University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

01 University of Plymouth Research Outputs University of Plymouth Research Outputs

2021-12-06

Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety

Tam, K

http://hdl.handle.net/10026.1/18567

10.4236/jtts.2022.121001
Journal of Transportation Technologies
Scientific Research Publishing

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

Scientific Research Publishing

Journal of Transportation Technologies, 2022, 12, 1-27
https://www.scirp.org/journal/jtts
ISSN Online: 2160-0481
ISSN Print: 2160-0473

Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety

Kimberly Tam[1], Rory Hopcraft[1], Kemedi Moara-Nkwe[1], Juan Palbar Misas[1], Wesley Andrews[1], Avanthika Vineetha Harish[1], Pablo Giménez[2], Tom Crichton[1], Kevin Jones[1]

[1]Maritime Cyber Threats Research Group, University of Plymouth, Plymouth, UK
[2]Fundacion Valenciaport, Valencia, Spain
Email: kimberly.tam@plymouth.ac.uk, rory.hopcraft@plymouth.ac.uk, kemedi.moara-nkwe@plymouth.ac.uk, juan.palbarmisas@plymouth.ac.uk, wesley.andrews@plymouth.ac.uk, avanthika.vineethaharish@plymouth.ac.uk, pgimenez@fundacion.valenciaport.com, T.Crichton@plymouth.ac.uk, kevin.jones@plymouth.ac.uk

How to cite this paper: Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J.P., Andrews, W., Harish, A.V., Giménez, P., Crichton, T. and Jones, K. (2022) Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. *Journal of Transportation Technologies*, **12**, 1-27.
https://doi.org/10.4236/jtts.2022.121001

Received: October 20, 2021
Accepted: December 3, 2021
Published: December 6, 2021

Copyright © 2022 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

As the maritime sector embraces more technology to increase efficiency, lower carbon emissions, and adapt to meet modern challenges, cyber and cyber-physical safety become a more significant issue. However, unfortunately, much of past research view cyber-security issues in transportation as primarily information technology problems. This paper designs and uses a case study to illustrate how cyber-security and physical safety should be viewed together, cyber and physical (*i.e.* cyber-physical), when considering ship-to-ship and ship-to-shore interactions. While there is some scenario designing, this case study is built with real port data and ship systems to demonstrate a real-world cyber-attack on a ship. It shows plausible physical effects that affect the safety of those involved. This case study is also made realistic with a novel hybrid cyber range and hardware testbed environment, designed to examine the different effects a ship-based cyber-attack could potentially have on a port. This informs several solutions, technical and social, that could enhance cyber-physical safety in marine transportation.

Keywords

Cyber-Physical Security, Safety, Port, Cyber Range, Cybersecurity

1. Introduction

In today's world, both ports (sea and inland) and vessels are undergoing significant change as technology evolves. While vessel control and crew situational awareness can be improved with new technologies, the cyber-security concern would be whether these advantages could introduce new vulnerabilities and

safety risks. This includes global concerns around fully autonomous systems, but also remote access, when crew and computers need to hand-off control to each other depending on the situation [1] [2] [3]. Sector-specific systems, supporting sensor and communication networks, and the Internet of Things (IoT) are also growing in availability, ease of use and ease of integration. In general, ports are becoming more automated, reducing waiting times, and integrating themselves with surrounding smart cities and other transportation links (e.g. rail and road). Newly designed and built vessels, such as cruise and container, are physically becoming larger and have exhibited Information Technology (IT) converging with Operational Technology (OT) [4]. This convergence can provide useful monitoring and fine-grained control, sometimes even remotely, but also increases the possibility a cyber-attack could have physical consequences.

When a cyber-attack can have a negative effect on physical safety of crew, ship, or environment (e.g. nearby ships, ports, infrastructure), this article considers that to be a cyber-physical risk to safety. Hence, the over-arching goal of this research is to show how a cyber-attack can affect physical safety, through a maritime-themed case study. More specifically, this case study brings awareness to potential vulnerabilities and their possible outcomes. This is done by using real data and lab equipment to create an awareness raising, but plausible, scenario, where hijacking a large container ship's rudder while it enters a port can block the entrance and effectively reduce cargo throughput. The challenges of safeguarding ports and ships from cyber-attacks are often addressed separately.

Generally, ports have been perceived as more critical to the overall supply chain, and therefore received the most attention. However, as demonstrated with the Suez incident [5], larger ships are being used and they are facing more challenging maneuverers around existing channels and ports. This lowers safety margins when considering cyber-attacks on transportation infrastructure like ports and vessels. The COVID-19 pandemic has also had major effects, both in the flow of goods and the treatment of seafarers [6], highlighting the human element in maritime cyber-physical safety as well. For a realistic case study, the authors have collaborated with the Port of Valencia, ranked in 2020 as one of the ten largest container ports in Europe. In 2020, this port saw 80 million tons (5.428.307 TEU) of total traffic, 533,137 cars and 1,112,727 passengers [7]. The Port of Valencia is highly specialized in containerized merchandise but also attends to other cargo such as liquid, solid bulk, and ro-ro (roll-on/roll-off). It manages passenger and merchandise traffic with the Balearic Islands, and receives many cruise ships annually. The port has three big container terminals managed by the most significant shipping lines in the world with 4.7 km of berths.

While targeting a port itself could result in downtime measured from hours to weeks [8] and increase the physical risks of operations, this case study seeks to determine if similar effects could be achieved if an approaching ship is compromised instead of the port itself. This could raise considerable safety concerns, and this case study is designed to encourage more discussion around improving cyber-physical safety. This is true in maritime transportation, critical national

infrastructure, and transportation in general. While the scenario is designed to be as realistic as possible, some simulation is required to not cause any actual damage to those involved (e.g., the Port of Valencia). Along with realistic port information, this case study uses a ship simulator running in a cyber range, and a cyber-physical testbed.

While the authors do use cyber range technology to simulate a large container ship, the Port of Valencia environment (e.g., layout), and any resulting damage to ship or port, hacking a simulator does not provide a realistic attack scenario. Therefore, the authors execute the cyber-attack on real off-the-shelf ship systems in a secure testbed and use a known CVE[1] for validation. This is to provide the most realistic scenarios possible, both from the attack aspect and an effects aspect. To quantify the port downtime as the result of this attack chain, further simulation is provided to calculate delays from both the effect of blocking the entryway, when possible, and the secondary effects of delays and other port-related logistics.

The results of this case study are multi-fold: 1) Approach the challenges of maritime cyber-physical risks to safety and raise awareness on possible, high-impact, risks between ship and port; 2) Use cyber range hosted simulations to realistically explore potential damages in a safe manner; 3) Simulate downtimes to port throughput; 4) Inform potential technical solutions and appropriate training to reduce risks. The remaining sections are as follows. Section II examines relevant works to maritime cyber-security, leading into Section III covering the essential technologies and tools relevant to this case study. Section IV explains how these tools are best used to explore a cyber-physical attack on a ship's steering mechanisms at a critical point of inbound pilotage into the Port of Valencia. Section V discusses the case study itself, including different outcomes by varying where and when the same attack chain is executed. Overall results, impacts, concerns, limitations, and future work can be found across Sections VI-VII.

2. Cyber-Security in Maritime Transport

There are several areas of cyber-security work that relate, but approach the problem very differently, to this case study. These are needed, as recent trends of cyber-attacks on infrastructure, such as power, water, and oil, show that sector-specific operations in the maritime sector, and transportation in general [9] [10] [11], could also be in danger. Moreover, securing ports or ships in isolation will not mitigate all risks, and that cyber-physical risks should be viewed at a high-level, possibly even cross-sector. As explained more in Section VII, a port infecting a ship or a personal device affecting either ship or port are out of the scope of this paper, but the authors intend to explore this in future research. The scenario in this paper is built on both cyber range (CR) and hardware testbed technology to provide realism. Both technologies have been well researched, and individuals are beginning to adopt these solutions for use across the maritime

[1]Common Vulnerabilities and Exposures (CVE) ID and Programmable Logic Controller's make and model not published for security purposes.

sector [12] [13]. Understanding the cyber-security vulnerabilities and potential cyber-physical risks to safety are also growing areas of research across transportation and maritime.

The case study this paper presents is different from IT-focused scenarios, and has a higher probability of causing significant damage to people, goods, environment, and infrastructure because of its OT focus. Affecting critical ship mechanisms through cyber-attacks has, to the best of the authors' knowledge, no related published work. A research project injected similar data into ship systems; however, this was done without actually exploiting a vulnerable system [14]. Moreover, the attack only blue-screened a bridge terminal, whereas this study uses a known vulnerability in ship systems that would trigger significant physical effect on both ship and surrounding port. There has also been research on satellites and their connections to marine systems [15]. In contrast, this paper focuses on ship vulnerabilities that can be exploited locally, isolated, and does not rely on external connectivity.

