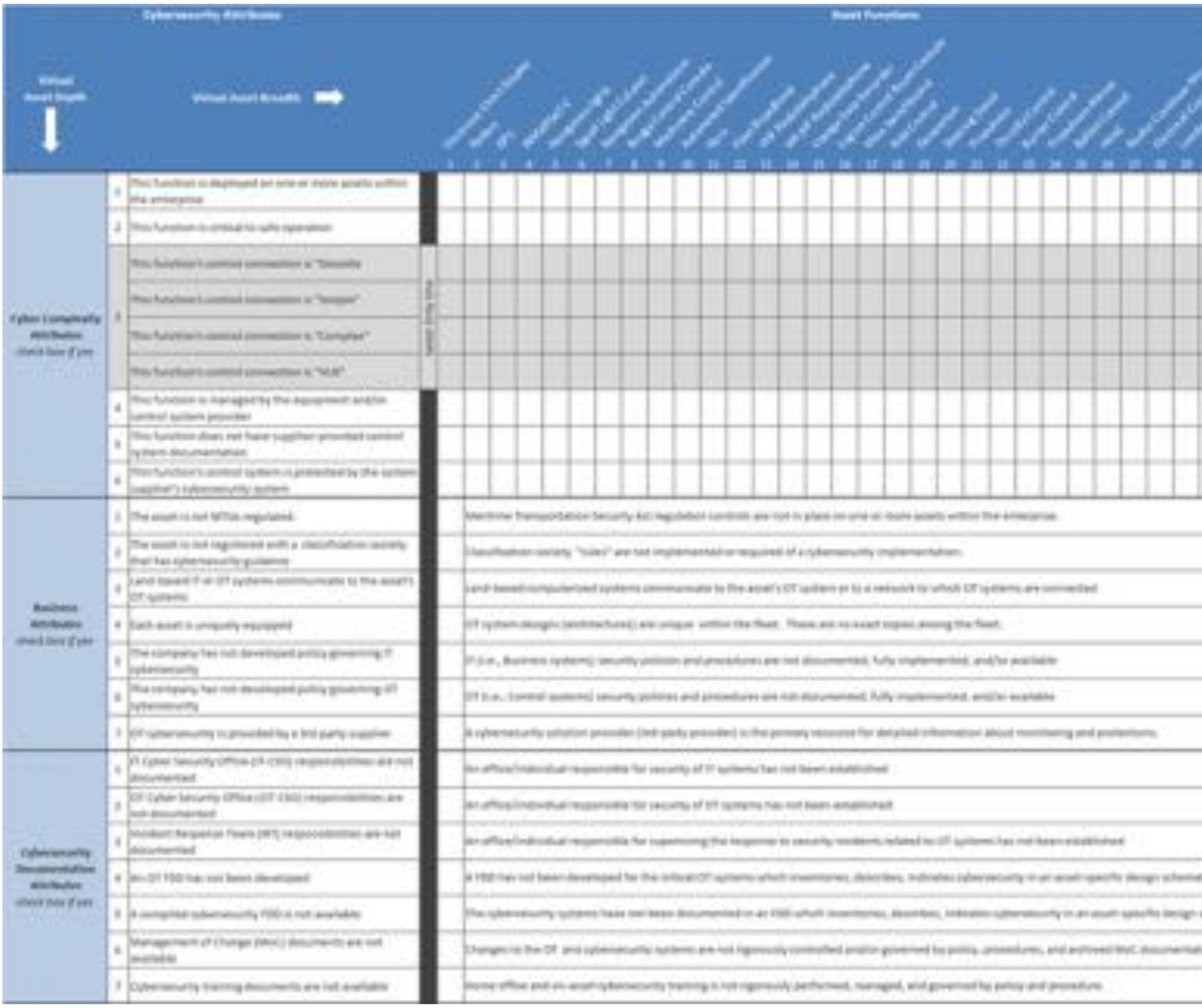
During Year 1, MSC administrators created a document for the Center's academic partners and research PIs containing general orientation information (e.g. partner contact information, reporting requirements, and DHS acknowledgement and disclaimer statements), and copies of the Center's policy and security requirements for handling sensitive material, as well as student safety and security guidelines. The MSC General Information and Guidelines for Academic Partners document was updated in Year 4 and shared with each of the MSC partner schools, with the requirement that they acknowledge receipt and confirm that they have reviewed and understand the policy and security requirements for handling sensitive material and the student safety and security guidelines.

5. Budget

The budget breakdown was provided separately as part of the Stevens financial reporting requirements.

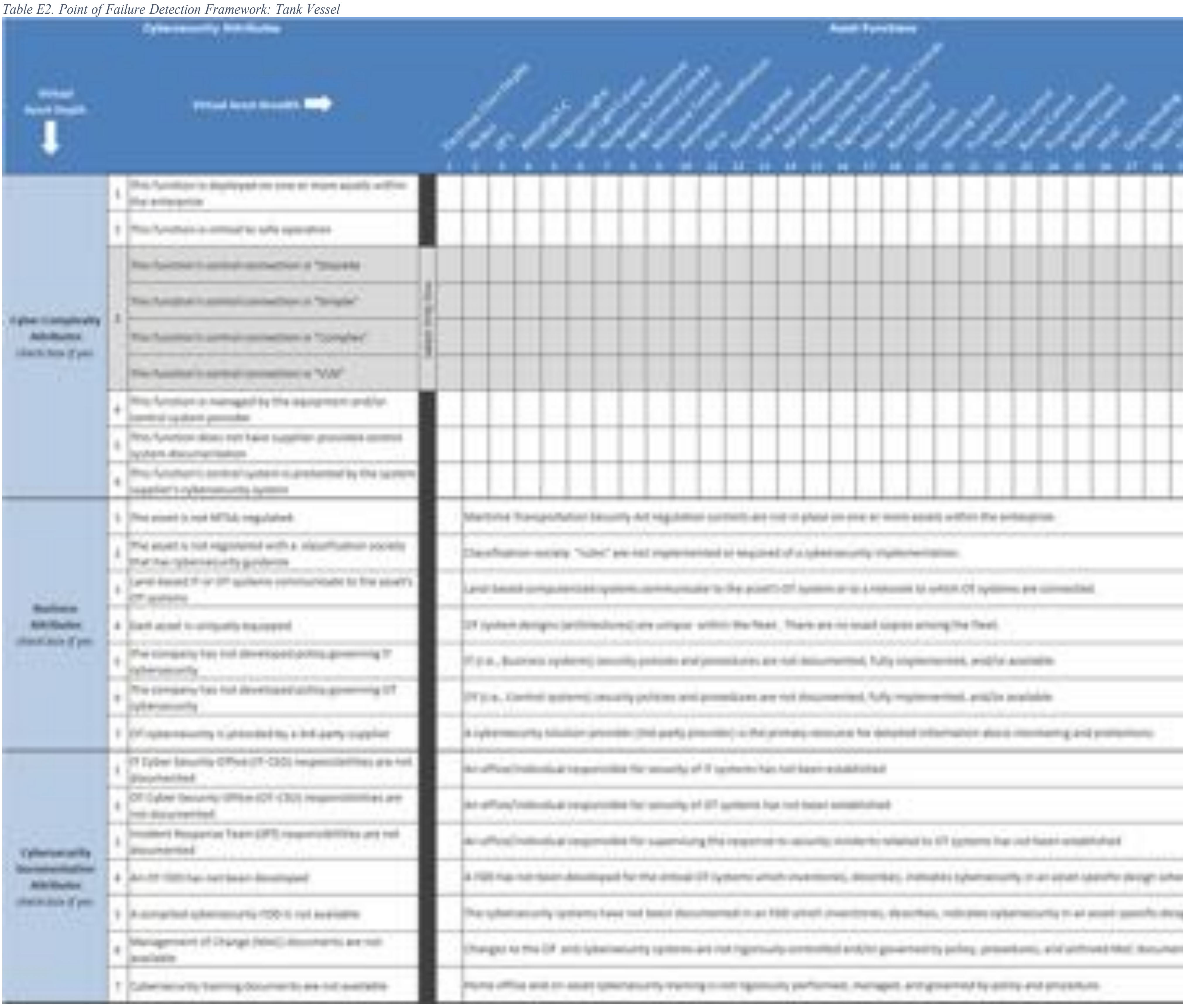
Appendix C-1. Point of Failure Detection Worksheets

The following figures provide sample worksheets for high consequence asset classes. The asset functions listed across the top of the worksheet are based on systems commonly deployed on the assets.



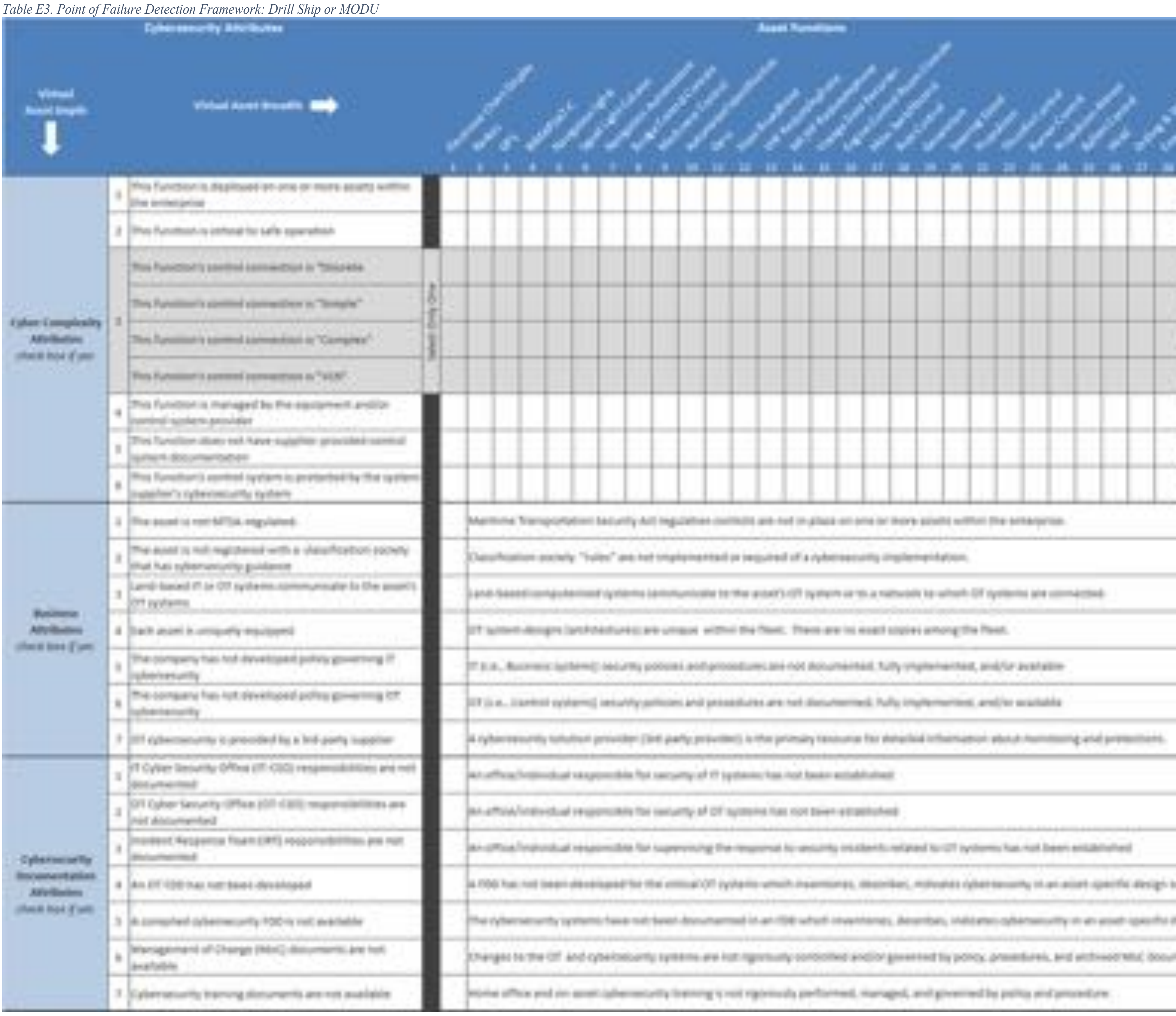
	Cybersecurity Attributes			Asset Functions																												
Virtual Asset Depth		Virtual Asset Breadth		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Cyber Complexity Attributes *check box if yes*	1	This function is deployed on one or more assets within the enterprise																														
	2	This function is critical to safe operation																														
	3	This function's control connection is "Discrete"	Select Only One																													
		This function's control connection is "Simple"																														
		This function's control connection is "Complex"																														
		This function's control connection is "HUB"																														
	4	This function is managed by the equipment and/or control system provider																														
	5	This function does not have supplier provided control system documentation																														
	6	This function's control system is protected by the system supplier's cybersecurity system																														
Business Attributes *check box if yes*	1	The asset is not MTSA regulated.		Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.																												
	2	The asset is not registered with a classification society that has cybersecurity guidance		Classification society "rules" are not implemented or required of a cybersecurity implementation.																												
	3	Land based IT or OT systems communicate to the asset's OT systems		Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected																												
	4	Each asset is uniquely equipped		OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.																												
	5	The company has not developed policy governing IT cybersecurity		IT (i.e., business systems) security policies and procedures are not documented, fully implemented, and/or available																												
	6	The company has not developed policy governing OT cybersecurity		OT (i.e., control systems) security policies and procedures are not documented, fully implemented, and/or available																												
	7	OT cybersecurity is provided by a 3rd party supplier		A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protections.																												
Cybersecurity Documentation Attributes *check box if yes*	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented		An office/individual responsible for security of IT systems has not been established																												
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented		An office/individual responsible for security of OT systems has not been established																												
	3	Incident Response Team (IRT) responsibilities are not documented		An office/individual responsible for supervising the response to security incidents related to OT systems has not been established																												
	4	An OT FSD has not been developed		A FSD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific design schemat																												
	5	A compiled cybersecurity FSD is not available		The cybersecurity systems have not been documented in an FSD which inventories, describes, indicates cybersecurity in an asset specific design																												
	6	Management of Change (MoC) documents are not available		Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC documentat																												
	7	Cybersecurity training documents are not available		Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.																												

