Lessons Learned from Teaching a Maritime Industrial Control Systems Cybersecurity Course

Brien Croteau
Cyber Science Department
United States Naval Academy
Annapolis, MD, USA
croteau@usna.edu

***Abstract*—A new technical elective course was taught in 2023 by the Cyber Science department at the U. S. Naval Academy. The goal of this course was to expose undergraduate students to the unique cybersecurity challenges and opportunities that exist in the Industrial Control Systems that are part of modern commercial vessels and warships. The course began with a survey of shipboard systems which included Propulsion, Electrical, Water, and Bridge Systems. Next, the students got hands-on practice coding ladder logic on Programmable Logic Controllers, from toggling lights to sending data via Modbus TCP. Finally, a project was completed where the students built a small-scale simulation of the alarms and monitoring system of local patrol craft. While these Operational Technology concepts have applications in many fields from energy production to smart cities, the maritime domain was chosen to ground in an important domain relevant to our students. This paper includes an outline of the course, what worked and didn't, and changes envisioned in future offerings.**

***Index Terms*—marine vehicles, industrial control, control system security, marine safety, programmable logic devices**

I. Introduction

There is a severe shortage of cybersecurity professionals in the global job market [1]. Within that broad field, there is an even greater need for experience in Operational Technology (OT) or Industrial Control Systems (ICS) systems which are integral to the critical infrastructure that our country and communities depend on. The recent attacks on power grids [2], water treatment facilities [3], and petroleum pipelines [4] demonstrate the catastrophic damage that can take place if these vital systems are left vulnerable to cyber attacks. For too many years, the industry has relied on a leaky air gap that separated these systems from the public internet or the fact that many of these systems required extensive knowledge of specific proprietary development technology. Recent malware discoveries have shown that nation-states are targeting these systems, thus the need for exposure to ICS for cybersecurity professionals starting as early as possible is vital.

This course was designed to allow undergraduate students to learn and gain hands-on experience with Programmable Logic Controllers (PLC) and then investigate the unique cybersecurity challenges in this domain. To provide a relevant application focus, the subdomain of Maritime Industrial Control Systems Cybersecurity was chosen since most of our graduates will go on to serve on ships and submarines, whose Hull, Mechanical, and Electrical (HM&E) systems typically are built with commercial industrial controllers and communications protocols.

Some material was adapted from a course taught by the Navy Cyber Warfare Development Group (NCWDG) assisted by Idaho National Labs whose focus was to expose Navy cyber technicians to the kinds of networks and systems found on maritime vessels. Additionally, a discussion was had with the instructor of a one-credit special topics Maritime Cybersecurity course that was taught at the United States Coast Guard Academy and an optional textbook [5] from that researcher was suggested to the students.

While other university courses cover a variety of maritime cybersecurity topics such as risk mitigation [6], administration [7], management [8], and more [9]. And there are college and university courses that cover practical Industrial Control Systems and Programmable Logic Controllers [10], [11]. To the best of the author's knowledge, there is no undergraduate-level course that combines these two topics into a single semester-long hands-on technical offering.

II. Maritime Systems Background

This section is intended to give an overview of the types of systems and how they are connected and related on an ocean-going vessel. A vessel at sea must be a floating (or submerged) self-contained city able to provide for its own power, water, food, heating, cooling, ventilation, waste treatment, and much more. The vessel as a whole needs to be a system of systems to ensure that each system works in harmony with the others.

A maritime vessel cannot execute its mission without moving from place to place: accordingly, the heart of the ship is its propulsion system. It typically comprises one or more massive large-bore slow-speed diesels, gas-turbine or steam-turbine engines, or electric motors that are connected to one or more propulsors via gearing and shaft-line components. Electrical generators may be integrated directly into the main propulsion system or be driven by independent prime movers. These generators provide power to the whole ship based on the total electrical demand; this can vary greatly, as shipboard operations change. Redundancy for casualty scenarios of outages or failures requires that the system architecture include two or more independent generators that can separately supply power to the ship's most vital electrical loads.

Continuing this analogy, auxiliary systems function much like the circulatory system and are also critical to the full operability of the ship and crew. Freshwater systems are required for crew drinking, cooking, and bathing, but are also used for a great many other functions on the ship including cooling specialized machinery and operating the steam plant. To conserve fresh water, sea water systems are used to cool major machinery, fight fires, flush toilets, and even ballast the ship to the appropriate draft in the water.

