Seeing is Believing – a Practical Study of Cyber Attacks on a Ship Navigation Bridge

Frederik Basels°, Philipp Sedlmeier•, Elmar Padilla°, Jan Bauer°

°Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

•Fraunhofer CML
Ship and Information Management
Hamburg, Germany

{frederik.basels, elmar.padilla, jan.bauer} @fkie.fraunhofer.de
philipp.sedlmeier@cml.fraunhofer.de

***Abstract*—The maritime transportation system is the backbone of global trade and the economy. At the same time, the legacy IT and communication systems onboard modern cargo ships with their integrated bridge systems are increasingly vulnerable to cyber attacks, as researchers have repeatedly demonstrated. Despite the growing threat, progress on securing maritime systems remains slow. One major obstacle is the protracted standardization process, which delays the deployment of effective countermeasures. Another, however, is the limited awareness – and resulting inaction – among maritime stakeholders regarding the potentially fatal impact of cyber attacks on bridge systems and navigation decisions. In this paper, we therefore compile known academic cyber attacks targeting ship IT and apply them to a representative, real-world ship navigation bridge to highlight its vulnerabilities and raise stakeholder awareness. We also share insights and lessons learned from our implementation.**

***Index Terms*—Maritime Cyber Security; Security Testing Automation; Integrated Navigation System; IEC 61162-450; NMEA 0183**

I. Introduction

In today's globalized world, ships play a crucial role in the movement of goods around the globe, transporting over 80% of world trade by volume [1]. Due to complex logistics and production chains, even small delays can cause high costs to all involved parties. Single accidents can even impact the global economy, which was impressively demonstrated by the grounding of the *Ever Given* in the Suez Canal in 2021 [2]. To reduce the risks of such situations, international conventions require ship bridges to be equipped with specific digitalized and interconnected systems that improve situational awareness, such as an electronic chart display and information system (ECDIS), a navigation RAdio Detection And Ranging (RADAR), and the automatic identification system (AIS) [3].

While improving the ships' safety, these integrated navigation systems (INSs) have been shown to be vulnerable to cyber attacks [4] and incidents have become more frequent [5], [6]. Bridges have been targeted by jamming and spoofing attacks and typical security flaws have been identified, e.g., default credentials or outdated software [9], which have enabled infections with common ransomware [7], [8]. Researchers have gone one step further, proposing attacks that specifically target navigation systems and vessel operations. These range from cyber attacks [10]–[12] to combined cyber-electromagnetic actions to create complex hybrid attacks [13]–[15].

Nowadays, this topic is taken more seriously among shipyards, owners, classification societies, and the International Maritime Organization (IMO), which have recently added cyber security to their regulations and classification standards, e.g., [16]–[18]. Additionally, organizations and research groups published guidelines to perform cyber risk assessments and proposed mitigation strategies for ships' information technology (IT) and operational technology (OT), e.g., [19], [20]. However, it will take time until security measures are widely adopted, while limited availabilities of secure-by-design products and a lack of in-house expertise complicate the upgrading of existing vessels. At the same time, 93% of surveyed crew members feel under-prepared to handle cyber incidents [21] and thus have to be adequately trained [22]. To encourage shipping companies and suppliers to demand and build secure systems and to provide cyber security training for their crews, it requires practical demonstrations of attacks on INSs. Therefore, attacks from research must be transferred to real bridge systems and demonstrated in scenarios well-known to seafarers, because only *seeing is believing*.

In this paper, we performed the important step towards a real system and studied the general applicability of network-based attacks on a ship bridge with real maritime hardware under realistic conditions. We used our tools from previous work and implemented hybrid attacks proposed in the literature. In addition, we share some insights into the challenges we faced when transferring academic tools to the bridge system. Our contributions in this paper can be summarized as follows:

- Study of the feasibility of network-based cyber attacks known from literature on real ship bridge hardware,
- Holistic investigation on the ship's navigation and communication systems including their electromagnetic attack surfaces,
- Report on the lessons learned when transferring the attacks from the scientists' simulators to a real-life bridge.