Table E2. Point of Failure Detection Framework: Tank Vessel



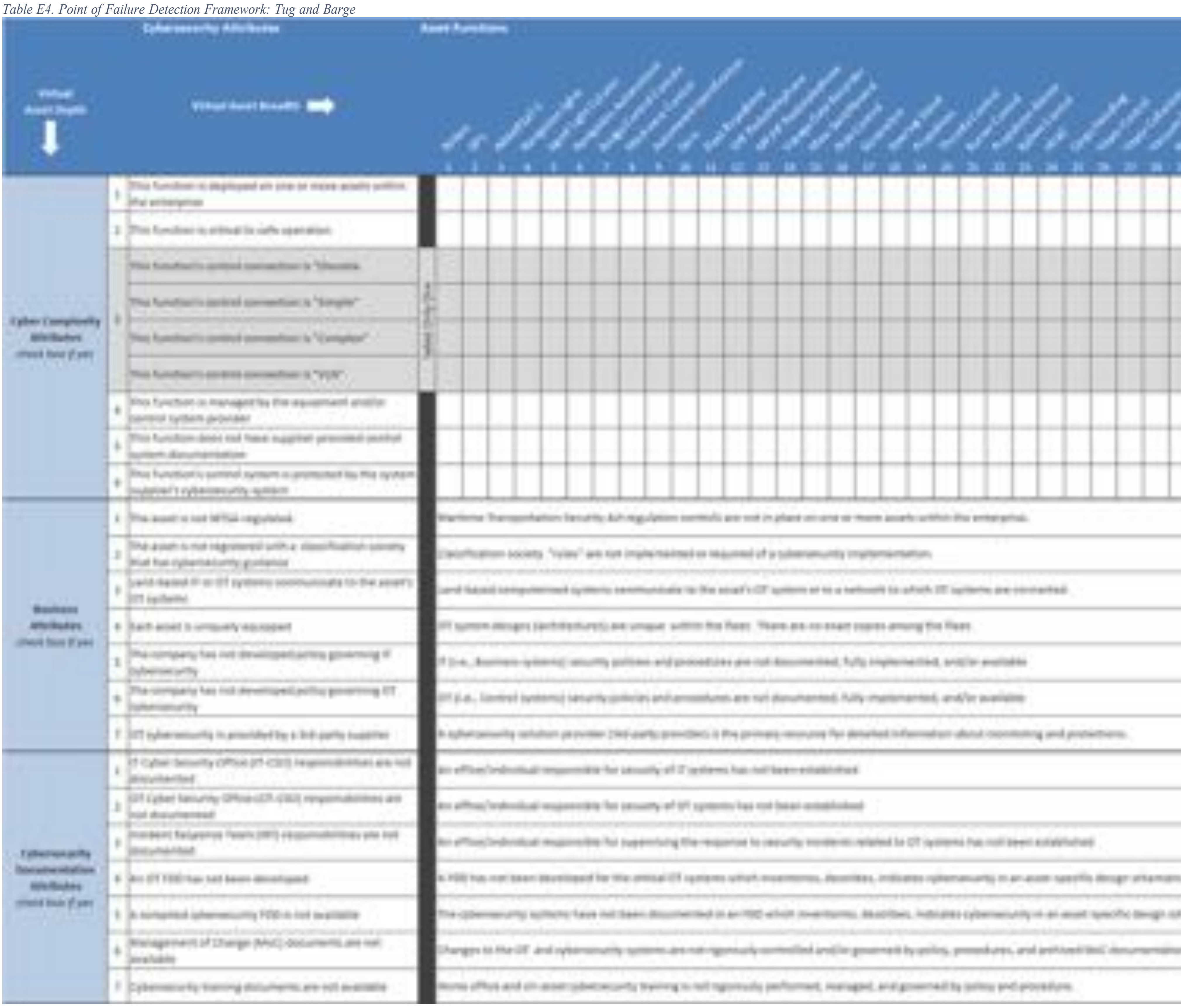
Cybersecurity Attributes			Asset Functions
Virtual Asset Depth		Virtual Asset Breadth	[illegible]
Cyber Complexity Attributes check box if yes	1	This function is deployed on one or more assets within the enterprise	
	2	This function is critical to safe operation	
	3	This function's control connection is "Discrete"	
		This function's control connection is "Simple"	
		This function's control connection is "Complex"	
		This function's control connection is "V.IN"	
	4	This function is managed by the equipment and/or control system provider	
	5	This function does not have supplier provided control system documentation	
	6	This function's control system is protected by the system supplier's cybersecurity system	
Business Attributes check box if yes	1	The asset is not MTSA regulated	Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.
	2	The asset is not registered with a classification society that has cybersecurity guidance	Classification society "rules" are not implemented or required of a cybersecurity implementation.
	3	Land-based IT or OT systems communicate to the asset's OT systems	Land based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.
	4	Each asset is uniquely equipped	OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.
	5	The company has not developed policy governing IT cybersecurity	IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available.
	6	The company has not developed policy governing OT cybersecurity	OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available.
	7	OT cybersecurity is provided by a 3rd-party supplier	A cybersecurity solution provider (3rd party provider) is the primary resource for detailed information about monitoring and protections.
Cybersecurity Documentation Attributes check box if yes	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented	An office/individual responsible for security of IT systems has not been established
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented	An office/individual responsible for security of OT systems has not been established
	3	Incident Response Team (IRT) responsibilities are not documented	An office/individual responsible for supervising the response to security incidents related to OT systems has not been established
	4	An OT FDD has not been developed	A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific design sche
	5	A compiled cybersecurity FDD is not available	The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset specific desig
	6	Management of Change (MoC) documents are not available	Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC documen
	7	Cybersecurity training documents are not available	Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedures.

Table E3. Point of Failure Detection Framework: Drill Ship or MODU



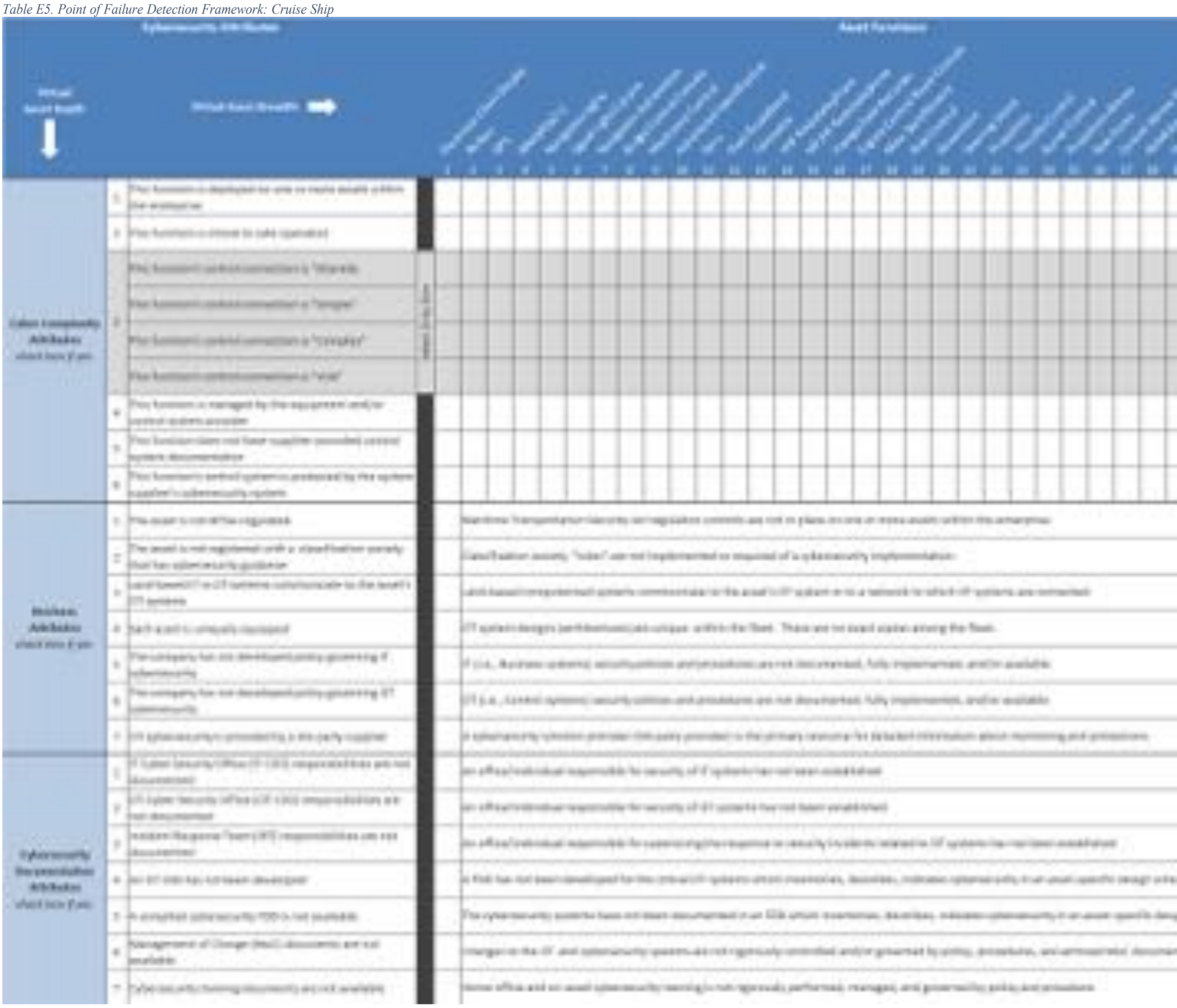
Cybersecurity Attributes				Asset Functions																											
Virtual Asset Depth ⇩		Virtual Asset Breadth ⇨		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Cyber Complexity Attributes (check box if yes)	1	This Function is deployed on one or more assets within the enterprise																													
	2	This Function is critical to safe operation																													
	3	This Function's control connection is "Discrete"	Select Only One																												
		This Function's control connection is "Simple"																													
		This Function's control connection is "Complex"																													
		This Function's control connection is "VLN"																													
	4	This Function is managed by the equipment and/or control system provider																													
	5	This Function does not have supplier provided control system documentation																													
	6	This Function's control system is protected by the system supplier's cybersecurity system																													
Business Attributes (check box if yes)	1	The asset is not MTSA regulated		Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.																											
	2	The asset is not registered with a classification society that has cybersecurity guidance		Classification society "rules" are not implemented or required of a cybersecurity implementation.																											
	3	Land-based IT or OT systems communicate to the asset's OT systems		Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.																											
	4	Each asset is uniquely equipped		OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.																											
	5	The company has not developed policy governing IT cybersecurity		IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available																											
	6	The company has not developed policy governing OT cybersecurity		OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available																											
	7	OT cybersecurity is provided by a 3rd-party supplier		A cybersecurity solution provider (3rd party provider) is the primary resource for detailed information about monitoring and protections.																											
Cybersecurity Documentation Attributes (check box if yes)	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented		An office/individual responsible for security of IT systems has not been established																											
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented		An office/individual responsible for security of OT systems has not been established																											
	3	Incident Response Team (IRT) responsibilities are not documented		An office/individual responsible for supervising the response to security incidents related to OT systems has not been established																											
	4	An OT FDD has not been developed		A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific design s																											
	5	A compiled cybersecurity FDD is not available		The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset specific d																											
	6	Management of Change (MoC) documents are not available		Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC docu																											
	7	Cybersecurity training documents are not available		Home office and on asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.																											