Considering the security of internal components, work on Programmable Logic Controllers (PLCs), buses, and more, are a part of port and ship security [8]. As an example, closed-circuit television (CCTV) would be an isolated system on a ship or at a port. Most modern CCTV camera's movements (e.g. swivel) are controlled by a number of protocols sent over RS-422. This has some semblance to NMEA 0183, and it has been shown that these serial ports and protocols are vulnerable [16]. For the more modern Ethernet-based NMEA or NMEA 2000, similar works on Controller Area Network (CAN) buses highlight potential vulnerabilities in both cars and ships [17]. In addition to vulnerabilities in these protocols for transmitting data and controls, there can also be vulnerabilities in local PLCs, which read and write serial data. There are several examples of this, which have been studied extensively, particularly in the context of critical national infrastructure [18]. As a part of transportation, ports and vessels are similarly vulnerable. Therefore, this case study differs in both the delivery of the scenario and the scenario itself from previous works.

In one study [19], risks of a single simulated Electronic Chart Display and Information System (ECDIS) were explored, with particular focus on the Windows Operating System (OS) running on the system. Existing vulnerability scanning tools were used; however, the paper did note the limitations of analyzing an isolated system. In comparison, the testbed and cyber range combination in this approach gives a higher view of the connected systems-of-systems (SoS) and how an attack on one system (PLC) can have an effect on another (rudder). Other work examining wireless communications going from satellite to vessel(s) has also been examined for AIS (Automatic identification system) and satellite vulnerabilities in isolation [15] [20]. Both have shown that many systems, such as AIS, have not been designed to be secure. Moreover, in the case of AIS, spoofing data is relatively simple, as the levels of authentication and encryption do not match most other modern systems in the IT space. As there are currently

state-level actors involved with spoofing attacks on ships, it is clear that there are cyber-security concerns for this sector [21].

3. Tools and Methodology

This case study was developed in collaboration with the Port of Valencia ($port_V$) in Spain to examine physical disruptions and safety risks caused by a cyber-attack on an approaching container ship ($ship_C$). To best analyze this, a combination of accurate, safe, simulation and realistic cyber-attack is needed. To simulate $ship_C$ and $port_V$ faithfully, experiments use Wärtsilä software [22] installed on a portable cyber range, useful for demonstrations, as explained more further on. However, hacking the simulation software proves little realism, so a hardware testbed comprised of real ship systems is used to explore real-world bridge cyber-attacks in the safety of a cyber-secure lab. For more comparison on simulation, emulation, and hardware-based testbed for researching maritime cyber-security, please refer to [12]. In addition to discussing some of the design and use of the cyber range and testbed, this section also discusses the ship data that is being altered in transit. Systems core to the case study experiments, including programmable logic controllers, and navigation systems will also be covered in this section for background knowledge.

3.1. Cyber Range Simulations

Cyber ranges (CR) are interactive, simulated representations that provide a safe environment for trainees to gain hands-on skills, and/or a secure environment for product development and testing. Uses of CRs, and their concepts, are broadly defined and cater to a wide number of users and scenarios. In 2013, the Australian government attempted to classify publicly available CRs around the world [23], however much has happened in this space since then. A more complete survey of existing CR architecture, design, and use is [24]. This provides a comprehensive literature review on several aspects of CRs used globally. The definition of cyber range this article shall use comes from this publication, which defines a CR as an environment to realize and execute training scenarios and provide a playground for trainees. Shortly after that publication in 2020, came one of first published works discussing CRs for maritime cyber-security training [13]. However, this paper only theorized the potential benefits, whereas this article actually uses a cyber range to demonstrate safety hazards using a realistic cyber-physical case study.

The CR used for this study is capable of simulating port and ship characteristics, operations, and most importantly, interactions. Physical elements like the ship build (e.g., length, weight, turning radius) and port layout (e.g. entryway, water depth, terminals) are critical for this case study (see **Figure 1**). Many cyber ranges have been used in the past to play out IT focused scenarios, with a small but growing interest in OT systems, the latter including notable elements like Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS) [25]. A significant advantage to addressing these issues with a CR, is

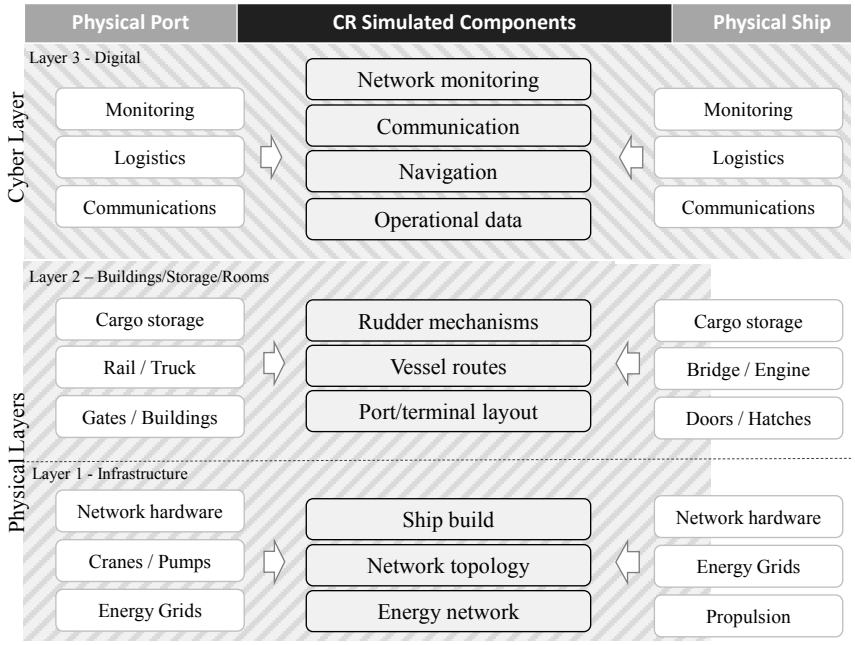

Figure 1. Physical and Cyber layers of port and ship, with some simulated in the CR.

they often simplify complex systems, like the Internet, into smaller-scale scenarios that CRs of all sizes could deal with. Moreover, they are safe environments, so this study's simulations will only show likely damage, instead of inflicting real damage. While it is often desirable to have a realistic training environment, scalability hinders that development. Besides SCADA there are other OT systems, but like the Internet is a significant focus for IT, SCADA has often been the focus for most OT research.

There are over 42 features defining $ship_C$'s simulation, including the name of the ship it is modelled after, but for security purposes this paper will only state the ship's rough length is 390+ meters, and that it is based on a real container ship that has entered $port_V$ several times as of 2021. The length and a few other features determine essentials such as speed, turning radius, and the attack's effects on the ship physically, as seen in Section V. Sea areas and ship models were purchased from Wärtsilä and can be assumed sufficiently accurate to demonstrate the physics of compromised $ship_C$ interacting with $port_V$ as the scenario's cyber-attack plays out. **Figure 2** shows the charts as would be see on a ship's ECDIS. These electronic charts (e-charts) are identical to those used by real ships and produced by the United Kingdom Hydrographic Office, which are highly accurate. Thus, with accurate environment, route and ship profile, the simulator is able to generate and send live ship data to the testbed, in real-time to other systems, or saved and replayed for training.

Based on the port data, historic routes/data, and certified mariners, a route of entry was planned using the specified $ship_C$ target into $port_V$, taking into full account the physical attributes of both and the date of arrival. For security, these details are out of the scope for this paper, with the critical point being that a vessel of this size is likely to enter this port with a specific range of speed and with

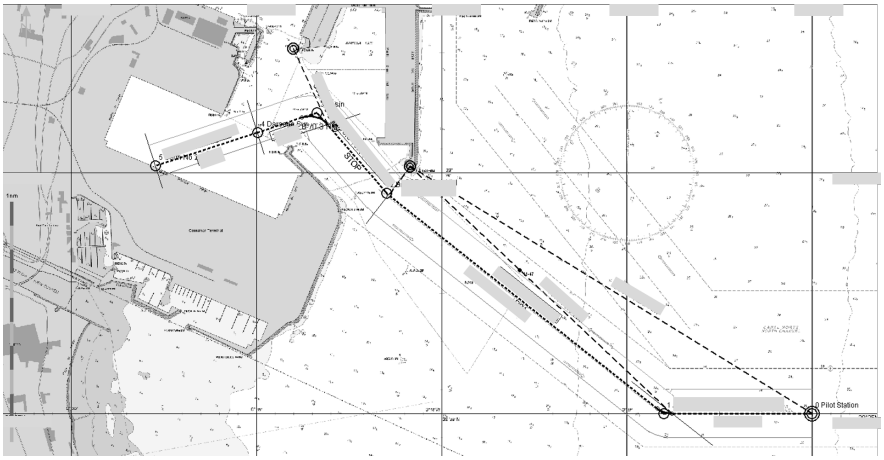

Figure 2. Anonymised pilot plan of large container $ship_C$ entering portp as seen on simulated ECDIS in CR.

the rudder changing angles precisely at four critical points (see **Figure 2**). Therefore, the objective of our case study is to either alter the angle, or block legitimate commands to lock the rudder. In our simulations, the resulting difference of rudder angle after attack, even though not a huge deviation, was sufficient to block the entry way to $port_V$'s container terminal, and in some variants (see Section VI), the passenger terminal as well. This has provided safe but trustworthy verification that the cyber-attack proposed could have a significant physical effect on safety and throughput.