II. Cyber Attacks against Ship's Systems

With regard to offensive INS cyber security, two research streams are investigated: *exploitation- and malware-based* attack vectors on one side, and *network-based* vectors on the other. Typically, the former focuses on a single system, using system-specific exploits or infecting the devices with malware to infer their behavior or the data that they receive.

 DOI: 10.1109/LCN65610.2025.11146370

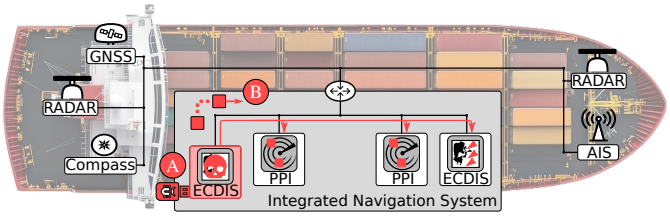


Fig. 1. Sensor data converges in the INS. Malware-based attacks (A) infect the targeted device to intercept and manipulate received data, whereas network attacks (B) affect multiple subsystems simultaneously by spoofing sensor data.

Lund et al. [23] described an attack chain to manipulate global navigation satellite system (GNSS) information displayed on an ECDIS. Using a USB flash drive, they deployed malware that acts as a machine-in-the-middle (MitM) to change the received network data before processing. A security company achieved the same result on a different ship and was also able to manipulate a RADAR screen, enabling them to selectively remove single echoes from the RADAR [24]. Unfortunately, their attack chain was not described in detail, but their report indicates that they installed malicious software on the targeted devices. Another company demonstrated a second way to manipulate the displayed position of a ship. Instead of interfering with the received GNSS data, they reconfigured the stored position of the ship's GNSS antenna in the settings of the ECDIS by using a vulnerable configuration interface [9]. Without having full control over the ship's position, this still led to a fixed yet potentially harmful offset.

While the ECDIS is an obvious target of a cyber attack due to its relevance in manual operation, other systems were also found to be vulnerable. Hopcraft et al. [25] investigated a standard compliant voyage data recorder (VDR). They showed that these systems are prone to data manipulation via the network, although data integrity is a crucial mandatory requirement for which the VDR has been certified. Despite having no noticeable effect during the operation of the targeted ship, attacking the VDR could be used to conceal traces of a cyber attack and impede post-incident investigations. A general study scanning for exploitable vulnerabilities of a real navigation systems has been performed by Sviličić et al. [26]. Although they classify the risk level for the majority of such systems as low, they were able to carry out exploitation-based attacks due to an insecure and outdated configuration of the tested device.

In contrast to exploitation- and malware-based approaches, *network-based* attacks inject manipulated or forged information into a ship's bridge network. Although such attacks still require a compromised device, they enable the simultaneous, system-wide manipulation of all devices in the network that receive and process the spoofed data, as sketched in Fig. 1.

These injection attacks are possible due to the lack of encryption and (source) authentication in maritime network [10]. The use of IP-based communication e.g., in IEC 61162-450 [27] or various proprietary RADAR network protocols [28], facilitates the development of INS network simulation environments, several of which have been proposed for research [29]–[31]. Within these simulators, research groups have developed and demonstrated different attack tools.

As a framework that combines different manipulative attacks against sensor data representations on an ECDIS, our BRidge Attack Tool (BRAT) [10] can track the current state of the ship by listening to IEC 61162-450 network traffic and injecting forged packets. Following this approach, Wolsing et al. [11] and Longo et al. [12] published tools to manipulate the image of a simulated navigation RADAR. Both were able to either completely disturb the screen, to stealthily manipulate only parts of the image [11] or to mimic electromagnetic false-flag operations [32].