Table E4. Point of Failure Detection Framework: Tug and Barge



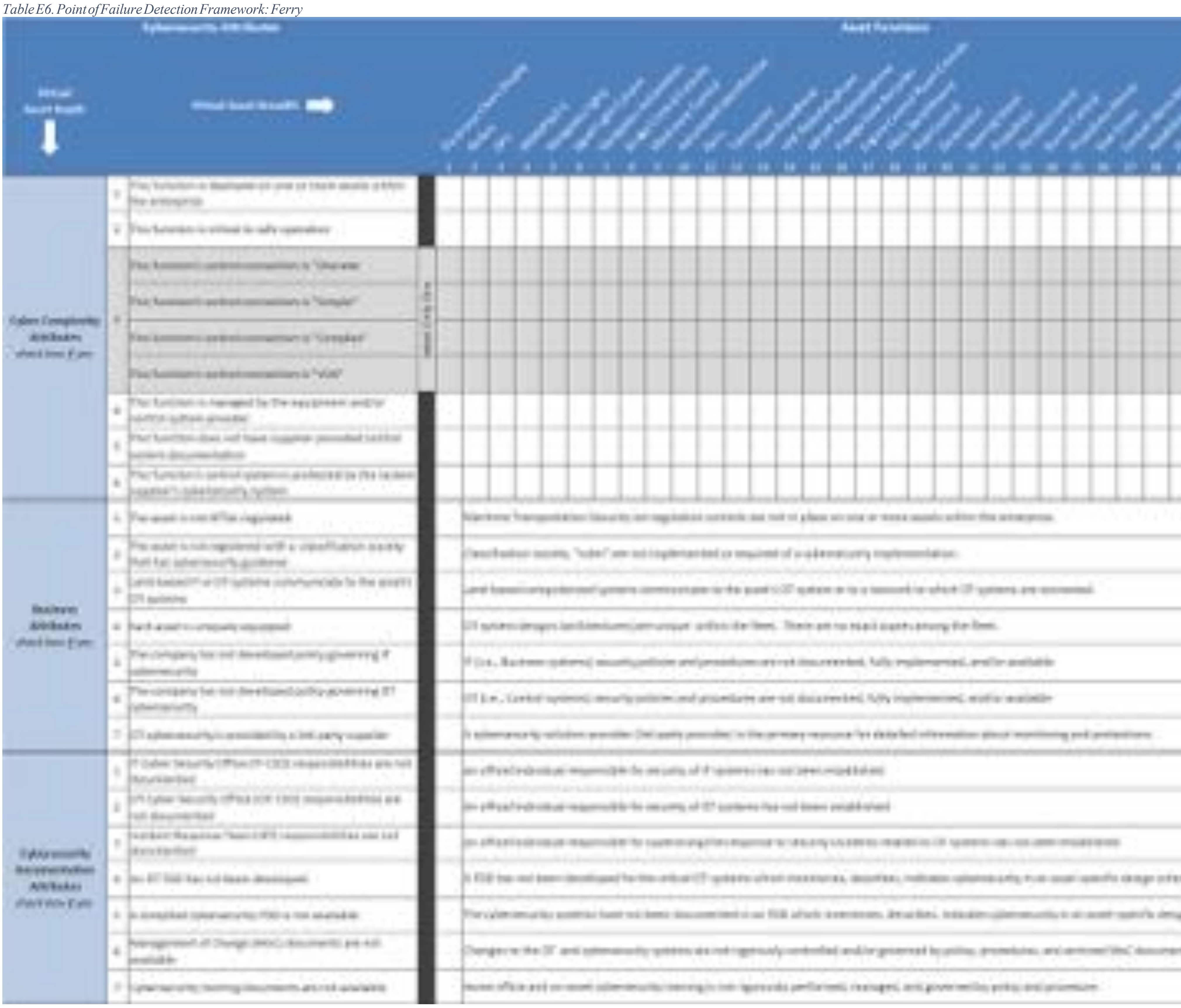
Virtual Asset Depth		Cybersecurity Attributes Virtual Asset Breadth	Asset Functions 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Cyber Complexity Attributes (check box if yes)	1	This function is deployed on one or more assets within the enterprise	
	2	This function is critical to safe operation	
	3	This function's control connection is "Discrete" This function's control connection is "Simple" This function's control connection is "Complex" This function's control connection is "VLN" Select Only One	
	4	This function is managed by the equipment and/or control system provider	
	5	This function does not have supplier provided control system documentation	
	6	This function's control system is protected by the system supplier's cybersecurity system	
Business Attributes (check box if yes)	1	The asset is not MTSA regulated	Maritime Transportation Security Act regulation control(s) are not in place on one or more assets within the enterprise.
	2	The asset is not registered with a classification society that has cybersecurity guidance	Classification society "rules" are not implemented or required of a cybersecurity implementation.
	3	Land-based IT or OT systems communicate to the asset's OT systems	Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.
	4	Each asset is uniquely equipped	OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.
	5	The company has not developed policy governing IT cybersecurity	IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available
	6	The company has not developed policy governing OT cybersecurity	OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available
	7	OT cybersecurity is provided by a 3rd-party supplier	A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protections.
Cybersecurity Documentation Attributes (check box if yes)	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented	An office/individual responsible for security of IT systems has not been established
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented	An office/individual responsible for security of OT systems has not been established
	3	Incident Response Team (IRT) responsibilities are not documented	An office/individual responsible for supervising the response to security incidents related to OT systems has not been established
	4	An OT FDD has not been developed	A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific design alternative
	5	A completed cybersecurity FDD is not available	The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset specific design alt
	6	Management of Change (MoC) documents are not available	Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC documentation
	7	Cybersecurity training documents are not available	Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.

Table E5. Point of Failure Detection Framework: Cruise Ship



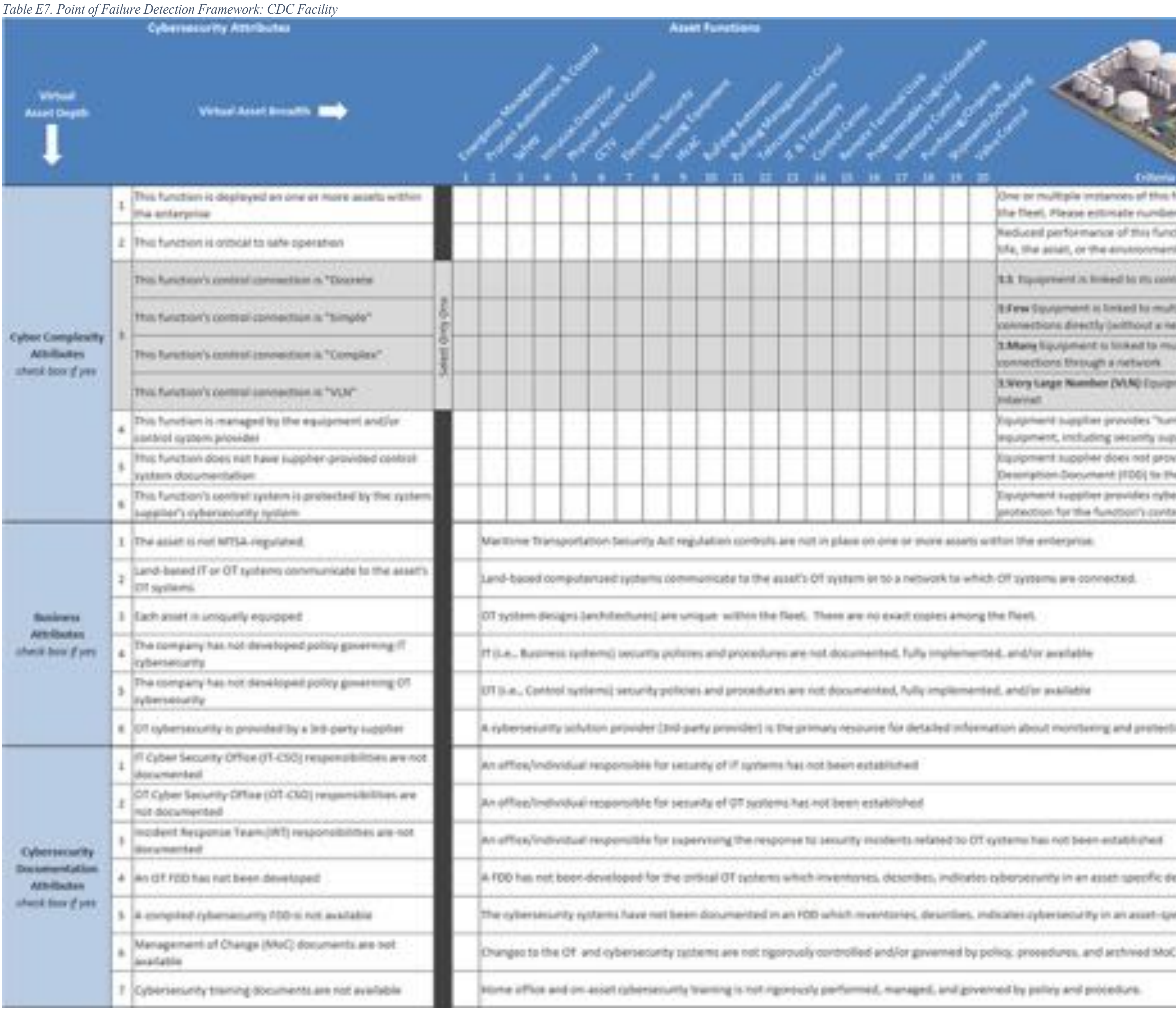
Virtual Asset Depth ↓		Cybersecurity Attributes Virtual Asset Breadth ➡	Asset Functions
Cyber Complexity Attributes check box if yes	1	This function is deployed on one or more assets within the enterprise	
	2	This function is critical to safe operation	
	3	This function's control connection is "Standalone"	
		This function's control connection is "Simple"	
		This function's control connection is "Complex"	
		This function's control connection is "Vital"	
	4	This function is managed by the equipment and/or control system provider	
	5	This function does not have supplier provided control system documentation	
	6	This function's control system is protected by the system supplier's cybersecurity system	
Business Attributes check box if yes	1	The asset is not MTSA regulated	Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.
	2	The asset is not registered with a classification society that has cybersecurity guidance	Classification society "rules" are not implemented as required of a cybersecurity implementation.
	3	Land based IT or OT systems communicate to the asset's OT systems	Land-based/company-owned systems communicate to the asset's OT system or to a network to which OT systems are connected.
	4	Each asset is uniquely equipped	OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.
	5	The company has not developed policy governing IT cybersecurity	IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available.
	6	The company has not developed policy governing OT cybersecurity	OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available.
	7	OT cybersecurity is provided by a 3rd party supplier	A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protections.
Cybersecurity Documentation Attributes check box if yes	1	IT Cyber Security Officer (IT CSO) responsibilities are not documented	An official/individual responsible for security of IT systems has not been established.
	2	OT Cyber Security Officer (OT CSO) responsibilities are not documented	An official/individual responsible for security of OT systems has not been established.
	3	Incident Response Team (IRT) responsibilities are not documented	An official/individual responsible for supervising the response to security incidents related to OT systems has not been established.
	4	An OT SDD has not been developed	A SDD has not been developed for the onboard OT systems which inventories, describes, indicates cybersecurity in an asset specific design and
	5	A simplified cybersecurity SDD is not available	The cybersecurity systems have not been documented in an SDD which inventories, describes, indicates cybersecurity in an asset specific desig
	6	Management of Change (MoC) documents are not available	Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and administrated documen
	7	Cybersecurity training document(s) are not available	Home office and on asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedures.