To understand the wider impact of a port with partially or fully blocked entryways, a simulation model has been developed separately to the CR to calculate delays due to the cyber-physical vessel attack, a critical first step to understanding econometric and supply-chain impact. While several experts in navigation and from $port_V$ verified the simulations, some of this information is publicly available and therefore there is less added risk when discussing the route. However, details of the network and $ship_C$'s systems are still kept private or have been obfuscated in some way. Discussions of findings will also obfuscate some details. Apart from accurately simulating the interactions between ship and port with or without various cyber-attacks, live data is extracted from the cyber range simulation in real time, and fed into the physical testbed. It is here where vessel systems are attacked to change valid rudder inputs, or drop valid inputs. While there is a known vulnerability, with a known CVE, that shows this attack is possible, doing the cyber-attack with real hardware in a secure network-isolated environment provides some additional verification.

3.2. NMEA Data

Previously it was mentioned that the case study's cyber-attack was able to modify ship data. More specifically, this manipulated NMEA (National Marine Electronics Association) data. As this data is being extracted from the simulator in real time, it is possible to get all the accurate headings, speed, Global Positioning

System (GPS) coordinates, and more, of $ship_C$ entering $port_V$. This can be fed into the ship equipment in the authors' testbed. NMEA is the primary electrical and specification for communication vessels. All of the network signals in Figure 3 use NMEA, between the compasses, AutoPilot, rudder control units, and sensors. This is typically the protocol used on the OT side on vessels, whereas SCADA is still more popular for port OT.

NMEA 0183, the replacement for the previous NMEA 0180 and 0183 standards, is still used. However, in many areas of the sector it is being phased out for NMEA 2000, which allows equipment to exchange data over a single backbone and is the current modern standard. As of 2014, however, there now exists a NMEA marine Ethernet standard. This uses Controller Area Network (CAN) technology that can co-exist with NMEA 2000. Organizations like the U.S. Coast Guard do not believe this will replace NMEA 2000/0183 [26], but it may still become more prevalent with future, possibly autonomous, builds based on its increased capacity for linking systems. By focusing on a known and documented vulnerability it can be shown, and validated with testbed experiments, that NMEA data can be used by malicious software to make decisions and influence physical behavior through the manipulation of data alone. As seen in Figure 3, these data readings and manipulations in a comprised PLC would happen between bridge and steering gears, making intrusion detection by conventional IT or Internet based solutions very difficult.

The average ship life span in the global fleet is roughly 20.3 years [27], meaning that there still exist ships that do not use Ethernet for marine equipment, and may not for several more years. Therefore, one advantage of using the physical hardware testbed is the ability to test the attack with different NMEA standards and systems. From these experiments, not all ships are vulnerable to this specific attack chain, but so far it has been possible to achieve similar effects with different attacks. However, that is outside the scope of this paper. A sample of NMEA strings extracted from the simulations are below, with coordinates changed to obfuscate exact physical location:

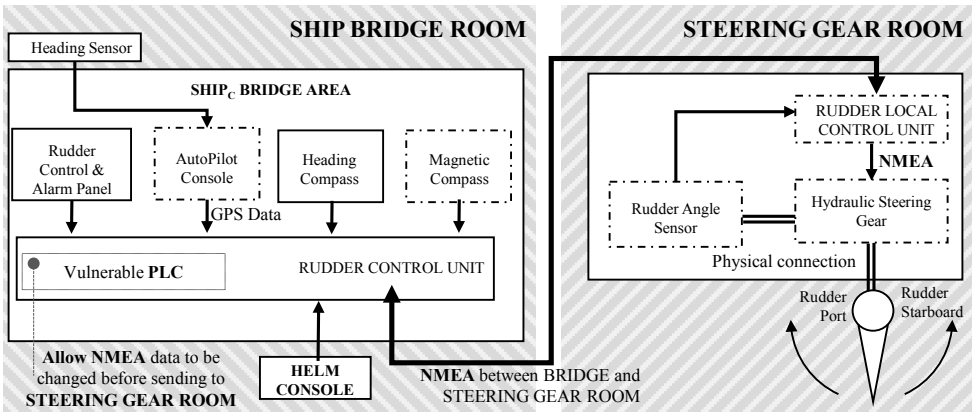

Figure 3. Simulated CR elements on the left in solid lined boxes, and physical hardware testbed on the right, with some hardware, shown with dotted boxes, on left side.

$GPGGA, 225444, 25.00000, N, 0035571.00000, W, 3, 25, 0.87, −37.50, M, 52.50, M, *7A;

$GPRMC, 225444, A, 25.00000, N, 0035571.000, W, 0.000, 90.000, 010221, 0.000, E, A, V*44;

$GPGNS, 225444, 25.00000, N, 0035571.00000, W, AN, 10, −37.50, 52.50, V*30;

$GPGLL, 25.00000, N, 0035571.00000, W, 121624, A*36;

$GPVTG, 90.000, T, 90.000, M, 0.000, N, 0.000, K*4E;

$GPGSV, 10, 1, 10, 2, 17, 87, 40, 10, 58, 68, 42, 15, 18, 146, 40, 16, 17, 322, 40, 1*62;

$GPGSA, A, 3, 02, 10, 15, 16, 18, 21, 24, 26, 29, 30, 1.4, 0.9, 1.1, 1*23;

$GPZDA, 225444.00, 01, 02, 2021, 00, 00*66;

$GPHDT, 90.000, T*0C.

3.3. Hardware Testbed

To better understand the global positioning system (GPS) data, please refer to the NMEA headers in Table 1. Once the vulnerability in a ship system is exploited as shown in our case study, the malicious PLC can alter certain message that are then be sent to the rudder mechanisms (see Figure 3 and Figure 4). To mitigate corrupted commands, NMEA does have a checksum at the end of each command; however, this can be easily forged. Several manufactures of ship equipment have their own proprietary NMEA 2000 compatible networks with unique names. However, for the purpose of this study, these will all be referred to as NMEA 2000, as they are semantically identical in this scenario. Details of the subsequent attack on the control unit, altered messages, and checksum are in Section IV-A. While the hardware testbed ($testbed_H$) is built with as many

Table 1. Relevant NMEA header and fields which all start with the $ symbol. Checksum is not included.

Header	Purpose
GPGGA	Global Positioning System Fix Data
GPRMC	Recommended minimum specific GPS/Transit data
GPGNS	GNSS capable receivers will always output this message with the GN talker ID
GPGLL	Geographic position, latitude/longitude
GPVTG	Track made good and ground speed
GPGSV	GPS Satellites in view
GPGSA	GPS DOP and active satellites
GPZDA	Date and time
GPHDT	Heading, True
HEHDT	Heading, True
IIXDR	Rudder sensor angle

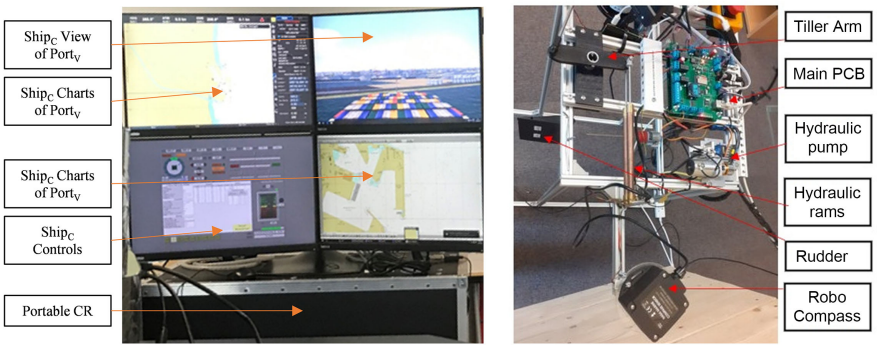

Figure 4. CR displays ontop of portable CR computers and servers on left, main rudder testbed components on right with some systems like ECDIS out of view for security purposes, and the "attacker's" computer.

off-the-shelf, and therefore real, marine systems as possible to replicate a number of ship bridges, there are limitations as the lab itself is stationary. Therefore, NMEA from the CR simulations can realistically drive these systems. While there are numerous NMEA simulators and generators available, to ensure the most realistic data and reactions, these experiments use a certified simulator from Wärtsilä, used to train professional seafarers globally.

As mentioned before, this includes a large suite of virtual assets and an accurate physics engines to simulate complex environments, situations and maneuvers. In particular, the authors are interested how the ship model would handle in restricted waters with accurate waves, currents, depths, wind, and obstacles both fabricated and natural. This includes general geographical topology, environmental conditions, vessel type (e.g., capacity, length, turning radius) and physical entrance to $port_P$. Simulations also include accurate tide and on-average weather patterns for CR's simulation date (*i.e.* day, month, year), which does have some effect on the cyber-physical outcomes. This can be varied for training and research. For this case study, $testbed_H$ consists of several real system found on-board $ship_O$, all connected with each other in a realistic manner, providing real-world vulnerabilities and reacting to a cyber-attack as accurately as possible in a lab environment (see Section VI). However, given the size of vessels and the ocean or port environments they often interact with, the simulation described earlier is required. In terms of related works, despite a vessel or port being a complex system-of-systems [28], there is less research on a realistic multi-system setup. Examples of complex systems include the power grids, oil pipelines etc., have all been well-researched [29]. While some solutions can be applied cross-sector, others cannot as ships have unique threats to consider [30] [31].