The brain of the ship is the bridge. Here, sailors on watch are responsible for the safe operation and navigation of the ship. The bridge team will use a number of systems and sensors including real-time geolocation, communication, and machinery control to maintain a cohesive picture of where the ship is and what it is doing.

III. Outline of the Course

The course was broken into three major sections. In the first section, common Maritime systems such as propulsion, electrical, water, and bridge systems were introduced, and hands-on labs were developed to give them some practical experience using computer-based simulations. The second section focused on learning to program PLCs and how they typically communicate with each other or outside systems. The final section of the course had the students build a benchtop lab environment that replicated a portion of the alarms and monitoring system of USNA Yard Patrol vessels.

Each week typically started with an overview lecture given by the instructor. The next class period was a double lab period where a hands-on exercise was performed individually, with collaboration, by each student. The final class period of the week typically started with presentations by the students where they spoke more in-depth about a chosen topic or technology that they researched outside of class. The remainder of that class was used to complete the lab assignment or further discussion about the presented topics. Holidays and other changes to the content meant that this weekly schedule often had to be adjusted.

In the sections of the paper below, each class component, summarized in Table I, is described. Following that is a discussion about what worked and didn't during this first offering and some changes that are envisioned during future semesters. A repository of the course material developed has been made available for use by other educators and feedback to the author is highly encouraged [12].

IV. Lectures

Early lectures were built from open source materials and some leverage the materials prepared for the NCWDG course described above. Short topical YouTube videos were also employed to explain certain key topics and give the context of the systems to those found on commercial vessels and are linked in the lecture slides. In the Propulsion Systems lecture, different propulsion types ranging from oars, sails, paddle-wheels, pump-jets, to propellers were introduced. Additionally, different Power Generation means were discussed, including steam engines, steam turbines, diesel, gas turbines, liquid natural gas, and fuel cells. Finally, some information was also shared about ship configurations in how engine rooms, propeller shafts, and reduction gears are typically arranged. Lecture 2 covered Maritime Electrical Systems and started by identifying some key components, including generators, switchboards, busbars, circuit breakers, and transformers. Then the concept of three-phase power was introduced and the benefits of using such a system were outlined.

The next Water Systems lecture spoke also about ballast, cooling, fire mains, potable water, and sewer water treatment. The Bridge Systems lecture, number 4, also introduced the main systems found on commercial vessels: Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS), RAdio Detection And Ranging (RADAR), Communications, Heading Control System (HCS), and other automation technology. Additionally, some comparisons were made between the bridge manning requirements between commercial and military vessels and recent improvements the U. S. Navy has made in Crew Endurance [13], part in response to the USS Fitzgerald and USS McCain collisions [14] that took place in 2017.

The next portion of the class moved to introducing Programmable Logic Controllers (PLC), Lecture 5 defined what is a PLC, talked some about the history of these devices, spoke about the typical components, and showed how they are used as part of industrial processes. The next lecture introduced the most important ideas of Ladder Logic: how they evolved from relay electrical diagrams, the symbols found on ladder logic diagrams, how basic logic functions can be implemented, and how the inputs and logic are scanned. The lecture finished with some examples of ladder logic programs that were investigated as a group. Additional time was taken the following week to introduce more advanced Ladder Logic concepts such as latches, toggles, counters, and timers.

The next few lessons covered the ICS protocols that PLCs and other devices use to communicate with each other. First, the earliest and most ubiquitous protocol, Modbus, was outlined. The first Modbus lecture covered the history, main philosophy, types of Modbus protocols, and introduced the Remote Terminal Unit (RTU) message format and components. Examples of messages were decoded and some information specific to the PLCs that the students used during the labs was shown. Lecture 8 briefly described some of the other types of ICS protocols in use including Common Industrial Protocol (CIP), Ethernet/IP, Distributed Network Protocol 3 (DNP3), Highway Addressable Remote Transducer (HART), BACNet, Open Platform Communications (OPC), and Profinet.