Table E6. Point of Failure Detection Framework: Ferry



Cybersecurity Attributes			Asset Functions
Virtual Asset Depth		Virtual Asset Breadth	
Cyber Complexity Attributes check box if yes	1	This function is duplicated on one or more assets within the enterprise	
	2	This function is critical to safe operations	
	3	This function's control connection is "Discrete"	
		This function's control connection is "Simple"	
		This function's control connection is "Complex"	
		This function's control connection is "VSAT"	
	4	This function is managed by the equipment and/or control system provider	
	5	This function does not have supplier provided control system documentation	
	6	This function's control system is protected by the (asset) supplier's cybersecurity system	
Business Attributes check box if yes	1	The asset is not MTSA regulated	Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.
	2	The asset is not registered with a classification society that has cybersecurity guidance	Classification society "rules" are not implemented or required of a cybersecurity implementation.
	3	Land based IT or OT systems communicate to the asset's OT systems	Land based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.
	4	Each asset is uniquely equipped	OT systems designs (architectures) are unique within the fleet. There are no equal assets among the fleet.
	5	The company has not developed policy governing IT cybersecurity	IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available
	6	The company has not developed policy governing OT cybersecurity	OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available
	7	OT cybersecurity is provided by a 3rd party supplier	A cybersecurity solution provider (3rd party provider) is the primary resource for detailed information about monitoring and protections
Cybersecurity Documentation Attributes check box if yes	1	IT Cyber Security Officer (IT-CSO) responsibilities are not documented	An official individual responsible for security of IT systems has not been established
	2	OT Cyber Security Officer (OT-CSO) responsibilities are not documented	An official individual responsible for security of OT systems has not been established
	3	Incident Response Team (IRT) responsibilities are not documented	An official individual responsible for coordinating the response to security incidents related to OT systems has not been established
	4	An OT SSD has not been developed	A SSD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific design [illegible]
	5	A compiled cybersecurity SSD is not available	The cybersecurity controls have not been documented in an SSD which inventories, describes, indicates cybersecurity in an asset specific desig
	6	Management of Change (MoC) documents are not available	Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and sanctioned MoC documen
	7	Cybersecurity training documents are not available	Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.

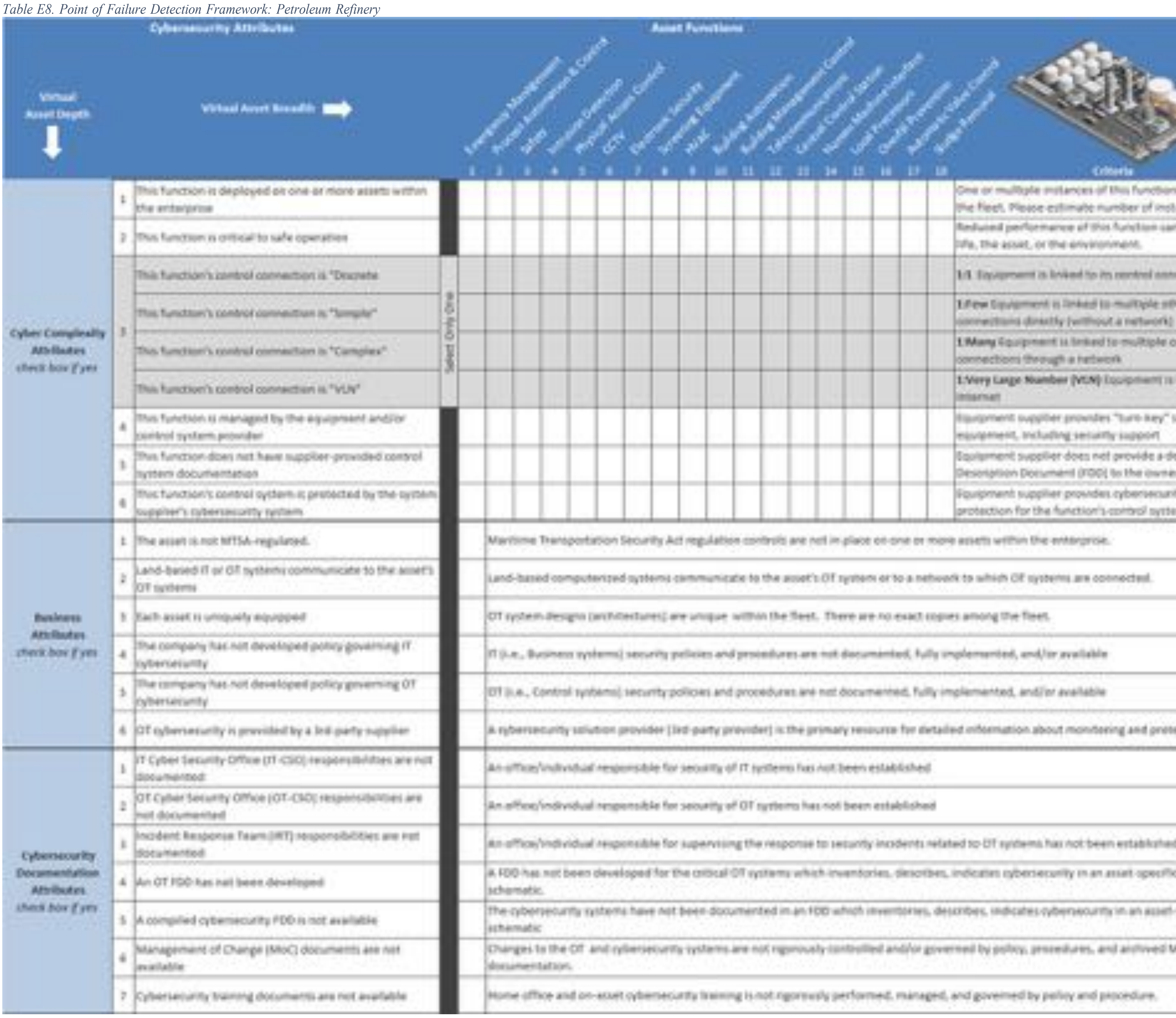
Table E7. Point of Failure Detection Framework: CDC Facility



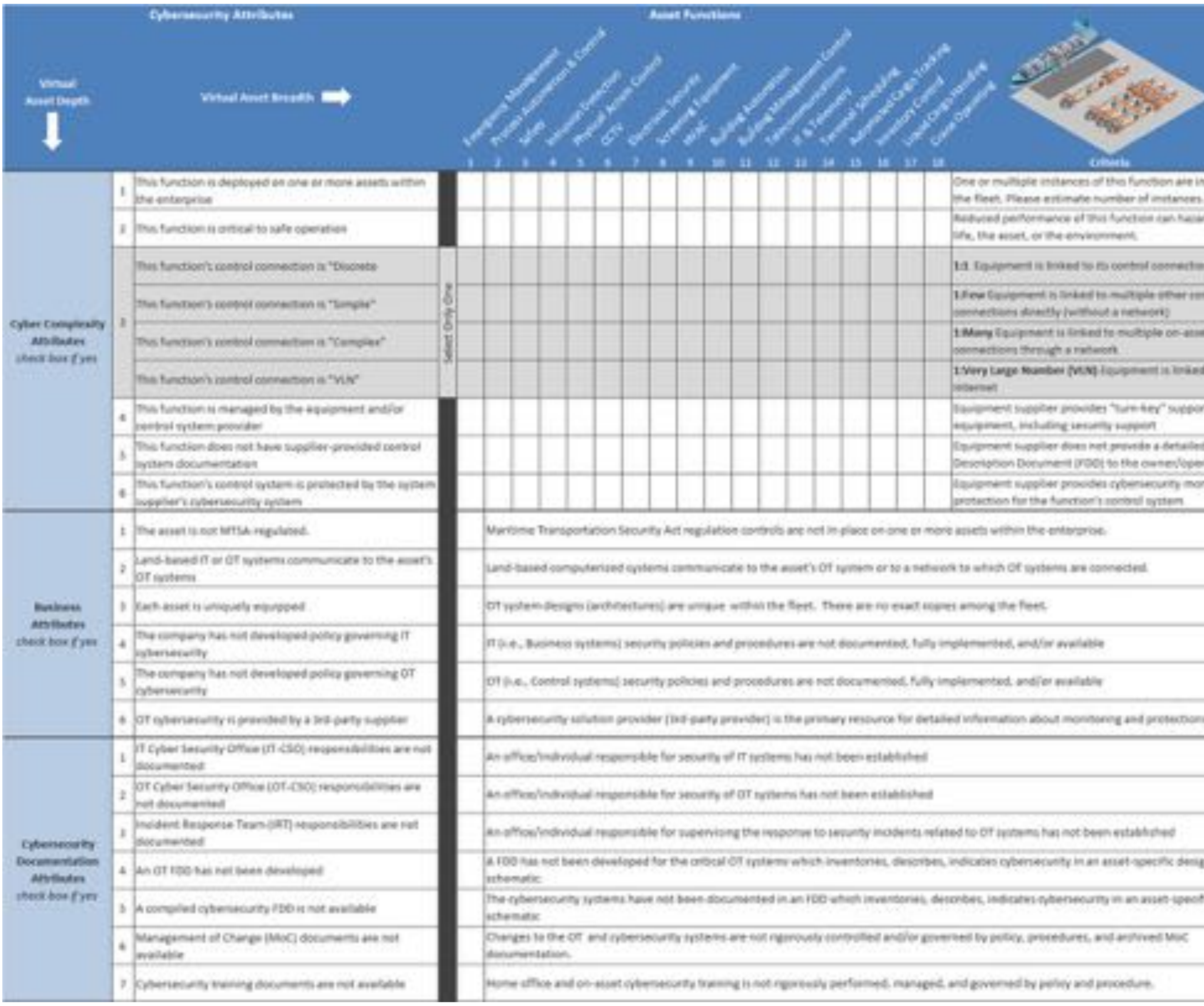
Virtual Asset Depth		Cybersecurity Attributes Virtual Asset Breadth		Asset Functions Emergency Management 1	Process Automation & Control 2	Safety 3	Intrusion Detection 4	Physical Access Control 5	CCTV 6	Electronic Security 7	Screening Equipment 8	HVAC 9	Building Automation 10	Building Management Control 11	Telecommunications 12	IT & Telemetry 13	Control Center 14	Remote Terminal Units 15	Programmable Logic Controllers 16	Inventory Control 17	Purchasing/Ordering 18	Shipments/Scheduling 19	Valve Control 20	Criteria
Cyber Complexity Attributes *check box if yes*	1	This function is deployed on one or more assets within the enterprise																						One or multiple instances of this f the fleet. Please estimate number
	2	This function is critical to safe operation																						Reduced performance of this func life, the asset, or the environment
	3	This function's control connection is "Discrete	Select Only One																					**1:1** Equipment is linked to its cont
		This function's control connection is "Simple"																						**1:Few** Equipment is linked to mult connections directly (without a ne
		This function's control connection is "Complex"																						**1:Many** Equipment is linked to mu connections through a network
		This function's control connection is "VLN"																						**1:Very Large Number (VLN)** Equip Internet
	4	This function is managed by the equipment and/or control system provider																						Equipment supplier provides "turn equipment, including security sup
	5	This function does not have supplier-provided control system documentation																						Equipment supplier does not prov Description Document (FDD) to the
	6	This function's control system is protected by the system supplier's cybersecurity system																						Equipment supplier provides cybe protection for the function's conta
Business Attributes *check box if yes*	1	The asset is not MTSA-regulated.			Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.																			
	2	Land-based IT or OT systems communicate to the asset's OT systems.			Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.																			
	3	Each asset is uniquely equipped			OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.																			
	4	The company has not developed policy governing IT cybersecurity			IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available																			
	5	The company has not developed policy governing OT cybersecurity			OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available																			
	6	OT cybersecurity is provided by a 3rd-party supplier			A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protecti																			
Cybersecurity Documentation Attributes *check box if yes*	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented			An office/individual responsible for security of IT systems has not been established																			
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented			An office/individual responsible for security of OT systems has not been established																			
	3	Incident Response Team (IRT) responsibilities are not documented			An office/individual responsible for supervising the response to security incidents related to OT systems has not been established																			
	4	An OT FDD has not been developed			A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific de																			
	5	A compiled cybersecurity FDD is not available			The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset-spe																			
	6	Management of Change (MoC) documents are not available			Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC																			
	7	Cybersecurity training documents are not available			Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.																			