The developed $testbed_H$ hosts hydraulics systems, a rotating robotic compass platform, a rudder feedback unit, a scaled-down rudder with tiller arm, a custom designed NMEA interface, and off-the-shelf ECDIS with display (see **Figure 4**). The testbed is capable of interpreting NMEA sentences over a wide range of communication protocols, including the aforementioned Ethernet, RS232, RS422 and CAN (Controller Area Network) bus. Which systems communicate with NMEA and the direction of communications can be seen in **Figure 3**. In

this figure, it is also important to note that $testbed_H$ replicates the local rudder control unit that would normally be found in the steering gear room. With the bi-directional communication between bridge and steering, this feedback loop from rudder angle sensor into the autopilot/interpreter could potentially detect discrepancies between instructions and action taken by the rudder, and therefore an attack. However, as it is now, manipulations of NMEA introduced by the attack have not, so far, triggered any alarms in these systems throughout our experiments. This is explored in Section VI.

Both the rudder and rotating robotic compass system receive commands via the corresponding NMEA sentences received live from CR simulations, which are indistinguishable from a container ship actually entering the real port of Valencia. For realism, the robotic platform is also designed to faithfully spin the compass to match the simulated direction of the target ship (see **Figure 4**), and therefore produces real compass readings that are then fed into the other real marine systems in the testbed, like the ECDIS. A full hydraulics system was also employed, which was the closest alternative the authors could find to move the rudder on such a smaller scale.

4. Case Study Design

Previous sections have provided the background knowledge to illustrate how a CR with appropriate maritime simulation capabilities and a cyber-secure hardware testbed, when used together, can both simulate and accurately demonstrate how a cyber-attack can manipulate the rudder of a large vessel (390 plus meters, roughly 1280 feet). Now it is possible to show that this case scenario, which has been validated and tested with lab capabilities, can have significant negative consequences to physical and econometric safety. It has also been established that a ship of that type and size has entered the Port of Valencia in the recent past. Moreover, the geographic and terminal layout is known based on accurate charts and was confirmed by the port itself. Such contextual information is fed into both simulations and used to physically configure the hardware testbed. The following section will describe the general hybrid experiment operations, the actual firmware cyber-attacks, and the various outcomes of the simulations and testbed experiments.

The Wärtsilä [22] ship simulator runs in a standalone, portable, cyber range with 4 CPUs, 16 GB RAM, 3 computers and 2 servers. This makes it easier to isolate, and therefore, secure. The computer used for throughput simulation has a 2.6 GHz Intel Core i7 with 16 GB, 1600 MHz, and DDR3, although this is not discussed until Section V. These can also be seen in **Table 2**. All systems that are used for the cyber-physical attack are connected to an internal lab network to ensure no attack could affect systems outside the lab. While the uni-directional flow of data from the CR to the testbed means the simulation cannot be changed, it does mean there is no way for the testbed to negatively affect the realism of the simulation. The only data fed into the throughput simulations are information

Table 2. Hardware setup for experiments.

Cyber Range	$Testbed_H$	Throughput simulation
3 computers (4 CPU, 16 GB RAM)	ECDIS	MacOS Core i7
2 servers	COMPASS	16 GB 1600 MHz
Windows	Rudder & Thrusters	DDR3

of port goods and statistics, the rail and road connections in the terminals, and damage created with simulation, which is manually input into the throughput model. Therefore, there is no need to isolate the machine hosting the throughput model.

Case Study Scenario

With the scenario background and lab, it is now possible to explain the use of these for experiments and training. It is also possible to examine the resulting safety risks, and explore the cyber-attack that is the trigger for these concerns. This case study takes one known, high-risk, CVE case that could affect steering, but is one of many known such vulnerabilities [32] [33]. As discussed later in Section VI, it was necessary to remove the specifics of the CVE case, PLC make and model from the paper for security purposes. That said, there have been a number of PLCs in general that are vulnerable to firmware update attacks, and others, as shown in Section II. Past research shows that malicious firmware can cause a wide range of outcomes [33]. There are three stages to the attack: 1) Malicious firmware change; 2) Monitor $ship_C$ location; 3) Execute rudder change.

For the purpose of a plausible, awareness raising case study, the authors choose a supply chain attack to deliver the malicious firmware. This can be during upgrade services, or scheduled maintenance. There are other known methods of a malicious firmware update, however, this is useful for developing CR-based training and supply chain awareness exercises, of which there are not many despite existing threats [34]. For the second part of the attack, the now compromised device monitors NMEA traffic (see **Figure 3**). With the way $testbed_H$ mirrors a real ship bridge, the malicious software sitting in $testbed_H$ can see the GPS coordinates within the NMEA stream in real-time. To create a scenario where the software is isolated and does not require external control, the purpose-built malicious firmware is able to use geo-fencing or a countdown timer to define the physical entry of $port_V$ with GPS coordinates, and use that knowledge to decide when to begin actively manipulating NMEA data, instead of passively observing.

While geo-fencing is a possible trigger mechanism for an attack, although unlikely, this scenario has again been designed and optimized to best demonstrate various cyber-physical risks for short training, and awareness raising, scenarios. Based on previously established PLC and malicious firmware research, there is a possibility of a remote or manual trigger for these injections as well. The authors have also tested this possibility with some success. Therefore, there are other ways an attacker could attempt to trigger such an attack based on location, time,

or situation. However, the method chosen requires no external communication, making this malicious device a completely autonomous attacking agent. Unfortunately, this is then very difficult to detect via traditional IT methods that tend to be built on Internet packet analysis and operating system logs, demonstrating how security solutions need to develop more to address cyber-physical uses.

Although unlikely, a geo-fencing type of attack trigger is possible, as the NMEA strings for GPS coordinates are available, and geo-fencing has been proposed for ships to optimize fleet management in the past [35]. This deviates from past research focusing on communication to and from ships, and instead showcases an internal threat created by a supply chain vulnerability. This highlights supply chain and maintenance security concerns that are often left out [34], and the unique cyber-physical risks it can cause. This case study shows that the movements, position and even speed of a ship are equally relevant to understanding the threats, as knowledge of the underlying technology. In this case, triggering the rudder change as $ship_C$ enters a specific zone in $port_V$ gives the crew little time or space to react (*i.e.* small reaction window), increasing the chances of a major event, more so than if the attack were to happen at sea.

In general, this case study is a worst-case scenario, as it is unlikely that an attacker can get all these elements (*i.e.* supply chain, vulnerable PLC, perfect trigger) to work. Moreover, crew are able to physically bypass the rudder and steer completely manually. However, if crew are unable to act quickly, and the window to act is small, then an attack can still have severe consequences. Moreover, malware can be spread over multiple vessels, and only one needs to succeed to cause significant harm and damage. That is why the actual rudder hijacking, implemented in the $testbed_H$ but with effects played out in the CR for trainees, occurs at a critical point, to maximize the physical risk and potential harm for an awareness and training case. If this attack were to happen out at sea, while the vulnerability is still serious, there is likely to be less damage. It is also important to note that ships of $ship_C$'s size are often assisted by tugs in real life, and while they could mitigate the issue, that only shifts the safety risks to the tugs and their crews [36] instead of the wider port environment. Therefore, while the threat to safety, econometric cost and port throughputs may vary depending upon tug presence, actions, and capabilities, the overall risk to safety is still high, just either focused around the tugs or surrounding port and other ships [36].

There are actually multiple locations within $ship_C$ where the attack could be triggered with different outcomes and levels of threat to safety, see Section V for more, however at what exact points and at which specific rudder angles will not be discussed in detail, only in general terms. Once the compromised device starts to alter NMEA data, this can either change the angle of the rudder, or lock it. Both of these have been proven to be possible in the $testbed_H$, and both the physical rudder mechanism and the real ECDIS accept these altered packets as if they were genuine. With both methods of injecting and changing NMEA data established, it is important to explore what could be achieved with this access, and the negative cyber-physical outcomes that could occur as a result.

For injecting a custom rudder angle, two NMEA field values need to be changed, the numeric angle of the rudder (*i.e.*, −30 degrees for port, and 30 degrees starboard) and the two hexadecimal long checksum at the end of the string, following the * character. An example of a malicious rudder instruction can be found below, where 30.00 is the new angle instructed, and 4D is the new checksum to pass any potential error checks:

$IIXDR, G, 30.000000, RUDDER1, G, 0.000000, RUDDER2*4D.

Figure 5 shows one possible location and one possible rudder angle deviation. By varying the attack, *i.e.* trigger and angle, it is possible to create a range of safety risks and detrimental changes to port throughput. Variations in tug presence and tug actions also vary results. With this case study established, it is now possible to discuss the range of outcomes, and the types of training and solutions that can be used or created, without releasing specific details on system vulnerability, route, and rudder angles to provide some security to the authors' findings.

5. Results and Findings

It is worth discussing the human element of this scenario more before examining the physical and digital results. A ship engineer did say that engineering crew is able to bypass any compromised systems and insert a physical wheel directly onto the steering gear as a manual override. However, it was also said that it would likely take ten or more minutes to detect drift, and in this case, that has proven to be enough time to still cause harm. That said, a few experts have mainly theorized this, and now that this case study is a repeatable training scenario on a portable CR, that could be taken to other training locations, future work will look at subjecting a number of crews to this scenario and building statistics around their reactions. As discussed in Section VII, this will be a useful extension to this work by finding and addressing gaps in training. That said, even with the limited validation testing during this study to ensure realism, there have been variants of the simulated scenario where, even if an experienced crew knew the attack was happening, it was difficult to prevent damage due to the position and inertia of $ship_C$ and the layout of $port_V$.