Lecture 9 is listed in the outline but slides were not produced to introduce this material. It was in conjunction with Lab 9, explained below, and borrowed heavily from an ICS security paper [15]. The final lecture was part of the introduction to the project, where the major systems and the alarms and monitoring systems of the Yard Patrol vessel were described. It started with basic information about the ship and descriptions of the main engines and generators that are found

TABLE I
COURSE OUTLINE

week	Lect #	Lecture Topics	Lab #	Lab Topics
1	0	Class Introduction	-	Introduction Video
2	1	Ship Propulsion Systems	1	VER Install and Engine Startup Tutorial
3	2	Ship Electrical Systems	2	VER Power Plant and Generators
4	3	Ship Water Systems	3	VER Ballast, Fire Fighting, Bilge, and Cooling Systems
5	4	Ship Navigation and Bridge Systems	4	Bridge Command Install and Tutorial
6	5	Introduction to PLC	-	Exam 1
7	6	Introduction to Ladder Logic	5	CCW Install and Ladder Logic Basics
8	6.5	Advanced Ladder Logic	6	More Ladder Logic: Toggles, Counter, Timers
9	7	ICS Protocols I (Modbus)	7	Modbus RTU RS-232
10	8	ICS Protocols II (others)	8	Modbus RTU RE-485 and Modbus TCP
11	9	Attacking ICS	9	Attacking ICS (part I)
12	-	Attacking ICS (part II)	-	Exam 2
13	10	YP703 Systems Overview	-	YP Field Trip
14	-	YP Project Introduction	-	HILICS Install and Tutorials
15	-	YP Project Work	-	YP Project Status Update
16	-	YP Project Work	-	YP Project Demonstrations
-	-	Review and Feedback Forms		Final Exam

onboard. Then moved to the Alarm and Monitoring system, including functional diagrams and photos of the components and interfaces of the system.

V. LABS

Nine labs in total were developed that were designed to allow the students to gain hands-on experience with the system or technology being introduced that week. The first three labs used a free-for-educational-use Windows-based ship high-fidelity system simulator called Virtual Engine Room (VER) Free Student Version [16]. VER allowed students to gain an appreciation for the complexity and interdependencies that exist on most modern maritime vessels' HM&E systems.

The first lab followed the start-up checklist given as part of the simulator. Since these students were not that familiar with these ship systems, an extensive tutorial with many annotated screenshots was created and shared with them to help aid them in finding the hundreds of individual valves and switches that needed to be operated in a particular order to bring the 7-cylinder main diesel engine online. An example of the VER interface is shown in Fig. 1. The second lab had the students investigate the electrical systems and fail-over functionality between the various generators. Different configurations of standby and already running backup power generation sources were investigated. Additionally, manual and automatic synchronization was performed to connect a running generator to an existing ship's load.

Lab 3 had the students figure out which pumps and values were required to change the ship's heel and trim by filling and emptying 16 individual ballast tanks, as shown in Fig. 2. It also had them turn on and verify the emergency operation of the Fire Mains. The Bilge and Cooling systems were also investigated showing how the ship would malfunction if these systems failed or were attacked.

Unfortunately, the VRE simulator did not have great integration to bridge systems such as the helm and radar. Thus, a free (GPL v2) Bridge Command simulator [17] was found and employed to allow students to interact with these systems. Lab 4 had the students first become familiar with the basic

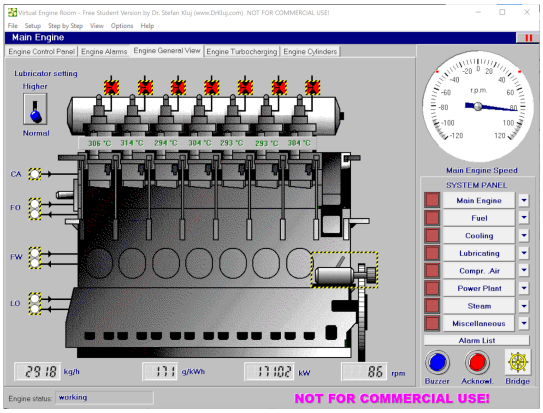

Fig. 1. Screenshot of the Virtual Engine Room simulator interface showing the Main Engine [16]. Different main systems of the simulator can be accessed through the tiles on the right side of the display. Once within a system, there are multiple pages accessed via the tabs across the top.

simulator commands to move the vessel, then they moved to a more comprehensive model that also included a simulated radar system. The simulator interface is shown in Fig. 3.