ABS

Table E8. Point of Failure Detection Framework: Petroleum Refinery



	Cybersecurity Attributes			Asset Functions																		
Virtual Asset Depth ⇩		Virtual Asset Breadth ➡		Emergency Management	Process Automation & Control	Safety	Intrusion Detection	Physical Access Control	CCTV	Electronic Security	Screening Equipment	HVAC	Building Automation	Building Management Control	Telecommunications	Central Control Station	Human Machine Interface	Load Processors	Overfill Prevention	Automatic Valve Control	Sludge Removal	
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Criteria
Cyber Complexity Attributes *check box if yes*	1	This function is deployed on one or more assets within the enterprise																				One or multiple instances of this function the fleet. Please estimate number of inst
	2	This function is critical to safe operation																				Reduced performance of this function can life, the asset, or the environment.
	3	This function's control connection is "Discrete	Select Only One																			**1/1** Equipment is linked to its control conn
		This function's control connection is "Simple"																				**1:Few** Equipment is linked to multiple oth connections directly (without a network)
		This function's control connection is "Complex"																				**1:Many** Equipment is linked to multiple o connections through a network
		This function's control connection is "VLN"																				**1:Very Large Number (VLN)** Equipment is internet
	4	This function is managed by the equipment and/or control system provider																				Equipment supplier provides "turn-key" s equipment, including security support
	5	This function does not have supplier-provided control system documentation																				Equipment supplier does not provide a de Description Document (FDD) to the owne
	6	This function's control system is protected by the system supplier's cybersecurity system																				Equipment supplier provides cybersecuri protection for the function's control syste
Business Attributes *check box if yes*	1	The asset is not MTSA-regulated.			Maritime Transportation Security Act regulation controls are not in place on one or more assets within the enterprise.																	
	2	Land-based IT or OT systems communicate to the asset's OT systems			Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.																	
	3	Each asset is uniquely equipped			OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.																	
	4	The company has not developed policy governing IT cybersecurity			IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available																	
	5	The company has not developed policy governing OT cybersecurity			OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available																	
	6	OT cybersecurity is provided by a 3rd-party supplier			A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and prote																	
Cybersecurity Documentation Attributes *check box if yes*	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented			An office/individual responsible for security of IT systems has not been established																	
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented			An office/individual responsible for security of OT systems has not been established																	
	3	Incident Response Team (IRT) responsibilities are not documented			An office/individual responsible for supervising the response to security incidents related to OT systems has not been established																	
	4	An OT FDD has not been developed			A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset specific schematic.																	
	5	A compiled cybersecurity FDD is not available			The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset- schematic																	
	6	Management of Change (MoC) documents are not available			Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived M documentation.																	
	7	Cybersecurity training documents are not available			Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.																	



		Cybersecurity Attributes		Asset Functions																		
Virtual Asset Depth ⬇		Virtual Asset Breadth ➡		Emergency Management	Process Automation & Control	Safety	Intrusion Detection	Physical Access Control	CCTV	Electrical Security	Screening Equipment	HVAC	Building Automation	Building Management Control	Telecommunications	IT & Telemetry	Terminal Scheduling	Automated Cargo Tracking	Inventory Control	Liquid Cargo Handling	Crane Operating	
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Criteria
Cyber Complexity Attributes *check box if yes*	1	This function is deployed on one or more assets within the enterprise																				One or multiple instances of this function are in the fleet. Please estimate number of instances.
	2	This function is critical to safe operation																				Reduced performance of this function can haza life, the asset, or the environment.
	3	This function's control connection is "Discrete	Select Only One																			**1:1** Equipment is linked to its control connectio
		This function's control connection is "Simple"																				**1:Few** Equipment is linked to multiple other co connections directly (without a network)
		This function's control connection is "Complex"																				**1:Many** Equipment is linked to multiple on-ass connections through a network
		This function's control connection is "VLN"																				**1:Very Large Number (VLN)** Equipment is linked internet
	4	This function is managed by the equipment and/or control system provider																				Equipment supplier provides "turn-key" suppor equipment, including security support
	5	This function does not have supplier-provided control system documentation																				Equipment supplier does not provide a detailed Description Document (FDD) to the owner/oper
	6	This function's control system is protected by the system supplier's cybersecurity system																				Equipment supplier provides cybersecurity mon protection for the function's control system
Business Attributes *check box if yes*	1	The asset is not MTSA-regulated.			Maritime Transportation Security Act regulation controls are not in-place on one or more assets within the enterprise.																	
	2	Land-based IT or OT systems communicate to the asset's OT systems			Land-based computerized systems communicate to the asset's OT system or to a network to which OT systems are connected.																	
	3	Each asset is uniquely equipped			OT system designs (architectures) are unique within the fleet. There are no exact copies among the fleet.																	
	4	The company has not developed policy governing IT cybersecurity			IT (i.e., Business systems) security policies and procedures are not documented, fully implemented, and/or available																	
	5	The company has not developed policy governing OT cybersecurity			OT (i.e., Control systems) security policies and procedures are not documented, fully implemented, and/or available																	
	6	OT cybersecurity is provided by a 3rd-party supplier			A cybersecurity solution provider (3rd-party provider) is the primary resource for detailed information about monitoring and protection																	
Cybersecurity Documentation Attributes *check box if yes*	1	IT Cyber Security Office (IT-CSO) responsibilities are not documented			An office/individual responsible for security of IT systems has not been established																	
	2	OT Cyber Security Office (OT-CSO) responsibilities are not documented			An office/individual responsible for security of OT systems has not been established																	
	3	Incident Response Team (IRT) responsibilities are not documented			An office/individual responsible for supervising the response to security incidents related to OT systems has not been established																	
	4	An OT FDD has not been developed			A FDD has not been developed for the critical OT systems which inventories, describes, indicates cybersecurity in an asset-specific desig schematic:																	
	5	A compiled cybersecurity FDD is not available			The cybersecurity systems have not been documented in an FDD which inventories, describes, indicates cybersecurity in an asset-specif schematic:																	
	6	Management of Change (MoC) documents are not available			Changes to the OT and cybersecurity systems are not rigorously controlled and/or governed by policy, procedures, and archived MoC documentation.																	
	7	Cybersecurity training documents are not available			Home office and on-asset cybersecurity training is not rigorously performed, managed, and governed by policy and procedure.																	