5.1. Physical

In terms of biggest disruption to port operations, there is one scenario variant that caused the ship to block the entire container terminal of $port_V$. During simulations, $ship_C$ and its cargo was also often physically damaged. If this were to happen in real life, a cleanup of its surroundings would be needed to regain optimal operational efficiency. In the simulation variations, however, it is important to note that causing enough damage to sink $ship_C$ was highly unlikely, as was triggering a significant fire onboard. However, some containers could be shaken loose and fall off, and discussion with the port has informed our throughput model how long re-floating cargo and/or $ship_C$ would delay a return to normal operations.

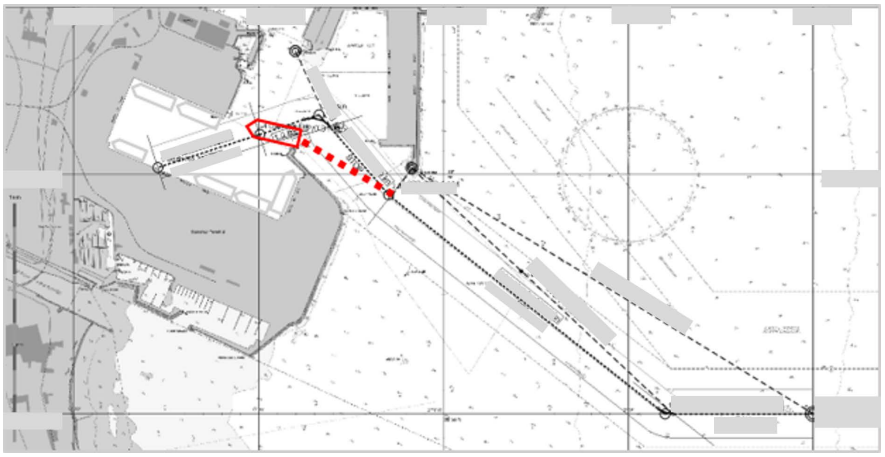

Figure 5. Example of route change based on NMEA alterations of rudder instructions. Positions are obfuscated.

The change in rudder could be physically observed by surrounding vessels (including tugs) and those on $ship_C$ may realize that the rudder is unresponsive or acting erroneously. However, with this very specific port and ship, many of the variations in attack inflicted a minor deviation to the rudder angle ($R\theta$). If there is a limited rudder angle change ($\delta R\theta$) that is difficult to detect through observations (lim_{Obs}), then for any of the case study cyber-attacks (a) in $ship_C$, the difference in rudder angle movements ($\delta R\theta$) is often less than what the limit of change that is easily observed (im_{Obs}). Again, this may not be true in other port or water entryways. With a range of 5 - 10 case study variants, the range of downtime to the port ranged from half a day to six days. Again, this takes the case study and realistically varies the point of attack, the cyber-attack action (*i.e.* rudder compromise), presence of tugs, and crew reaction. This has varied the percentage of throughput decrease, as some variants either fully, partially, or did not block the cargo entrance. Simulations also take into account connecting railways and road when appropriate to the port, which can lead to a larger overall transport view.

To begin understanding the wider physical effect on the transportation supply chain, the authors take $port_V$ data and case study downtimes and integrate them into a model. The details of this are outside the scope of this paper, but the model analyses port container operations using discrete event simulation techniques. Instead, this paper only focuses on using this model to calculate downtimes [37] [38], and not the mathematics involved. For background however, this model uses the MATLAB [39] platform using the *simevents* and *simulink* packages. This makes the ability to adjust the port throughput simulation to the situation in the ship simulator more valuable and the results of port delays are more granular. Knowledge of port repair and recovery operations, and the tools required to do, are also important to understand time to recovery if containers are submerged or floating. However, that level of detail is not considered in this scenario, and instead an average window of repair or recovery is used.

The port throughput simulation is a queue based model which models the high level operations of a port such as the unloading/loading of cargo, intra-port transport and container yard operations. The main parameters used to inform the modelling process include: 1) The number of vessels serviced by the port of Valencia during the entire year of 2020; 2) The mean duration it takes to service each vessel; 3) The proportion of land-based transport which is rail or truck based; 4) The mean dwell time of containers on the yard.

Vessel arrival times are modelled as following a poisson distribution and service time distributions are modelled as following an Erlang distribution, this is consistent with the traffic and service distributions usually experienced in ports and is consistent with the recommended distributions that UNCTAD recommends are assumed for port planning purposes. Details of this simulation are outside the scope of this paper, but the outputs are critical for understanding the scenario outcomes.

Figure 6 and Figure 7 show the service durations and the vessel wait times which could be experienced if the port suffers a complete blockage disruption that spans six days. This is around the upper limit of disruption that is estimated as being possible as per the scenario discussed in this paper. Each unit of time in the graphs corresponds to 15 minutes. The service duration graph shows the extent to which vessels would be severely disrupted by port operations halting. The time it would take for the most severely affected vessels to be serviced would increase from an average of one day to as much as eight days (six of those days would be spent waiting for port operations to open up, causing congestion and

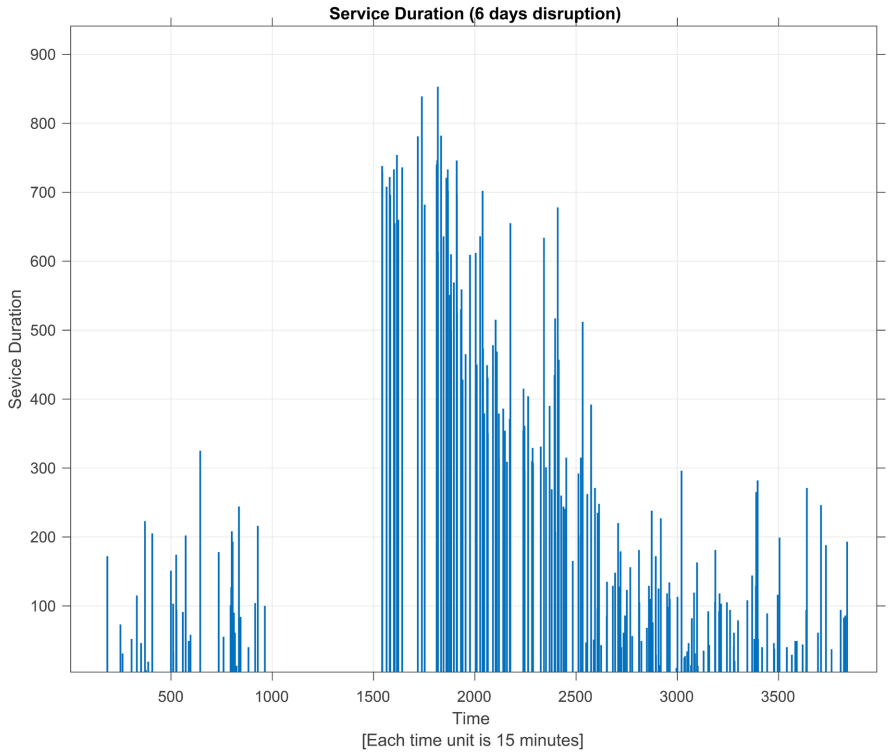

Figure 6. Service duration vs vessel depart time.

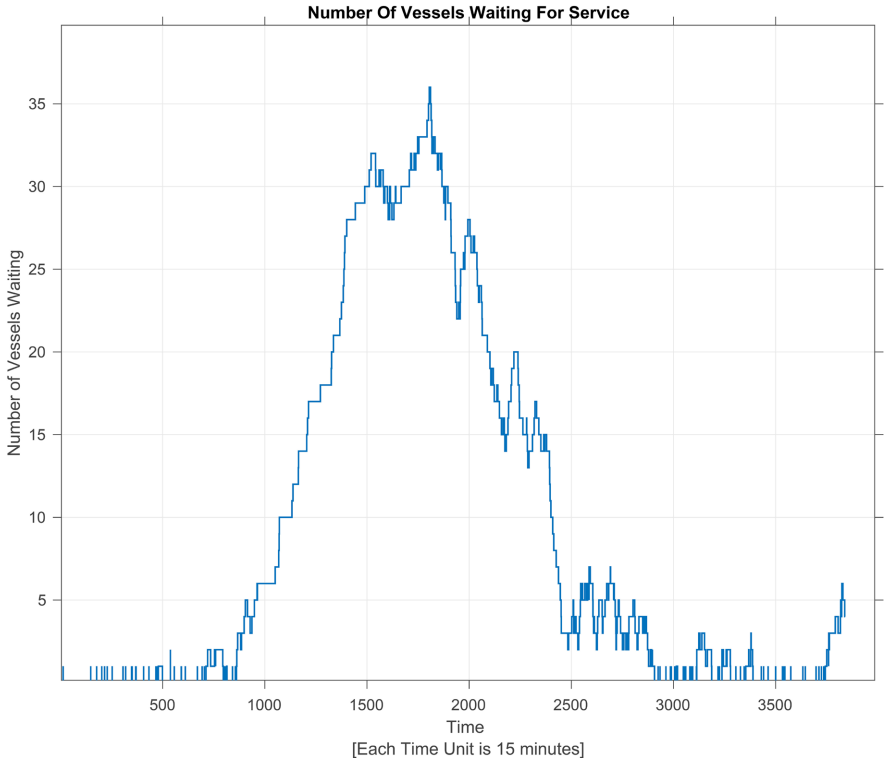

Figure 7. Number of vessels waiting vs time.

pollution near the port). The number of vessels waiting would also rise to over 35 vessels at its peak. This is assuming that the disruption occurs at a period of time when the port is experiencing an average amount of traffic, based on the date of simulation. If the disruption occurs at periods of time when the port is especially busy, then the disruption caused could be greater than the estimates in **Figure 6** and **Figure 7**. In terms of physical safety, in several case study variants the hull of $ship_C$ was damaged in some way, and in some cases it was possible that cargo may slide or even come off in the higher-impact variants. Safety of the crew and those on shore are also at risk, although the risk to those on shore may be re-assigned to those operating tugs, if they are present. With the date of the simulation there is little safety jones concerns of $ship_C$ colliding with other incoming or outgoing vessels, cargo, cruse, or any other type. However, is it possible that a different date would have more or less congestion at $port_V$, which would affect both other ship safety, and throughput.