Lab 5 had the students download the free version of the Rockwell Automation Connected Components Workbench (CCW) software [18] that was designed to work with the Allen Bradley micro820 trainers, shown in Fig. 4, which were located at each student's station [19]. It also guided them through the process of creating their first ladder logic program that connected each discrete input to a corresponding output. Then the program was downloaded to the PLC and run. Near the end of the lab, the concept of a latch was introduced and the students built a version of a circuit that controlled a single output that represented a piece of machinery, like an engine, with inputs from run and stop switches.

The following lab had them expand on their burgeoning Ladder Logic programming skills, by first creating a program that would toggle a single output whenever a particular input was energized, then that was modified to build two- and three-bit counters. Where one input would cause the binary value

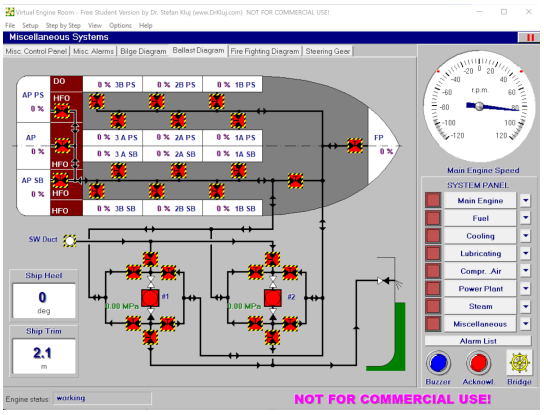

Fig. 2. Screenshot of the Virtual Engine Room simulator interface showing the Ballast system [16]. Sixteen ballast tanks can be filled or emptied using the ballast pumps and valves. Clicking on each value will toggle its status, and the ballast pumps are energized from the Misc. Control Panel (not shown). The ship's current heel and trim are updated based on the status of the tanks shown in the lower left corner.

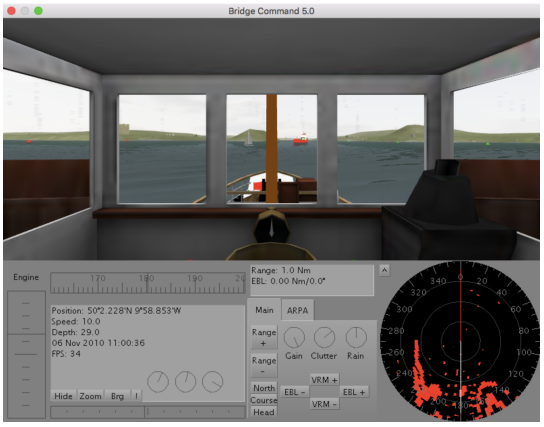

Fig. 3. Screenshot of the Bridge Command simulator interface when a tug boat model is loaded [17]. Keyboard shortcuts can be used to update the rudder and engine inputs. A robust surface radar simulation including realistic controls and clutter is shown in the lower right corner.

shown to increase, another would cause it to decrease, and a third input would reset the value back to all zeros (lights off). The students were also challenged to expand that logic one level more to build a four-bit counter, and most were successful. Near the end of this lab, timer blocks were also introduced.

Labs 7 and 8 had the students start to work with sending Modbus messages between the PLCs that were connected initially by shielded copper wires. A MSG_MODBUS block was created and configured initially to have one PLC read the status of another PLC's discrete inputs and display them on its outputs. Then two-way communication was established between the two devices. Eventually, another PLC was inserted into the middle that read in the inputs from one PLC and drove the outputs of the third PLC. Lab 7 had the PLCs connected in a point-to-point fashion using the RS-232 terminals. In Lab 8, the PLCs were connected in a flat bus using the RS-485 inputs. This allowed the students to see all the traffic