ABS

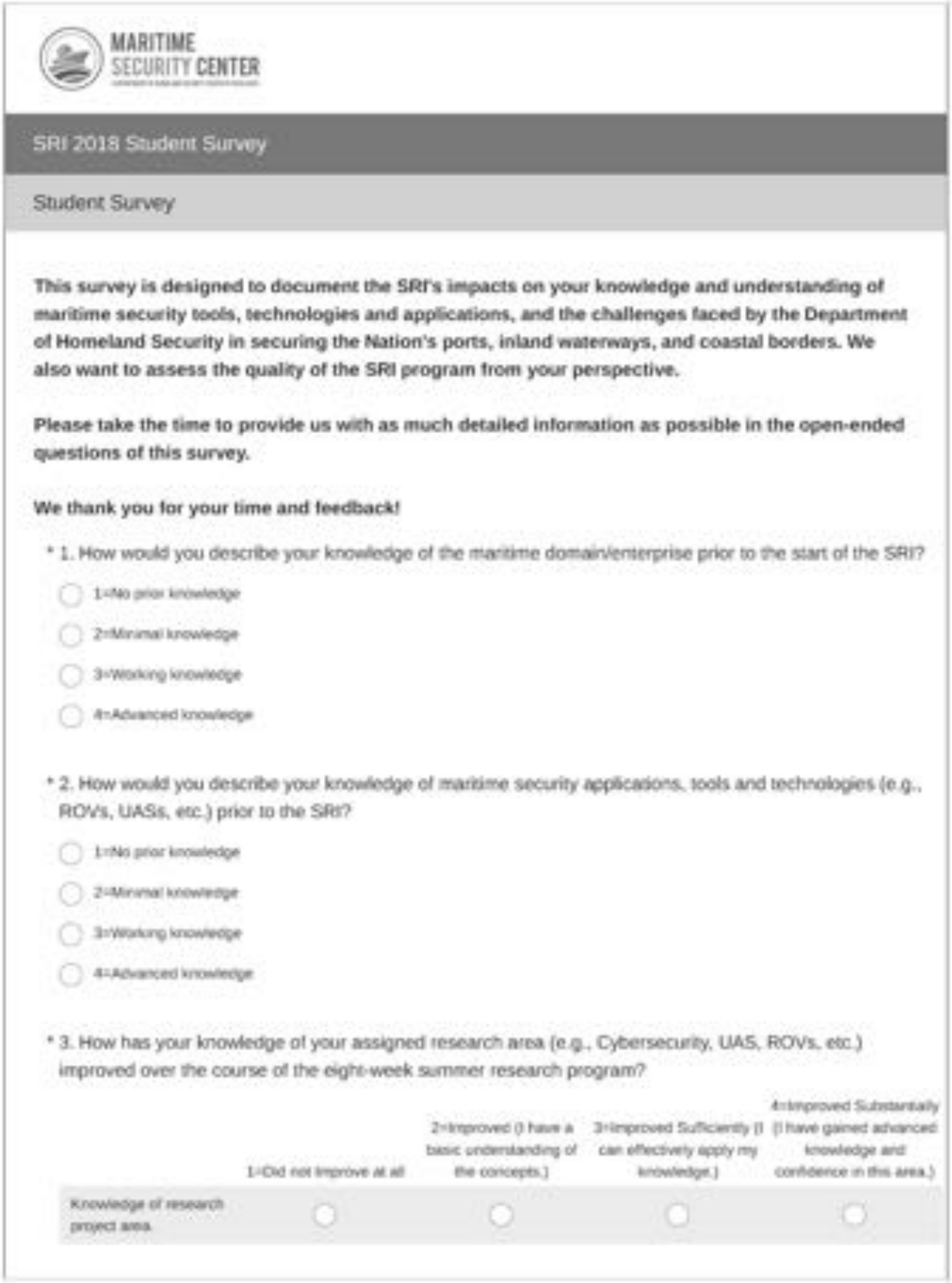
Appendix C-2 USMC CSR Questionnaire

Question	Answer
1. What are the staffing requirements and what are the skills required?	
a. Is there a distinction between range operational staff and security research staff?	Both are available through ManTec.
b. What are the skill requirements for ops staff?	ManTec offers hardware, software, specialized research, and management skills as required. Services are scalable and can be adjusted to meet special requirements of clients.
c. What are the skill requirements for the research staff?	Research staff skill requirements are "flexed" based on client research and training requirements.
d. Are the needed skills provided by formal education or field experience – in what mix?	Both
e. What is the most useful approach you have found to attracting staff?	Not discussed in depth. ManTec apparently has access to a relatively deep pool of resources and skills.
f. How does the range leverage "field" staff or user information to guide uses of or research by the range?	Clients provide information concerning research activities from multiple sources. Commercial clients test/validate products in the lab. Clients hold some test activities/results very closely as proprietary. Other clients jointly develop and share methods and research tools with the Cyber Range. Agreements on sharing follow multiple patterns based on client preferences.
2. What facility/physical requirements are necessary, nice, not needed?	
a. What are the CRITICAL facilities and support structures?	Did not discuss in detail. It was clear that during the 7-8 year service life of the Range, trial and error guided some of the Range development activities.
b. What are the NICE-TO-HAVE facilities and support structures?	Not discussed except for indications that the Range is able to extend its capabilities depending on the nature of the request and the ability of the requestor to "plus-up" unusual costs for a particular research activity.
c. What are the *"I wish I had thought of that…"* facilities and support structures?	Not discussed except for anecdotal information about having flexed capabilities and resources for clients in the past.
d. What are the *"I wish I hadn't bought that…"* facilities and support structures?	Not discussed.

e. Is there a lifecycle migration path that you recommend in hindsight?	This was not discussed specifically, but indications were that the Range has developed over its lifecycle to adjust to specific driving problems provided by multiple service branch and commercial clients.
3. What funding models worked/didn't work?	
a. In the commercial space, options for funding exist (e.g., subscription; “pay-for-play”; free access in association with work-for-hire contacts; internally funded and internal-use only). How do you control/provide access and recover costs?	The Range is open to all funding models in direct and indirect service of the service branches, “*.gov” agencies, and supporting commercial product and service providers – including the USCG. Range staff recommended further communication within the DHS. General feeling was a need for additional communication between DHS, USCG and the Stevens project.
b. How do you charge or get paid?	See above (3a)
4. What is to be mirrored?	
a. Internet traffic, others?	Yes
b. What do you simulate?	This varies based on client requirements. The Range possesses strong capabilities for high fidelity simulations of extraodinarily large communications and data loads.
c. What do you emulate?	Indications were that simulation rather than emulation is the primary approach (double check with Cris).
d. Have you determined which use case characteristics or “drivers” cause one approach to be more useful than the other?	Yes, through observation, funding tradeoffs, and empirical results à simulation.
5. Are there transfer opportunities?	
a. Technology, processes...	Yes
b. What are the “outputs” of the range?	Training, test results, and research
c. Were outputs driven by formal requirements or anecdotally discovered?	Both. The outputs of the Range are need and opportunity driven.
d. Can your experimental and use-case targets be transferred outside of the range (e.g., …security architectures?; …secured function architectures?; …threat types/modes? …identities behind threats? …calculable risk models [“equations”]? …design for “protectability?”)?	Yes. The Functions-Connections-Identities model was discussed and was very interesting to the director. Cris also raised the idea of “mutating” network forms as being useful for honey-netting and protecting in the future. The Range team seemed to already be working in those areas. They were a bit guarded in their comments.
e. How do you draw the line between public and proprietary information?	The line is drawn based on service branch requirements and agreed-to contract arrangements with commercial clients.
f. How do you stay away from picking winners in the commercial space (the competitive vs. pre- competitive issue)?	The Range is very careful to NOT pick winners and has a staff member who strongly enforces that directive. However, the Range is positioning itself to provide a type of “Good Housekeeping” seal based on specific test results and performance in the Range.
6. Are there licensing opportunities for software?	
a. Do you develop requirements or recommendations for proprietary or commercial security solutions?	This is not clear to me, but I think they might (Check with Cris).

b. How is range-generated IP classified, disseminated, and protected?	By in-place governmental guidelines carefully following by ManTec. ManTex is clearly a highly experienced government contractor.
c. Do you license solutions?	Not clear, but probably not.
7. Can you avoid full price software licensing for this use?	
a. Do you seek evaluation licenses? …product testing licenses? …other?	The Range tries to reduce costs at any opportunity. Since it is used for testing software solutions, some commercial products are "left behind" after testing for additional use by the Range.
8. How is range use and recognition "promoted"?	
a. Internal promotion (proprietary?)	Training, directed outreach, networking
b. External promotion (public domain?)	Training, directed outreach, networking

APPENDIX E-1 SRI 2018 Student Survey



SRI 2018 Student Survey

Student Survey

This survey is designed to document the SRI's impacts on your knowledge and understanding of maritime security tools, technologies and applications, and the challenges faced by the Department of Homeland Security in securing the Nation's ports, inland waterways, and coastal borders. We also want to assess the quality of the SRI program from your perspective.

Please take the time to provide us with as much detailed information as possible in the open-ended questions of this survey.

We thank you for your time and feedback!

* 1. How would you describe your knowledge of the maritime domain/enterprise prior to the start of the SRI?

○ 1=No prior knowledge

○ 2=Minimal knowledge

○ 3=Working knowledge

○ 4=Advanced knowledge

* 2. How would you describe your knowledge of maritime security applications, tools and technologies (e.g., ROVs, UASs, etc.) prior to the SRI?

○ 1=No prior knowledge

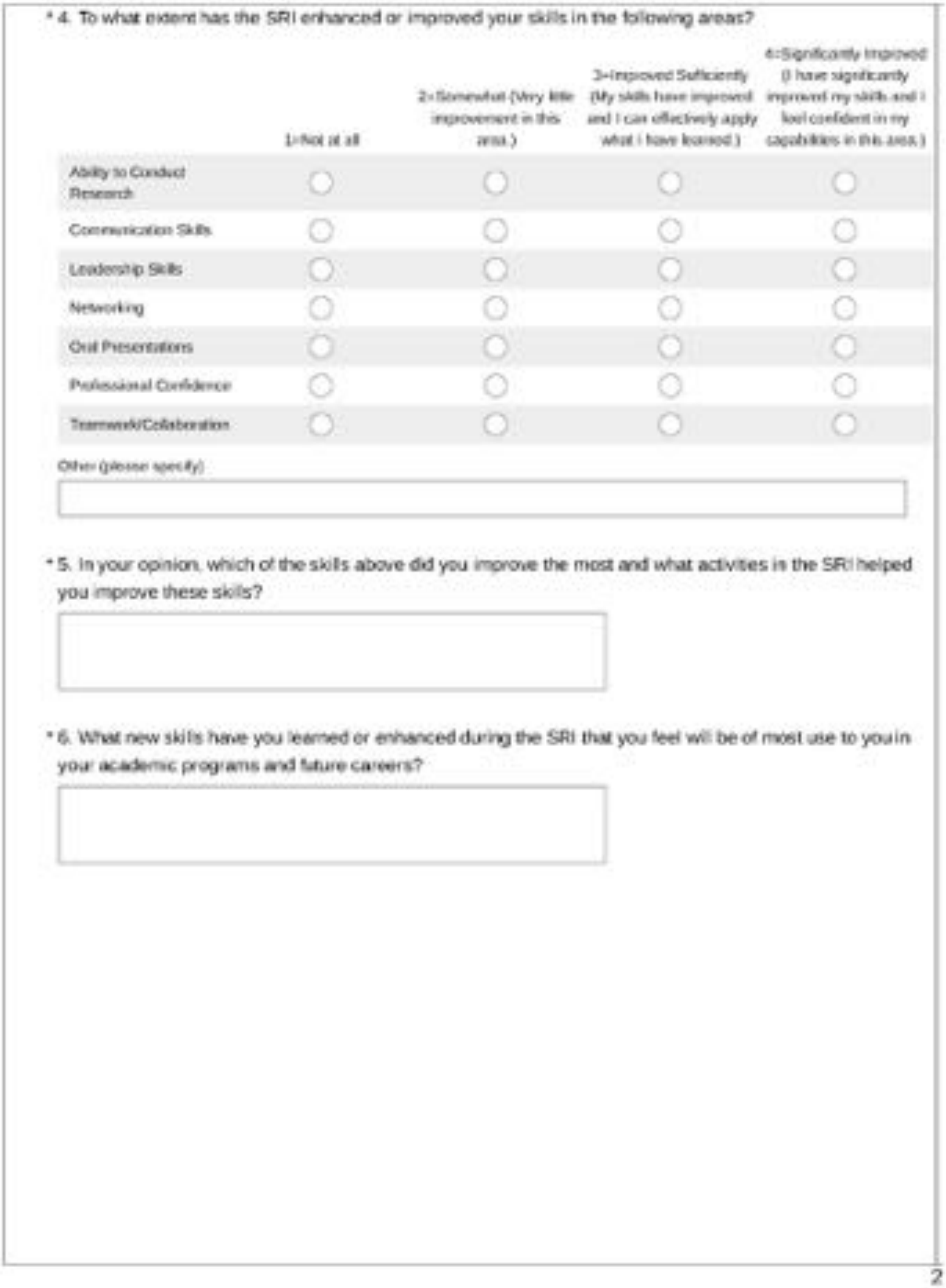
○ 2=Minimal knowledge

○ 3=Working knowledge

○ 4=Advanced knowledge

* 3. How has your knowledge of your assigned research area (e.g., Cybersecurity, UAS, ROVs, etc.) improved over the course of the eight-week summer research program?