5.2. Digital

Several aspects of this case study, while plausible and with real cyber-attacks demonstrating that these are possible, the likelihood of the worst-case scenario is unlikely. With the cyber-attack being designed as a supply chain attack, and with no external communication, this is also an unusual case for traffic it produces. Other variants would also be much easier to detect with existing detection software and mechanisms or even by crew.

Previous work affected visuals on the bridge [14] and this would be a clear indication that something had gone wrong. This makes human-based detection difficult, especially when the changes in the rudder angle are subtle. As nothing malicious, firmware or communication packets, ever enters the bridge during this scenario, any protection or detection software located in the bridge would be ineffective. There is little digital footprint or visible symptoms associated with this case study, as it was designed to be. This again is a useful training scenario, one that can be repeated in the cyber range. Sections on both mitigation and future work will explore this in more detail.

6. Discussions

This case study is not purely theoretical, but the parts that are, are validated and based on existing vulnerabilities (e.g. CVEs) and research. This led us to a plausible, yet difficult to detect, supply-chain and PLC firmware attack that could compromise a large container ship's rudder. While the threat may exist, a significant question to answer was, how much of a safety risk could one device on one ship inflict on the surrounding port and transportation links? With variations in the case study, it was also possible to establish a range of port downtime and range of risk to safety. With the combination of a cyber range (CR) with scenario simulations and hardware testbed, it is possible to repeat the scenario with small changes, which is also good for training the people to recognize, and react to, this cyber-physical attack. In summary, this case study highlighted some cyber-physical threats to:

1) Threat to crew: in scenario variants where collision occurs and with enough force to cause damage, crew safety is a concern;

2) Threat to port: in scenario variants where the ship collides with different zones of port, different levels of damage can be realized;

3) Threat to other vessels: in scenario variants where tugs are attempting to regain control or there is traffic, other vessels' safety may be in danger as a result;

4) Threat to supply chain: in all scenarios some delay is introduced, however some can cause significant delay, but also require clean-up time.

This following section will discuss these threats further while addressing, or re-addressing, several ethical and legal concerns. New protection, detection, and training solutions for these threats to safety are also proposed. Lastly, limitations and future work are discussed.

6.1. Ethical and Legal Concerns

Some of the data on ships entering into ports are publicly available through AIS databases and websites. While this is true, details on heading, rudder angle, speed, and specific coordinates of a large container ship are removed from the images and not explicitly shown in this paper. However, these details are within the CR simulations as they are critical for calculations, just not published for security purposes. Similarly, details of the large container ship are not explicitly

shared here, except for a rough length, even though that is also somewhat publicly available. Again, the CR simulation is based on a real container ship, but specifics are not shared here. This is to obfuscate details of certain classes of ships that could be vulnerable to a real attack. Lastly, the make and model of specific systems in $testbed_H$ are obfuscated for the purpose of publication, as well as the CVE used in the cyber-attack.

While all CVEs are public, naming the CVE could lead to dangerous situations. One detail the authors will disclose is that the CVE was judged to have an extremely high risk, especially since it was easy to exploit with high safety-risking consequences. The Port of Valencia is known to be working on this research based on public records of project funding, so there was little reason to obfuscate the port being used, but again NMEA messages with highly accurate positions for the ship are obfuscated as those details could be mis-used. Lastly, to obfuscate the most damaging points to trigger the attack and what the attack looks like, this case study also uses case study variants to put upper and lower limits on the delays and risks to safety possible with this scenario.

6.2. Future Protections and Solutions

There are several mitigation solutions that could prevent this scenario, and variants thereof, from occurring in real life. These can be categorized as intrusion detection systems (IDS), supply chain security, System-of-System pen-testing and audit tests, training, and hardware enforced security.

Firstly, IDS is a significant part of this research. When there are no visual symptoms to a cyber-attack, the ability for a trustworthy computing device to monitor digital activity of malicious behavior is critical. However, most off-the-shelf IDS solutions would not work to detect the attack proposed, based only on the fact that NMEA sentences are manipulated instead of Internet communications.

NMEA does provide a simple checksum method, which was introduced to identify errors, and in this case manipulations, in the data. However, this is a simple calculation, just XOR all of the bytes between two delimiters at the start and end of each string, and written in hexadecimal. Furthermore, our experiments showed that it was possible to inject data and a new valid checksum in a manner that could not be detected and resulted in us hijacking the rudder. Therefore, a way to mitigate this threat is to strengthen the NMEA checksum security with a more cryptographically secure hash or signature, and to insert more NMEA sentence checks at critical points in a vessel's SoS. Recent works that have tried to improve both of these and, if widely adopted as good and secure practice, would provide additional protection [40] [41]. In Section VII, future work on ship IDS will be explored, as there is not a lot of solutions that could be directly applied today.

In addition, enforcing software solutions with additional hardware, particularly for attacks low in PLC's like firmware, are also possible [32] [42]. As an example of adding or changing a system, a number of firewalls that were intro-

duced into $testbed_H$ were able to stop altered packets. This included a Hensoldt firewall. This does not mean that others were found vulnerable, as not all possibilities were tested. However, a working firewall alone is not a sufficient solution, as editing NMEA sentences could still result in a denial of service attack if the firewall will then prevent all rudder changing commands. More on this in the future works section.

Supply chain security is another critical part of protecting ships in general. As various vessel and port components are produced globally, and the lifetime of a ship means many systems are expected to have long life-cycles, acquiring parts and servicing those parts are critical aspects of supply chain security. However, even if a ship runs for twenty plus years, it is likely that some systems will be upgraded due to failures, changes in regulations, or to reduce various physical and cyber risks. Therefore, the security of the supply chain and the wider system-of-systems is critical. This issue is what the $testbed_H$ was designed to study and provide solutions, which is explained more in Section VII.

While physical testbeds are useful, for the reason our hybrid approach included simulation, it is also important to add and refine existing capabilities to existing simulation software to simulate cyber-attacks in a safe manner. Using these solutions together helps negate the drawbacks of each and provides a more multi-disciplinary and broader understanding of the issues. The port throughput simulations were an example of simulating physical effects of an attack, after they were tested and verified to work on the real hardware, without negatively affecting a port.

A significant reason for using a CR is that simulating the symptoms of ship and port cyber-attacks has been critical in training both security and seafarer professions in maritime cyber-threats (see Section VII for details). A realistic scenario that is re-playable in simulation creates a safe and effective way to train people [13] [43]. In the scenario variants where a faster reaction time could reduce safety risk and damage, this training is critical. In variants where crews were aware of the attack from the start of the exercise, training is a less effective solution, and so both technical solutions and training would be needed to prevent every scenario variant.

Lastly, updated regulations from bodies such as the International Maritime Organization (IMO) could greatly improve the cyber-security of a ship, as it has done for physical security for decades. In addition, understanding how to protect ports from vulnerable ships could strengthen security of the wider transportation connections rather than segmenting ships from ports. The experiments in this were novel in that sense, whereas most previous research (as discussed in Section II) into maritime cybersecurity have focused on one system, only ships, or only ports.

6.3. Training

As the previous sections have mentioned, the use of this particular testbed and CR, along with scenario variations, offers a good source of training material.

This training material provides a broad understanding of the cyber-physical risks within the sector, as well as offers a way to enhance core skills, like the ability to recognize and respond to a cyber incident. International Maritime Organization Resolution MSC.428(98) [44] stipulates that an approved safety management system should provide for the continuous improvement of safety management skills of personnel on board ships and ashore. Currently, the IMO's International Convention on the Standards of Training, Certification and Wathckeeping does not explicitly mention digital skills [45]. However, to fulfil the obligation of ensuring personnel are qualified, and fit for their duties, cyber skills must be developed.

The adoption of a testbed and CR like the ones discussed in this paper offers a way to address this growing need, and being able to run the same scenario with different types of personnel, not just seafarers, provides the opportunity for all in the sector to experience a "real" cyber incident. As [46] argues, the use of simulators, such as the one presented here, allows trainees to practice skills, and implement knowledge in a safe environment. The use of digital environments also adds repeatability into the training space. During cadet training, cadets spend time at sea on board vessels during real operations. This process means that cadet experiences are limited to what actually happens during their time on board, and will differ person to person depending on their placement. However, with simulation, it allows all cadets to have as close to "real-world" experiences as possible. What is more, they can also experience the same scenario multiple times, giving rise to the opportunity to learn from their mistakes, and work with others to overcome them. A quality that is not possible with traditional sea time.