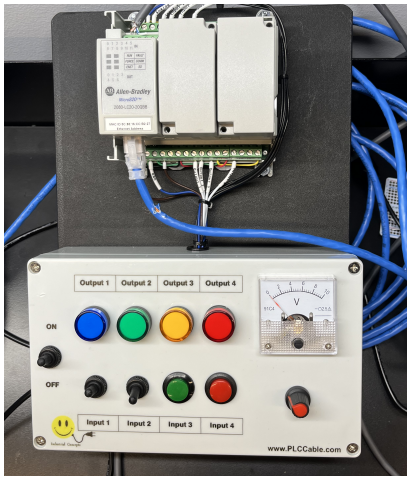

Fig. 4. Allen Bradley micro820 Programmable Logic Controller trainer kit manufactured by PLC Cables [19]. Each unit has four discrete inputs and four discrete outputs, in addition to a single analog input and output. Students used these for four PLC labs where they were introduced to programming with ladder logic and then communicating with the Modbus protocol over both RTU and TCP.

on an oscilloscope and a RS-485 to USB device was also used which allowed them to capture the serial traffic using a terminal program Also as part of this lab, a demonstration version of the modscan64 program [20] was used to send commands and data from their PCs to the PLCs and vice-versa. Finally, the students also switched over to communicating via Modbus TCP messages using a different message block, and TCP network traffic was captured using Wireshark [21] and analyzed.

Lab 9 started by having the students read the Tommy Morris and Wei Gao 2013 paper "Industrial Control System Cyber Attacks" [15] which describes how several different cyber attacks could be demonstrated using PLCs that are communicating using Modbus messages. They did some research on particular attacks from that paper and attempted with intermittent success to show tangible effects on the three-PLC lab setup.

VI. Presentations

For several topics, each of the students was assigned to further research some specific technologies and create a three to five slide presentation and brief the rest of the class in a five to ten minute discussion. Examples from the second lesson on shipboard electrical systems included information about the state-of-the-art and future technologies of Nuclear, Solar, and Gas Turbine systems. In the next lesson covering water systems, the students spoke about Fire Mains, Freshwater Supply, and Ballast systems, each going more in-depth on that topic than the overview lecture did at the start of the lesson. For the Bridge Systems lesson: Radar, Automatic Identification System (AIS), and Autopilot systems were further researched and presented. The final set of presentations was in conjunction with Lab 9, where the students read [15] and selected one of the attacks described in that paper to try out in the PLC lab environment. The three categories that were chosen were: Response and Measurement Injection Attacks,

Command Injection Attacks, and Denial of Service Attacks. For this presentation, the students were asked to describe their chosen attack in more detail, talk about how it could be performed on a maritime vessel, and find at least one academic paper or news article that describes this kind of attack on any system in the real world.

VII. Project

The final project took place over the last three weeks of the semester. It was intended to tie together everything that they had learned about maritime systems and industrial control systems by creating a benchtop lab environment that replicated a portion of the alarm and monitoring system and associated equipment from YP vessels that are used for small-craft ship-handling lessons and training at USNA.

Initially, the students were given a lecture that gave an overview of the systems on the patrol vessels and some basic information about the MAX II alarm system. Then a field trip was made during a lab period where the class went to a YP vessel that was tied pierside. During that visit the students were escorted around the bridge and engineering spaces by a civilian electronics technician who is the person responsible for maintaining these systems. They interacted with the six touchscreen displays that are located in the pilot house and engine room. They also saw the components including the two Personal Computer servers, two PLCs, and numerous interfaces between the sensors attached to components like the main engines, generators, and tanks. They also traced the two sets of wires that connected the two redundant controllers and observed when the emergency generator automatically came online after securing the single running main generator. The students enjoyed this opportunity to see and touch these ICS systems in action.

Fig. 5. The Hardware-in-the-loop industrial control system (HILICS) training platform manufactured by the Air Force Institute of Technology (AFIT) [22]. The trainer comprises an AB MicroLogix 1100 PLC connected to a RasPi via Serial Peripheral Interface (SPI). Python scripts running on the RasPi simulate the physical plants such as a garage door or a fluid tank process.