Other network-focused INS security research considers covert control channels. Such unidirectional communication could be used by external attackers to trigger and control previously implanted malware. Leite et al. [33] proposed spoofed AIS messages and specific RADAR jamming in this context. Similarly, Amro et al. [13] spoofed a special type of AIS messages that can carry binary data and used them to covertly transmit encrypted shell commands containing malware. By listening to the network traffic, a previously installed receiver decrypting incoming messages then executes these commands on the infected system. The feasibility has been shown in a simulated environment with artificial signals using off-the-shelf AIS transceivers.

Studying the effects of network attacks and developing countermeasures is relevant for all digitalized bridges. Even systems that are air-gapped in theory often are not in practice, e.g., because infected USB devices are plugged into equipment onboard or scrubber systems with remote connectivity are retrofitted onto older vessels [17]. For the development of these attacks and their proof of work, simulation environments are very useful, especially considering the limited research access to real ships. Nevertheless, transferring those attacks to real systems is crucial to validate their feasibility, effectiveness, and impact in practice. This need applies in particular to attack methods that claim to be independent of system configurations, as system redundancies and network configurations can limit the attacks' capabilities and may not be covered by simulators.

To this end, Tam et al. introduced a Cyber-SHIP lab [34], where they mirror different bridge setups by integrating actual bridge hardware, and thereby extend their research capabilities to include connected bridge systems instead of single devices. Similarly, the Grace Testbed [35] combines actual maritime equipment with simulations for training and research purposes. Such a hybrid approach was also chosen for the MariOT testbed [36], that interfaces hardware and simulations of four mandatory IT and OT systems of ships and provides a platform for various purposes, including cyber security research, risk assessment, and training of maritime personnel. Although the inclusion of simulations makes these test environments broadly applicable, it also introduces the risk that the simulated data, behavior, or configurations might not represent the state of the equipment in use at sea; protocols can also be implemented more or less strictly. Therefore, we strive to transfer network attacks to real hardware of a ship navigation bridge.

III. The Laboratory Equipment

Located directly at the edge of the Port of Hamburg, Germany, we have a fully functional INS available in our laboratory. There, we can study the feasibility of attacks given the system configurations we – and an arbitrary attacker – are confronted with. We can also study whether some attacks suddenly become infeasible when the INS is provided with real sensor data from outside. Moreover, demonstrations and trainings will emphasize the impact of cyber threats and the urgency of adequate countermeasures more convincingly and forcefully, if the tools are attacking real bridge equipment with authentic environmental sensor data rather than a simulation tool with synthetic data on an ordinary office monitor.

Our laboratory consists of two main parts. One part is the bridge equipment within the building, consisting of an INS and corresponding receivers and transponders, depicted in Fig. 2(a). It closely resembles the bridge of an actual (generic) container ship because all devices are regular merchant marine equipment and approved for installation on a maritime vessel. Further, the INS provides all required functions to fulfill the IMO regulations of an INS [37] (cf. Oruc et al. [38]). The other part is the antenna platform in Fig. 2(b) that is located on top of the building and is directly connected to the bridge. The sensors on this platform supply real data to the INS around the clock, making it unnecessary to simulate any data and allowing us to work with more realistic data, e.g., AIS messages containing erroneous target information or normal oscillations of the GNSS reading. Bridge and antenna platform were installed in accordance with the rules and regulations of two classification societies and could be found equally configured on any ocean-going container ship. The only major differences: no information on depth, rudder angle and propulsion are generated, and our systems are not redundant, because our laboratory is stationary and rather unsinkable.

Among others, the following devices are installed: ECDIS, chart RADAR, GNSS and satellite compass, AIS transponder, radio telephones for different wave lengths and VDR. All of these devices are from a single manufacturer, Furuno, except for the VDR, which is a Danelec device. In addition, Iridium and satellite antennas are integrated, so that network attacks from an external source can be tested as well.

(a) Bridge equipment. (b) Antenna platform.

Fig. 2. INS with real antennas and hardware systems, installed in accordance with classification rules and behaving as a real ship bridge.