Another skill that is vital for ensuring the continued safety of maritime infrastructure is communication. During academy training cadets spend time working with other mariners, in the classroom or at sea. These experiences teach them the skills required to communicate basic information with other bridge crew, or port operatives. However, because of the complex nature, and lack of technical skills and understanding personnel are ill-prepared to communicate with technical shore side staff about cyber risks. As [47] argues, effective communication is vital in a cyber-incident as it allows individuals to: 1) Assess what is happening, otherwise known as situational awareness; 2) Locate who or what is at risk; 3) Automate those personnel who need to act; 4) Notify what actions those personnel need to take. Simulator training could offer a unique opportunity for trainees to learn how to communicate cyber-physical safety concerns with those around them. Running these scenarios with a mixture of maritime personnel including: seafarers, port operatives, IT support and senior management, will illustrate what information needs to be shared, and how best it is shared. This may also be useful for other sectors concerned about cyber-physical.

6.4. Limitations

While this article's experiments are based on a realistic sequence of events in a realistic environment, the ability to do such a detailed deep-dive into the physi-

cal and cyber characteristics of a single ship and port, is a limitation in a way. There are many other types of ships with different cyber-vulnerabilities [4], and only container ships are considered in this case study. While shipping is significant to the global economy and supply chains, other ships are just as critical to provide fuel (e.g., oil tankers), food (e.g., fishing), or transportation (e.g. cruise ships). Moreover, while most modern ships will have PLCs integrated into the steering and propulsion systems, not all will have the specific PLC tied to the CVEs of the proposed attack. Therefore, this vulnerability is not likely to affect all ships, and may not have the same cyber-physical outcome depending on what any vulnerable PLC is in control of. Similarly, the simulator is capable of looking at all sea areas and loading any ship into that environment, but only one port was chosen for this scenario. Furthermore, simulations all happened on only one day of the year.

A significant limitation was not being able to send altered NMEA data back into the simulator, requiring the authors' to compare multiple simulations with and without the attack. Looping NMEA altered sentences back into the simulation would have allowed the observers to see the ship model react to the real hardware attack much more easily. While the authors were able to manually adjust the simulations to match the physical hardware under attack, the manual adjustment is not ideal for creating training without a trained instructor. To an extent, this limits the technical contribution; however, the case study and discussions on safety risks have not been limited. This does not reduce the importance of understanding the effect this has on crew, but is outside of the scope of this particular paper. Future work can improve CR simulators and work with providers of simulation software for more cyber-physical scenarios. For the purpose of this study, there are few limitations to $testbed_H$ as its only function was to provide an accurate ship SoS to be compromised and physically show the effect on the rudder. Any performance overhead introduced would not affect the simulation, as there is no loop for manipulated message to be injected back into the CR. This would need to be more closely monitored if that were to change however.

One limitation to the throughput simulation, which is completely separate from the cyber range simulations, is that it only calculated delays to container goods, and did not consider throughput changes to the passenger terminal. This one of several planned areas for future work.

7. Future Work

While the simulated part of the case study was replayed for a number of audiences, the purpose of this work was to produce a number of realistic, and re-playable, case study variations. Now this suite of simulations exists, future research can examine how useful these are in training crew and others in the maritime sector to understand and recognize non-traditional cyber-physical threats. It would also be possible to better assess their perception on safety threats as the

various scenarios are played out, and time their reactions before and after training. In most cases, but particularly those cases where even knowing the cyber-attack was happening was not enough for people to prevent it, new IDS is needed. While still somewhat new, intrusion detection for connected cyber-physical systems is a new and growing area of research [48], however much of the focus has been on-land infrastructure (e.g. smart grids). As shipping moves 90% of goods globally, and as the effects of COVID have shown, more attention needs to be on robust maritime transportation [49]. Moreover, as this case study hopes to illustrate, future research cannot only focus on ports. Regarding the testbed, the more real systems integrated into it, the more realistic case studies will be, and the range of scenario variants will be larger.

In addition, if more software or hardware solutions are created to stop these types of attacks, it would be beneficial to also add these to the testbed to verify that they would detect or even prevent altered NMEA sentences. Ongoing work is also being done to more easily configure the testbed to mirror different ship types, so that it could realistically also be used for cruise ship scenarios, just as one example. Creating a suite of multiple possible attacks to then audit test solutions on this testbed, is also ongoing work to improve the capabilities of $testbed_H$. This would be essential in allowing a number of users, not all security experts, to use the testbed as well as the cyber range for a number of training and solution testing exercises.

For understanding even wider impact, working with algorithms on the econometric effects of natural disasters (e.g. floods) to understand the potential cost of an attack could be useful for informing businesses [38]. This is also a part of ongoing work built on top of the case study in this and other papers. Future work also includes looking at more cyber-physical threats from port to ship, ship-to-ship, and people to either ship and/or port to fully scope out cyber-vulnerabilities that can lead to physical safety threats.

8. Conclusions

Cyber-security is an ever-growing concern as more technology is adopted into everyday operations, including transportation. While this brings significant improvements to monitoring and controlling devices, there is a concern that they increase the likelihood of a cyber-attack. In this article, a case study was used to further explore the potential risks to physical safety a cyber-attack could have. More specifically, it looks at transportation and examines how the cyber vulnerabilities in one entity, *i.e.* a ship, could actually affect the safety of those around it.

Therefore, even if a port were to remove all cyber-vulnerabilities, it could still be negatively affected by a cyber-physical attack on an entity in its environment. This study also uses a novel CR range to create a real training scenario for maritime cyber-security, and uses a hardware testbed to validate and physically demonstrate the effects of the cyber-physical attack. Simulations of how the port throughput is reduced as the result of this attack are also provided, to better

communicate the range and length of effects a cyber-physical attack can have in shipping. This work will be the basis of future work in maritime cybersecurity training, security solutions, and raising awareness on the possible threats, digital and physical, as technology in maritime transportation evolves.

Acknowledgements

This paper is partly funded through the research efforts under Cyber-MAR. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 833389. The content reflects only the authors' view, and the European Commission is not responsible for any use that may be made of the information it contains. Some parts were also funded by the Cyber-SHIP project (Research England). The authors' would also like to thank the wider Maritime Cyber Threats Research group including Paul T., and Tim D. from the Navigation team for all their valuable contributions.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Höyhtyä, M., Huusko, J., Kiviranta, M., Solberg, K. and Rokka, J. (2017) Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges. 2017 *International Conference on Information and Communication Technology Convergence*, Jeju, 18-20 October 2017, 345-350. https://doi.org/10.1109/ICTC.2017.8191000

[2] Tam, K. and Jones, K. (2018) Cyber-Risk Assessment for Autonomous Ships. 2018 *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow, 11-12 June 2018, 1-8. https://doi.org/10.1109/CyberSecPODS.2018.8560690

[3] Yağdereli, E., Gemci, C. and Aktas, A.Z. (2015) A Study on Cyber-Security of Autonomous and Unmanned Vehicles. *The Journal of Defense Modeling and Simulation*, **12**, 369-381. https://doi.org/10.1177/1548512915575803

[4] Tam, K. and Jones, K. (2019) Macra: A Model-Based Framework for Maritime Cyber-Risk Assessment. *WMU Journal of Maritime Affairs*, **18**, 129-163. https://doi.org/10.1007/s13437-019-00162-2

[5] Ramos, K., Rocha, I., Cedeño, T.D.D., dos Santos Costa, A.C., Ahmad, S. Essar, M. and Tsagkaris, C. (2021) Suez Canal Blockage and Its Global Impact on Healthcare Amidst the Covid-19 Pandemic. *International Maritime Health*, **72**, 145-146. https://doi.org/10.5603/IMH.2021.0026

[6] Doumbia-Henry, C. (2020) Shipping and Covid-19: Protecting Seafarers as Frontline Workers. *WMU Journal of Maritime Affairs*, **19**, 279-293. https://doi.org/10.1007/s13437-020-00217-9

[7] Valenciaport (2020) Statistical Report December 2020. https://www.valenciaport.com/wp-content/uploads/Statistical-Report-December-2020-NF.pdf

[8] Tam, K., Moara-Nkwe, K. and Jones, K. (2021) A Conceptual Cyber-Risk Assessment of Port Infrastructure. 2021 *World of Shipping Portugal, An International Research Conference on Maritime Affairs*, Parede, 28-29 January 2021, 1-22.