In subsequent classes, a subset of the systems to replicate was collaboratively identified. A set of three Air Force Institute of Technology (AFIT) designed and manufactured Hardware-in-the-loop Industrial Control System (HILICS) training platforms [22] were used. Each system, shown in Fig. 5, combines a Raspberry Pi single-board computer and touchscreen display with an Allen-Bradley MicroLogix 1100 PLC. These devices turned out to be the perfect platform since they provided the ability to simulate the engine and generators and the PLCs could communicate with each other via CIP messages. This required the students to download another set of free development software and learn a new interface, but they were able to clear those hurdles and they created a working demonstration. The system they created comprised one main engine, one generator, and one Human-Machine Interface (HMI) console. Analog data representing the speed and voltage or temperature of the simulated spinning systems as well as discrete fault information was passed to the display unit which consolidated the data from both subsystems into a single display. The display also had two inputs that would send start or shutdown signals to the individual components. The final deliverable for the class was a single Interface Control Document that fully described the interfaces, connections, and protocols for the data sent between the systems.

VIII. Things that worked

The lectures were a partial success, but this being the course's first offering, further polish, and more relevant and approachable content would go further to increase student engagement with the large amount of all new information that was being presented. Incorporating more interactive elements, read-ahead materials, and quizzes will also be explored.

The labs were very well received and went a long way toward making the connection between the lectures and the application. Adapting what has worked well in other technical courses with labs, the creation of a detailed tutorial document with plenty of pictures and links to external resources was the primary documentation the students followed along with. Then a Google Form was used to collect the submission, this was much shorter and primarily had them answer a few yes/no at some completion checkpoints, also would ask for proof in the form of screenshots, and finally, one or two discussion questions where the students were asked to summarize what they learned and also extend those ideas to the potential cybersecurity implications.

The presentations were also a success, the students were excited to research more about unique topics of their choice on their own. To make it easier to plan their time, consider making the list of acceptable topics available further ahead of the lecture.

IX. Things that didn't work

Enrollment was a challenge, during this first offering only three students signed up and all of those were Cyber Operations majors. This was despite sending information to other technical departments such as Electrical and Computer Engineering, Control Systems Engineering, and Naval Architecture. Working harder to have them cross-listed as an elective in those majors, will likely help this going forward. For this initial offering, so as to not overly burden the students with memorization for exams in this course, all the exams permitted the use of notes, slides, and the internet (although AI use was

prohibited). This allowed for more in-depth questions, but a more balanced approach going forward should be investigated.

Some of the mechanics of installing the PLC programming software on their issued laptops took a few class sessions to iron out. It may be possible to host that software on virtual machines that can stay connected to the PLC devices and the students can connect to them from the classroom or the dorms. That might also require a webcam to monitor PLC outputs, but for the ladder logic portions, they can also make use of the simulated PLC that is part of the Rockwell Automation suite.

X. Future Changes

Ideally, the same PLC could be used for both the PLC programming and project application. New hardware has been purchased including Siemens PLCs and HMIs will be evaluated over the summer. The licensing of Kongsberg Digital's K-Sim Connect [23] has been completed and this cloud-based ship simulation platform will also be evaluated for possible future inclusion. More class presentations could be scheduled each week, as the course calendar allows.

Additionally, more cybersecurity-focused topics and labs are envisioned to be included in future offerings. Recent awareness of other security researchers that are using the high-fidelity Bridge Command software when looking at attacks on radar systems [24] and the construction of an Integrated Navigation System (INS) range [25], prompts investigation to see if portions of their systems can be incorporated into future hands-on labs or projects.

XI. Conclusion

This paper highlights some lessons learned from the first offering of a new Maritime Industrial Control Systems Cybersecurity elective. The outline of the course included brief descriptions of the topics and technology covered. Additionally, a discussion about what worked and didn't and future changes that are envisioned was included. Faculty who are also working in this important field of filling the gap in our cyber workforce with exposure to Operational Technology are invited to view the materials shared at the author's GitHub repository [12] and are encouraged to provide feedback or suggestions.

References

[1] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action*. Cybersecurity and Infrastructure Security Agency, 2022.

[2] "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[3] S. Adepu and A. Mathur, "An investigation into the response of a water treatment system to cyber attacks," in *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 2016, pp. 141–148.

[4] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, "Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns," *IEEE Access*, vol. 8, pp. 128 440–128 475, 2020.

[5] G. C. Kessler and S. D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers (2ed)*, 2022.