As is common, these devices and the corresponding sensors and antennas are interconnected via NMEA 0183 [39] and IEC 61162-450 [27][1]. The IEC 61162-450 network contains additional switches that are approved and common in maritime practice. Those can be used as a gateway into the network, for data analysis, but also for network attacks. Since they are not used in a merchant marine setting, NMEA 2000 [42] connections are not installed in our laboratory.

IV. Transferring Attacks to the Bridge – Tools & Preparation

To transfer the network attacks to the real bridge, we have started from the perspective of an attacker and, thus, intentionally with little *a priori* knowledge about the specific behavior and configurations of the systems. There was only the information described in the previous section. Thus, we only knew the manufacturers, types, and product names of the integrated subsystems, which enabled us to find their manuals online. Additionally, we had a rough overview of the actual wiring, but we first had to figure out the purpose of each connection.

A. Setup & Attack Tools

In our attack study, we took the role of an *internal attacker*, who compromised a device within the INS network. For this purpose, we connected an ordinary laptop running an Ubuntu Linux to the central network switch. This laptop was able to capture the network traffic and is designated to test existing attack tools against the displayed sensor and RADAR data. We used BRAT [10] to test the manipulation of the displayed sensor data on ECDIS and chart RADAR. In a machine-on-the-side (MotS) attack, we targeted AIS, GNSS position, heading, and speed over ground (SOG) information. To study the feasibility of RADAR image manipulation, we relied on RAT [11], to which we added support for the network protocol of the Furuno RADAR installed in the laboratory.

B. Implementation of Remote Triggering

To investigate the feasibility of a covert control channel in practice, we implemented trigger agents waiting for control commands based on GNSS, AIS, and RADAR. The general concepts are similar to [13], [33] are and described below.

1) GNSS Trigger: First, we implemented two GNSS trigger agents. A time trigger enables a potential attacker to define two points in time at which a predefined attack should be started and stopped. Information on the date/time of day were taken from NMEA sentences of the respective sentence ID, i.e. GLL, GNS and ZDA. A second GNSS trigger agent implements geofencing functionality and triggers an attack as

[1]Note that all given certifications grant compliance of the devices with IEC 61162-450:2018. To date, compliance with IEC 61162-450:2024 [40] or it's safety and security add-on IEC 61162-460 [41] is not certified (yet). Thus, our study does not consider any functionalities specific to the latest editions.

soon as the ship enters a given rectangular zone defined by two coordinates. Without having to be near the target, a potential attacker can thus increase the maximum impact of an attack by waiting for the victim to enter a favorable area.

2) AIS Trigger: AIS information in NMEA sentences are almost identical to the data transmitted in raw AIS radio signals. This grants the transmitter control over the content of network messages and makes them suitable for triggering or controlling from within transmission range. Again, we implemented two different trigger agents. The first starts an attack when a received AIS message contains a predefined ship identifier (MMSI). Following the approach of Amro et al. [13], a second agent controls the behavior of our attack tools and determines the attack type to be executed next, based on information in the payload of an AIS binary broadcast.

3) RADAR Trigger: Finally, we implemented a trigger agent that expects a specific pattern in the observed RADAR video data. Inspired by Leite et al. [33], we chose a sequence of echo strengths received from one direction causing a dotted line as trigger pattern. Similar patters are caused by commercial search and rescue transponders or RADAR beacons and are induced by transmitting pulses in the frequency band of the RADAR antenna. Thus, we can expect attackers to have necessary capabilities. Instead of performing image processing on the chart display as in [33], the trigger agent analyzes the echos of each RADAR spoke individually by capturing them from network traffic. Using a threshold, the echo strengths are transformed into a binary representation and the result is compared to the expected triggering pattern.

V. Implementation, Lessons Learned & Results

In the course of our work, we came across a number of pitfalls that we were not aware of and that are usually not part of the assumptions of INSs security in the literature. These pitfalls include network protocols and protocol properties, which are part of the IEC 61162-450 standard but not necessarily implemented in academic simulators, as well as system-specific and configurable processing of sensor data. We have studied only a single bridge, so our findings might not directly apply to other INSs. Still, our results point towards the general demand for reconnaissance and preparations, even for attacks exploiting well-known network vulnerabilities.