	1=Did not improve at all	2=Improved (I have a basic understanding of the concepts.)	3=Improved Sufficiently (I can effectively apply my knowledge.)	4=Improved Substantially (I have gained advanced knowledge and confidence in this area.)
Knowledge of research project area	○	○	○	○



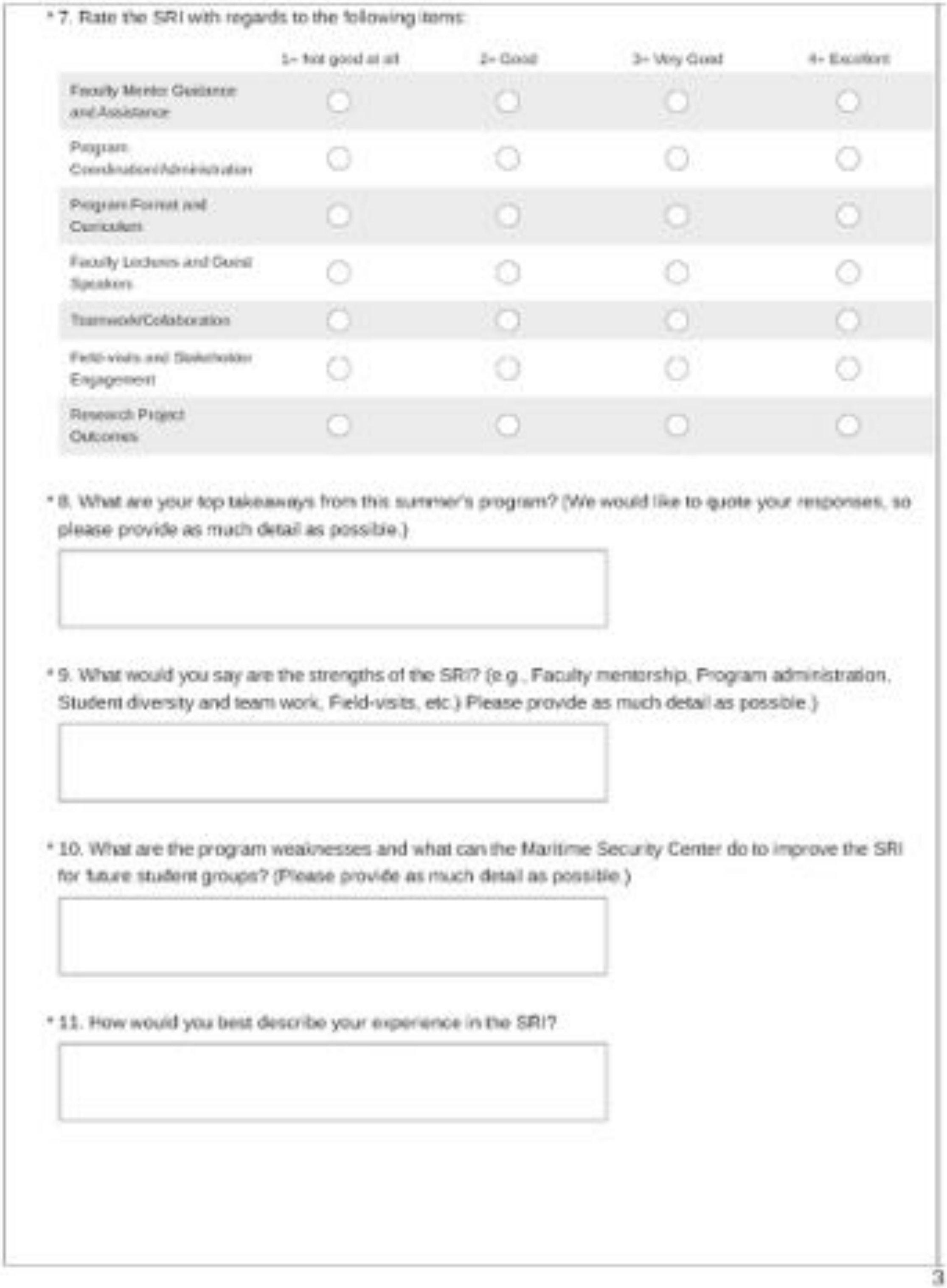
* 4. To what extent has the SRI enhanced or improved your skills in the following areas?

	1=Not at all	2=Somewhat (Very little improvement in this area.)	3=Improved Sufficiently (My skills have improved and I can effectively apply what I have learned.)	4=Significantly Improved (I have significantly improved my skills and I feel confident in my capabilities in this area.)
Ability to Conduct Research	○	○	○	○
Communication Skills	○	○	○	○
Leadership Skills	○	○	○	○
Networking	○	○	○	○
Oral Presentations	○	○	○	○
Professional Confidence	○	○	○	○
Teamwork/Collaboration	○	○	○	○

Other (please specify)

* 5. In your opinion, which of the skills above did you improve the most and what activities in the SRI helped you improve these skills?

* 6. What new skills have you learned or enhanced during the SRI that you feel will be of most use to you in your academic programs and future careers?



* 7. Rate the SRI with regards to the following items:

	1- Not good at all	2- Good	3- Very Good	4- Excellent
Faculty Mentor Guidance and Assistance	○	○	○	○
Program Coordination/Administration	○	○	○	○
Program Format and Curriculum	○	○	○	○
Faculty Lectures and Guest Speakers	○	○	○	○
Teamwork/Collaboration	○	○	○	○
Field-visits and Stakeholder Engagement	○	○	○	○
Research Project Outcomes	○	○	○	○

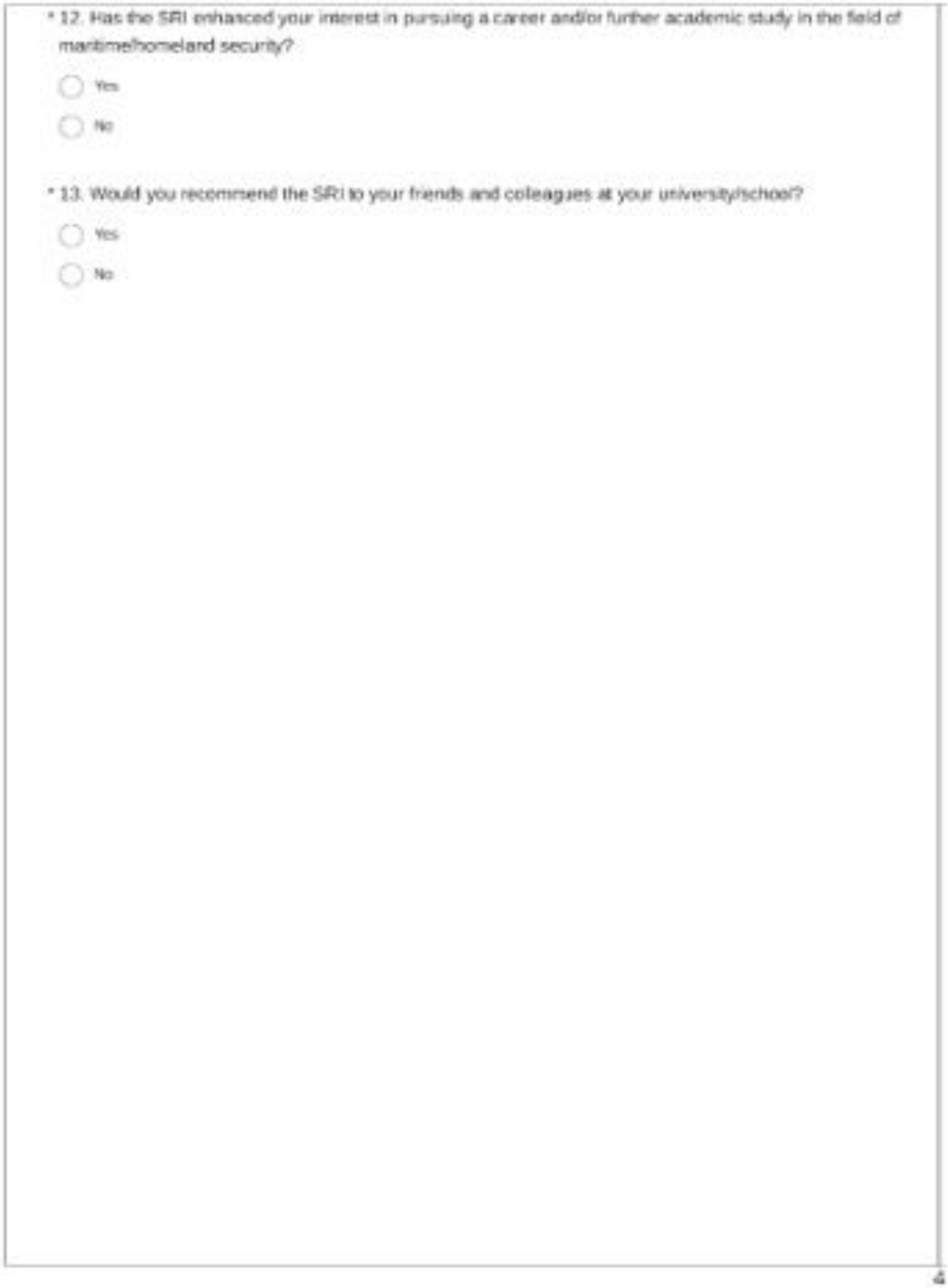
* 8. What are your top takeaways from this summer's program? (We would like to quote your responses, so please provide as much detail as possible.)

* 9. What would you say are the strengths of the SRI? (e.g., Faculty mentorship, Program administration, Student diversity and team work, Field-visits, etc.) Please provide as much detail as possible.)

* 10. What are the program weaknesses and what can the Maritime Security Center do to improve the SRI for future student groups? (Please provide as much detail as possible.)

* 11. How would you best describe your experience in the SRI?

3



* 12. Has the SRI enhanced your interest in pursuing a career and/or further academic study in the field of maritime/homeland security?

○ Yes

○ No

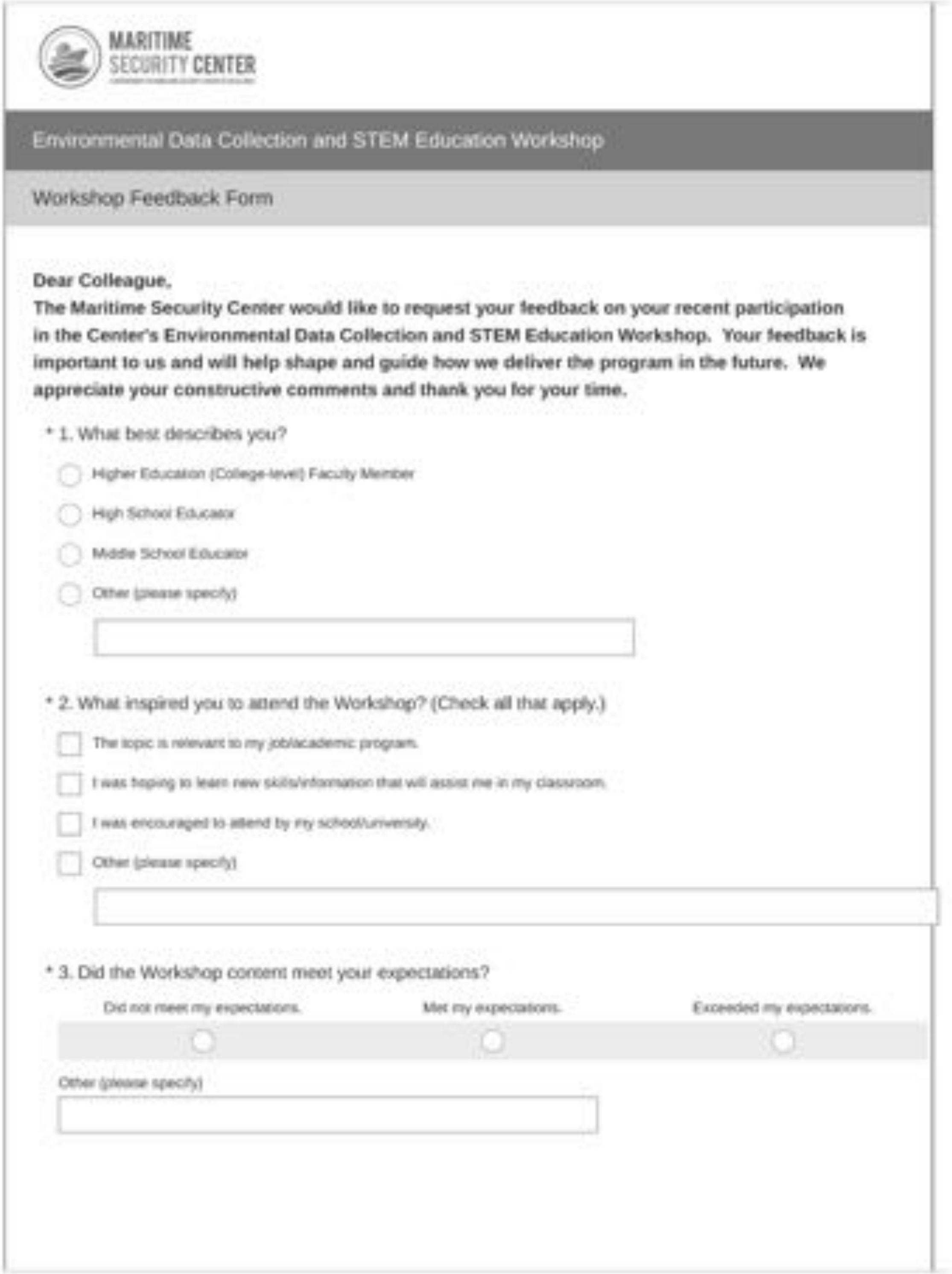
* 13. Would you recommend the SRI to your friends and colleagues at your university/school?