[9] Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A. (2021) Beware Suppliers Bearing Gifts!: Analysing Coverage of Supply Chain Cyber Security in Critical National Infrastructure Sectorial and Cross-Sectorial Frameworks. *Computers and Security*, **108**, Article ID: 102324. https://doi.org/10.1016/j.cose.2021.102324

[10] BBC News (2021) Hacker Tries to Poison Water Supply of Florida City. https://www.bbc.co.uk/news/world-us-canada-55989843

[11] Turton, W. and Mehrotra, K. (2021, June 4) Hacker Tries to Poison Water Supply of Florida City. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[12] Tam, K., Forshaw, K. and Jones, K. (2019) Cyber-Ship: Developing Next Generation Maritime Cyber Research Capabilities. *International Conference on Marine Engineering and Technology Oman* 2019, Muscat, 5-7 November, 129-135. https://doi.org/10.24868/icmet.oman.2019.005

[13] Tam, K., Moara-Nkwe, K. and Jones, K. (2020) The Use of Cyber Ranges in the Maritime Context: Assessing Maritime-Cyber Risks, Raising Awareness, and Providing Training. *Maritime Technology and Research*, **3**, 16-30. https://doi.org/10.33175/mtr.2021.241410

[14] Mass Soldal, L., Hareide, O.S. and Jøsok, Ø. (2018) An Attack on an Integrated Navigation System. *USENIX Security Symposium*, Baltimore, 15-17 August 2018, Submitted.

[15] Pavur, J., Moser, D., Strohmeier, M., Lenders, V. and Martinovic, I. (2020) A Tale of Sea and Sky on the Security of Maritime VSAT Communications. 2020 *IEEE Symposium on Security and Privacy*, San Francisco, 18-21 May 2020, 1384-1400. https://doi.org/10.1109/SP40000.2020.00056

[16] Costin, A. (2016) Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. *Proceedings of the* 6*th International Workshop on Trustworthy Embedded Devices*, Vienna, 28 October 2016, 45-54. https://doi.org/10.1145/2995289.2995290

[17] Avatefipour, O. and Malik, H. (2018) State-of-the-Art Survey on In-Vehicle Network Communication (Can-Bus) Security and Vulnerabilities. arXiv: 1802.01725. http://arxiv.org/abs/1802.01725

[18] Sandaruwan, G.P.H., Ranaweera, P.S. and Oleshchuk, V. A. (2013) Plc Security and Critical Infrastructure Protection. 2013 *IEEE 8th International Conference on Industrial and Information Systems*, Peradeniya, 17-20 December 2013, 81-85. https://doi.org/10.1109/ICIInfS.2013.6731959

[19] Svilicic, B., Brčić, D., Žuškin, S. and Kalebić, D. (2019) Raising Awareness on Cyber Security of Ecdis. *TransNav*: *The International Journal on Marine Navigation and Safety of Sea Transportation*, **13**, 231-236. https://doi.org/10.12716/1001.13.01.24

[20] Balduzzi, M., Pasta, A. and Wilhoit, K. (2014) A Security Evaluation of AIS Automated Identification System. *Proceedings of the* 30*th Annual Computer Security Applications Conference*, New Orleans, 8-12 December 2014, 436-445. https://doi.org/10.1145/2664243.2664257

[21] C4ADS (Center for Advanced Defense Studies) (2019) Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. Technical Report, Center for Advanced

Defense Studies, Washington DC.

[22] Wärtsilä (n.d.) https://www.wartsila.com/

[23] Davis, J. and Magrath, S. (2013) A Survey of Cyber Ranges and Testbeds Executive. Defence Technical Information Center, Fort Belvoir.

[24] Yamin, M.M., Katt B. and Gkioulos, V. (2020) Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*, **88**, Article ID: 101636. https://doi.org/10.1016/j.cose.2019.101636 https://www.sciencedirect.com/science/article/pii/S0167404819301804

[25] Qassim, Q., Jamil, N., Zainal Abidin, I., Rusli, M., Yussof, S., Ismail, R., Abdullah, F., Ja'afar, N., Hasan, H. and Daud, M. (2017) A Survey of SCADA Testbed Implementation Approaches. *Indian Journal of Science and Technology*, **10**, 1-8.

[26] Saftey4Sea (2012) National Marine Electronics Association Introduces Onenet. https://safety4sea.com/national-marine-electronics-association-introduces-onenet/

[27] International Chamber of Shipping (2016) Review of Maritime Transport. United Nations Conference on Trade and Development (UNCTAD), Geneva.

[28] Boardman, J. and Sauser, B. (2006) System of Systems—The Meaning of of. 2006 *IEEE/SMC International Conference on System of Systems Engineering*, Los Angeles, 24-26 April 2006, 6. https://doi.org/10.1109/SYSOSE.2006.1652284

[29] Sridhar, S., Hahn, A. and Govindarasu, M. (2012) Cyber-Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, **100**, 210-224. https://doi.org/10.1109/JPROC.2011.2165269

[30] Ray, C., Gallen, R., Iphar, C., Napoli, A. and Bouju, A. (2015) Deais Project: Detection of AIS Spoofing and Resulting Risks. *OCEANS 2015*-Genova, Genova, 18-21 May 2015, 1-6. https://doi.org/10.1109/OCEANS-Genova.2015.7271729

[31] Hambling, D. (2021) UK Ship Hit by GPS Spoof. *NewScientist*, **250**, 17. https://doi.org/10.1016/S0262-4079(21)01131-3 https://www.sciencedirect.com/science/article/pii/S0262407921011313

[32] Govil, N., Agrawal, A. and Tippenhauer, N.O. (2018) On Ladder Logic Bombs in Industrial Control Systems. *International Workshop on Security and Privacy Requirements Engineering* 2017, Oslo, 14-15 September, 110-126. https://doi.org/10.1007/978-3-319-72817-9_8

[33] Basnight, Z., Butts, J., Lopez, J. and Dube, T. (2013) Firmware Modification Attacks on Programmable Logic Controllers. *International Journal of Critical Infrastructure Protection*, **6**, 76-84. https://doi.org/10.1016/j.ijcip.2013.04.004

[34] Boyson, S. (2014) Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical It Systems. *Technovation*, **34**, 342-353. https://doi.org/10.1016/j.technovation.2014.02.001 https://www.sciencedirect.com/science/article/pii/S0166497214000194

[35] Reclus, F. and Drouard, K. (2009) Geofencing for Fleet & Freight Management. 2009 9*th International Conference on Intelligent Transport Systems Telecommunications* (*ITST*), Lille, 20-22 October 2009, 353-356. https://doi.org/10.1109/ITST.2009.5399328

[36] Talley, W.K., Jin, D. and Kite-Powell, H. (2005) Determinants of Crew Injuries in Vessel Accidents. *Maritime Policy & Management*, **32**, 263-278. https://doi.org/10.1080/03088830500139760

[37] Kotachi, M., Rabadi, G. and Obeid, M.F. (2013) Simulation Modeling and Analysis of Complex Port Operations with Multimodal Transportation. *Procedia Computer Science*, **20**, 229-234. https://doi.org/10.1016/j.procs.2013.09.266

https://www.sciencedirect.com/science/article/pii/S1877050913010661

[38] CyRiM (Cyber Risk Management) (2019) Shen Attack: Cyber Risk in Asia Pacific Ports. https://assets.lloyds.com/assets/pdf-cyrim-shen-attack-final-report/1/pdf-cyrim-shen-attack-final-report.pdf

[39] Mathworks (2019) Matlab. https://www.mathworks.com/help/rptgen/ug/create-links.html

[40] Agarwal, A. and Cohn, D. (2020) A Novel Data Acquisition Solution to Expedite Global Oceanographic Research. *Global Oceans* 2020: *Singapore-U.S. Gulf Coast*, Biloxi, 5-30 October 2020, 1-6. https://doi.org/10.1109/IEEECONF38699.2020.9389328

[41] Kessler, G. (2020) Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *TransNav*: *International Journal on Marine Navigation and Safety of Sea Transportation*, **14**, 279-286. https://doi.org/10.12716/1001.14.02.02

[42] Kuruvila, A.P., Zografopoulos, I., Basu, K. and Konstantinou, C. (2021) Hardware-Assisted Detection of Firmware Attacks in Inverter-Based Cyberphysical Microgrids. *International Journal of Electrical Power and Energy Systems*, **132**, Article ID: 107150. https://doi.org/10.1016/j.ijepes.2021.107150

[43] Pham, C., Tang, D., Chinen, K.-I. and Beuran, R. (2016) CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. *Proceedings of the Seventh Symposium on Information and Communication Technology*, Ho Chi Minh City, 8-9 December 2016, 251-258. https://doi.org/10.1145/3011077.3011087

[44] International Maritime Organization (2017) Resolution MSC.428(98)-Maritime Cyber Risk Management in Safety Management Systems.

[45] International Maritime Organization (2016) International Convention on Standards of Training, Certification and Watchkeeping. International Maritime Organization, London.

[46] Kobayashi, H. (2005) Use of Simulators in Assessment, Learning and Teaching of Mariners. *WMU Journal of Maritime Affairs*, **4**, 57-75. https://doi.org/10.1007/BF03195064

[47] Hawkins, H. (2017) Why Communication Is Vital during a Cyber-Attack. *Network Security*, **2017**, 12-14. https://doi.org/10.1016/S1353-4858(17)30028-4 https://www.sciencedirect.com/science/article/pii/S1353485817300284

[48] Mitchell, R. and Chen, I.-R. (2014) A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Computing Surveys*, **46**, Article No. 55. https://doi.org/10.1145/2542049

[49] Lund, M., Gulland, J., Hareide, O.S., Josok, E. and Weum, K. (2018) Integrity of Integrated Navigation Systems. 2018 *IEEE Conference on Communications and Network Security*, Beijing, 30 May-1 June 2018, 1-5. https://doi.org/10.1109/CNS.2018.8433151