A. Sensor Data Manipulation on INS in Practice

Both terminals, ECDIS and chart RADAR, are interconnected by an Ethernet switch exchanging data according to IEC 61162-450. As required for compliant network devices, and probably part of the advertised 'intelligent routing,' the network switch uses Internet Group Management Protocol (IGMP) snooping [43]. Joining the respective IP groups gained access to the NMEA sentences exchanged over the network. In order to be processed, the sentences have to strictly comply with the IEC standard, including header and tag fields for each NMEA sentence transmitted. All tag fields, i.e., source identifier, sequence number, and timestamp, as well as optional group-related tags, are validated by the

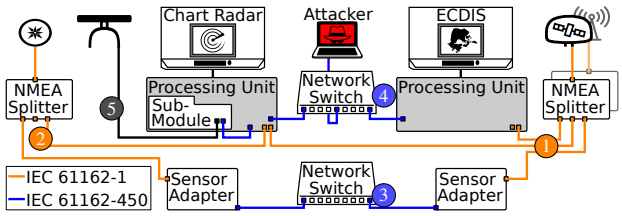


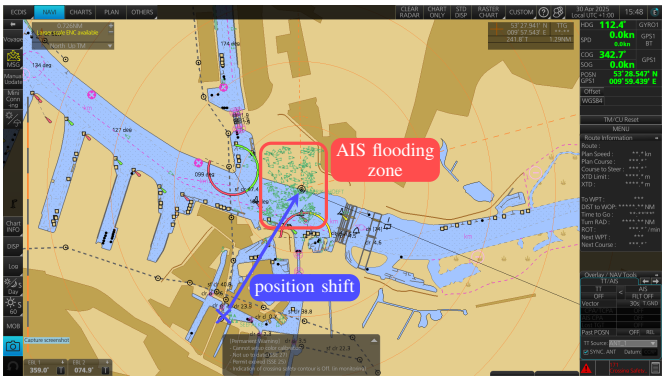
Fig. 3. Subset of INS devices and schematic network topology that we discovered in the laboratory.

receiving systems. Although not surprising, it distinguishes our bridge from simulators mentioned in Sec. II which all use Bridge Command's [44] non-standardized transmission of NMEA via UDP, lacking header and tag fields.

The most hindering aspects of the bridge were redundant connections and a prioritization of data sources. Both are probably part of the safety measures and, in fact, prevented a successful attack without any modification or reconfiguration of the systems. Contrary to our expectations, we did not connect BRAT to the main source of sensor data, but to one of three networks that are all intended to deliver data to systems distributed across the bridge. Fig. 3 schematically visualizes the different network segments we discovered. The prioritized data sources are individual serial connections (IEC 61162-1 1) from each sensor to both terminals. An exception is the satellite compass that is not directly connected to the ECDIS 2. If the terminals receive data on these wires, messages of the respective sensor from other sources are ignored.

The second network is an IEC 61162-450-based sensor network 3, which the terminals are not part of. All sensors are connected to that network through a sensor adapter that converts IEC 61162-1-compliant NMEA sentences into the IEC 61162-450 format. According to the manufacturer's manuals, such sensor networks can replace the individual serial connections from each sensor to each terminal. It is worth noting that multiple of these networks might be set up and could isolate different workplaces. Thus, a network-based attack at one single point would not necessarily affect the entire bridge. The final network, to which we connected BRAT and RAT, is an Ethernet 4 connecting all terminals distributed over the bridge. It synchronizes the settings of all workplaces and shares alerts and RADAR data among the systems. It also serves as a fallback option for devices that no longer receive data on the serial connections, as all devices forward sensor data from their prioritized sources to this network.