○ Yes

○ No

4

APPENDIX E-2 Environmental Data Collection Workshop Survey



MARITIME SECURITY CENTER

Environmental Data Collection and STEM Education Workshop

Workshop Feedback Form

Dear Colleague,
The Maritime Security Center would like to request your feedback on your recent participation in the Center's Environmental Data Collection and STEM Education Workshop. Your feedback is important to us and will help shape and guide how we deliver the program in the future. We appreciate your constructive comments and thank you for your time.

* 1. What best describes you?

○ Higher Education (College-level) Faculty Member

○ High School Educator

○ Middle School Educator

○ Other (please specify)

* 2. What inspired you to attend the Workshop? (Check all that apply.)

□ The topic is relevant to my job/academic program.

□ I was hoping to learn new skills/information that will assist me in my classroom.

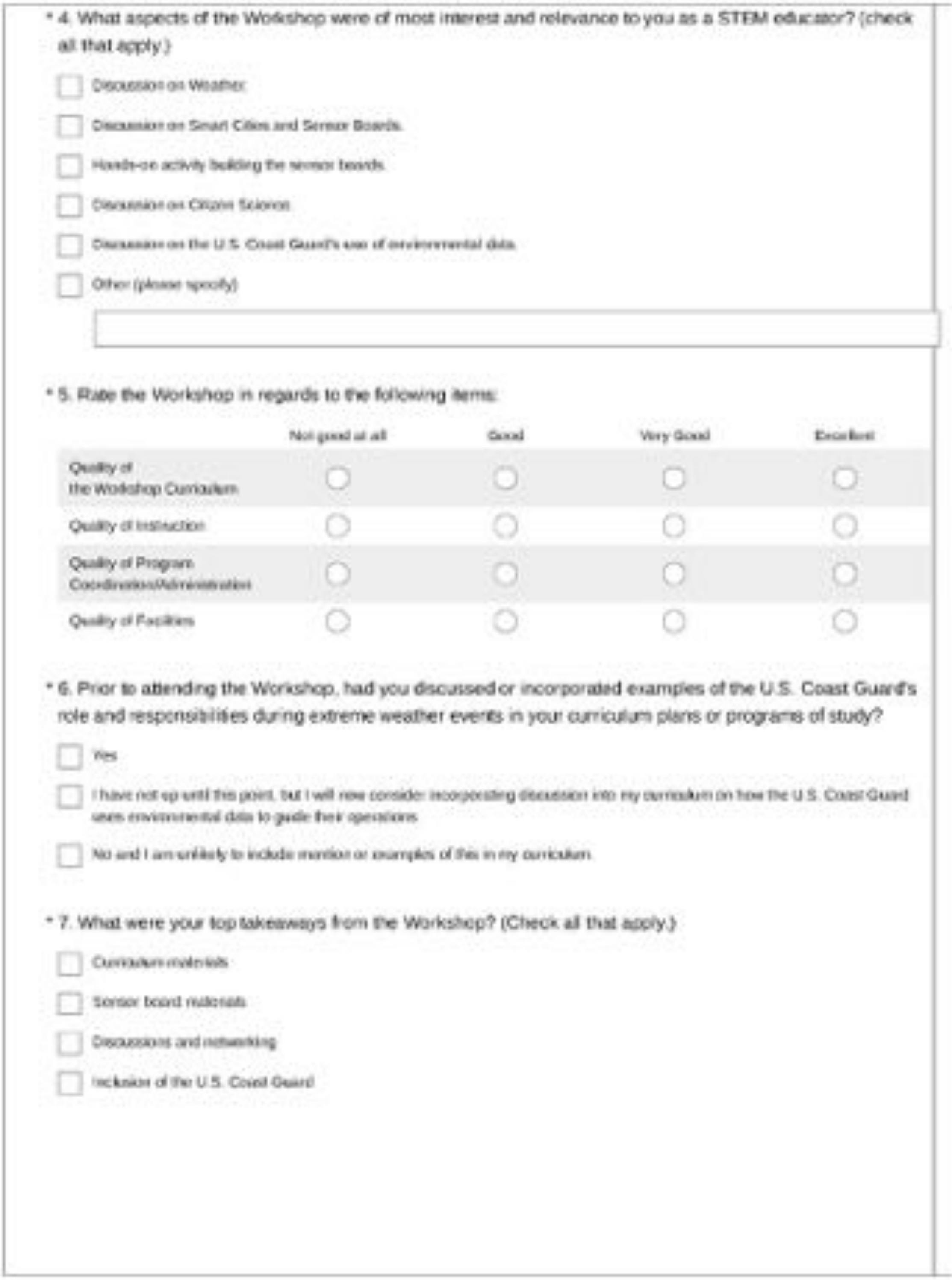
□ I was encouraged to attend by my school/university.

□ Other (please specify)

* 3. Did the Workshop content meet your expectations?

Did not meet my expectations.	Met my expectations.	Exceeded my expectations.
○	○	○

Other (please specify)



* 4. What aspects of the Workshop were of most interest and relevance to you as a STEM educator? (check all that apply.)

□ Discussion on Weather.

□ Discussion on Smart Cities and Sensor Boards.

□ Hands-on activity building the sensor boards.

□ Discussion on Citizen Science.

□ Discussion on the U.S. Coast Guard's use of environmental data.

□ Other (please specify)

* 5. Rate the Workshop in regards to the following items:

	Not good at all	Good	Very Good	Excellent
Quality of the Workshop Curriculum	○	○	○	○
Quality of Instruction	○	○	○	○
Quality of Program Coordination/Administration	○	○	○	○
Quality of Facilities	○	○	○	○

* 6. Prior to attending the Workshop, had you discussed or incorporated examples of the U.S. Coast Guard's role and responsibilities during extreme weather events in your curriculum plans or programs of study?

□ Yes

□ I have not up until this point, but I will now consider incorporating discussion into my curriculum on how the U.S. Coast Guard uses environmental data to guide their operations.

□ No and I am unlikely to include mention or examples of this in my curriculum.

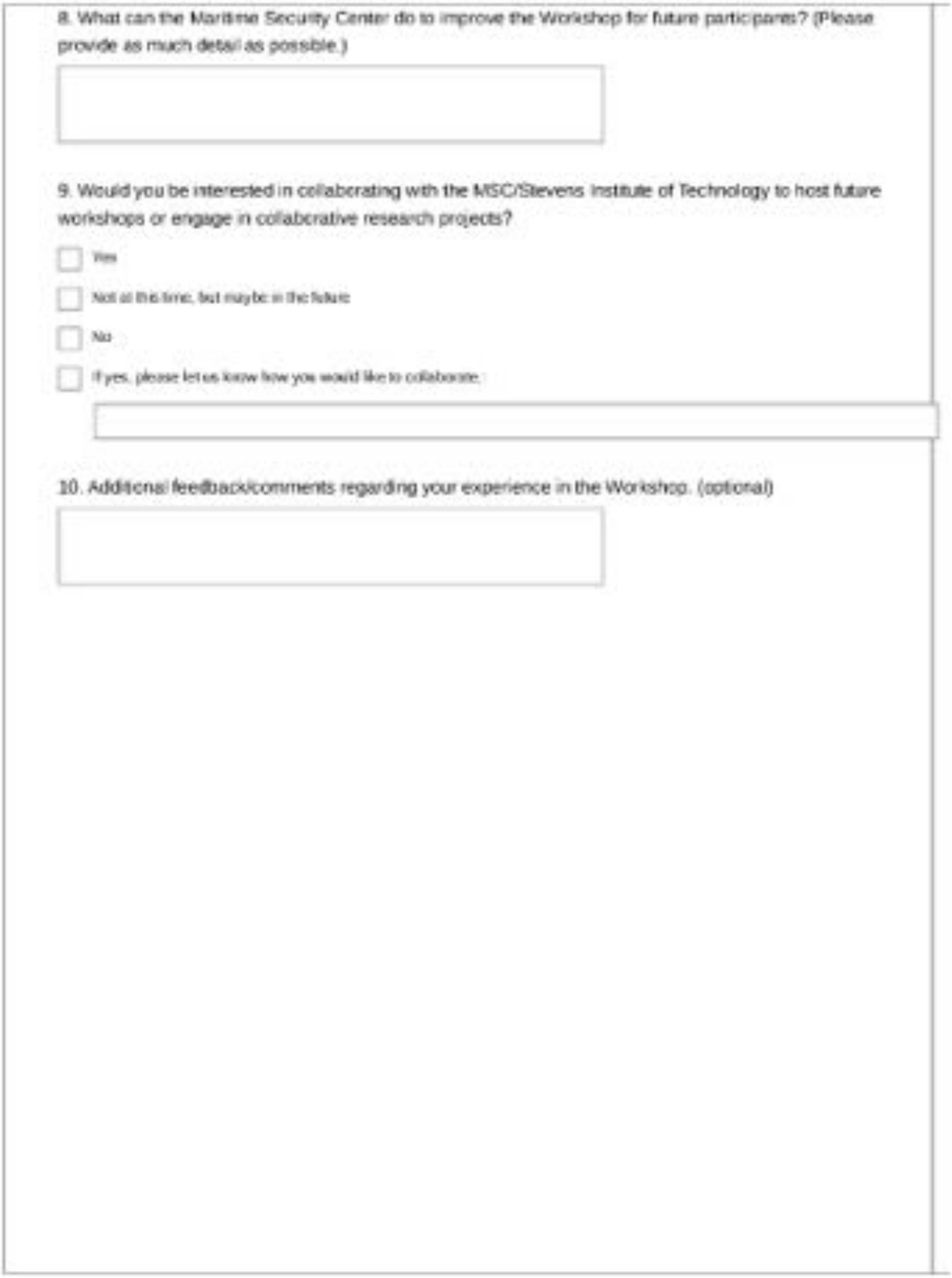
* 7. What were your top takeaways from the Workshop? (Check all that apply.)

□ Curriculum materials

□ Sensor board materials

□ Discussions and networking

□ Inclusion of the U.S. Coast Guard



8. What can the Maritime Security Center do to improve the Workshop for future participants? (Please provide as much detail as possible.)

9. Would you be interested in collaborating with the MSC/Stevens Institute of Technology to host future workshops or engage in collaborative research projects?

□ Yes

□ Not at this time, but maybe in the future

□ No

□ If yes, please let us know how you would like to collaborate:

10. Additional feedback/comments regarding your experience in the Workshop. (optional)