[6] Norwegian University of Science and Technology, "TS501822 Maritime Digital Security Course Description," accessed: 2023-07-19. [Online]. Available: https://www.ntnu.edu/studies/courses/TS501822/2023/1#tab=omEmnet

[7] Texas A&M University, "Maritime Administration Course Catalog," accessed: 2023-07-19. [Online]. Available: https://catalog.tamu.edu/undergraduate/course-descriptions/mara/

[8] Business College of Athens, "Maritime Cyber Security MSc Program Description," accessed: 2023-07-19. [Online]. Available: https://www.bca.edu.gr/en/master-degrees/shipping-transport-logistics-department/msc-maritime-cybersecurity/

[9] Stevens Institute of Technology, "Maritime Cybersecurity Professional Development Program Description," accessed: 2023-07-19. [Online]. Available: https://www.stevens.edu/page-basic/maritime-cybersecurity-program

[10] Penn State Berks, "PLC for Industry Certificate Program Description," accessed: 2023-07-19. [Online]. Available: https://berks.psu.edu/continuing-education/certificate-programs-adult-learners/plc-industry-certificate-program

[11] Southeastern Louisiana University, "IT 331 Industrial Control Systems Course Description," accessed: 2023-07-19. [Online]. Available: https://www.southeastern.edu/acad_research/depts/iet/undergrad_degree/courses/pdfs/it331.pdf

[12] Brien Croteau, "SY486K MICS Course Materials Repository," accessed: 2023-07-19. [Online]. Available: https://github.com/brienc23/MICS_Course_Materials

[13] N. L. Shattuck, P. Matsangas, H. Clifton, J. Hart, C. Czeisler, and L. Barger, "Crew Endurance Training in the United States Navy: Interim Assessment of a 3-year Project," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 64, no. 1. SAGE Publications, 2020, pp. 841–845.

[14] "Chief of Naval Operations: Memorandum with Enclosures Report on the Collision between USS FITZGERALD (DDG 62) and Motor Vessel ACX CRYSTAL and Report on the Collision between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC." United States. Office of the Chief of Naval Operations, 2017.

[15] T. H. Morris and W. Gao, "Industrial control system cyber attacks," in *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*, 2013, pp. 22–29.

[16] S. Kluj, "Virtual Engine Room – Free Student Version," 1999, accessed: 2023-05-30. [Online]. Available: https://drkluj.com/simulators/free-student-version/

[17] M. Sibly, "Bridge Command: An interactive 3D ship and radar simulator," Sep. 28, 2017, accessed: 2023-05-30. [Online]. Available: https://www.bridgecommand.co.uk/

[18] Rockwell Automation, "Connected Components Workbench Software," accessed: 2023-05-30. [Online]. Available: https://www.rockwellautomation.com/en-us/capabilities/industrial-automation-control/design-and-configuration-software.htmls

[19] PLC Cables, Inc., "Allen-Bradley Micro820 Analog CCW PLC Trainer Micro800 Training Kit," accessed: 2023-05-30. [Online]. Available: https://www.plccable.com/allen-bradley-micro820-analog-ccw-plc-trainer-micro800-training-kit/

[20] WinTECH Software, "ModScan64," 1990, accessed: 2023-05-30. [Online]. Available: https://www.win-tech.com/html/demos.htm

[21] G. Combs, "The Wireshark Network Analyzer," 1998, accessed: 2023-05-30. [Online]. Available: https://www.wireshark.org/

[22] S. Dunlap, "HILICS - Hardware-in-the-loop industrial control system training platform," Air Force Institute of Technology, 2019, accessed: 2023-05-30. [Online]. Available: https://github.com/sdunlap-afit/hilics

[23] Kongsberg Digital, "K-Sim Connect," 2020, accessed: 2023-05-30. [Online]. Available: https://kongsbergdigital.com/products/k-sim/connect/

[24] K. Wolsing, A. Saillard, J. Bauer, E. Wagner, C. van Sloun, I. B. Fink, M. Schmidt, K. Wehrle, and M. Henze, "Network attacks against marine radar systems: A taxonomy, simulation environment, and dataset," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*. IEEE, 2022, pp. 114–122.

[25] A. Oruc, V. Gkioulos, and S. Katsikas, "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)," *Journal of Marine Science and Engineering*, vol. 10, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2077-1312/10/1/107