As a result, this network topology only allowed the heading information on the ECDIS to be manipulated, as there is no serial connection for the compass on this terminal 2. Successful manipulation of the other sensors required an interruption of their respective serial connection at the targeted terminals. Unplugging the sensors however enabled arbitrary sudden or continuous (stealthy) manipulations of the displayed information on the disconnected terminal, as visualized in Fig. 4(a). It shows a striking flooding of AIS signals in close range to the own position, which was shifted from the original location (×) by a successful network-based GNSS spoofing.



(a) Combined AIS flooding and GNSS spoofing attack.

(b) Rotation of the RADAR overlay by 45° clockwise.

Fig. 4. Manipulation of AIS, GNSS, and RADAR overlay data displayed on ECDIS by injecting forged network packets.

B. RADAR Image Manipulation in Practice

At **ECDIS overlay**: In contrast to the NMEA standard for maritime sensor data, RADAR image distribution over the network is not standardized on maritime systems. Instead, manufacturers usually have their own proprietary protocols and encodings unknown to potential attackers. After analyzing packet captures and Internet research, we could implement an encoder for RAT that enabled us to spoof RADAR data for manipulation of the RADAR overlay on the ECDIS. A respective decoder was later used to build the RADAR-based trigger agents (cf. Sec. IV-B3).

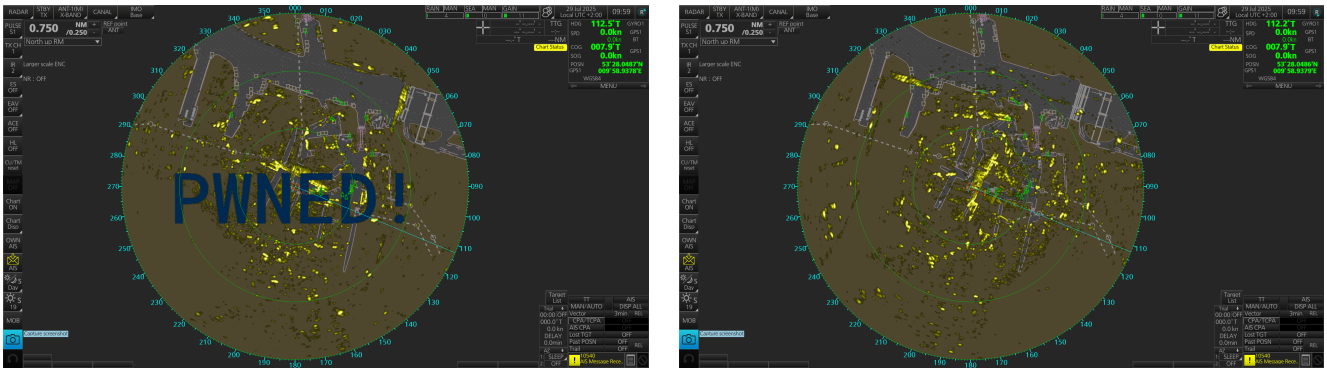
Using the encoder, we were able to arbitrary manipulate the RADAR overlay on the ECDIS by adding or removing RADAR echoes and changing the azimuth fields of each sweep (cf.Fig. 4(b)). However, original packets were still received by the ECDIS and led to some fragments of the original RADAR image being visible on the screen (○), due to the MotS position in the network. Further, we found some fields in the protocol header that could not be changed as a MotS attacker. For instance, modifying the range information in spoofed packets caused the ECDIS to switch back and forth between the spoofed and the original range setting, resulting in a constant redrawing of the entire overlay image.

At **chart RADAR**: While we were confident that we could have some effect on the ECDIS' RADAR overlay, we did not expect to be able to influence the chart RADAR from our position in the network. The chart RADAR is connected directly to the RADAR antenna (5) via a cable that appeared to be a conventional twisted pair network cable (cf. Fig. 3). We assume that it is used for control commands and to receive the RADAR image data. Any attempt to capture traffic on that cable failed and caused an alert signaling a lost connection of the chart RADAR to the antenna. Therefore, we suppose that the cable either carries raw video data instead of Ethernet frames or uses a unique wiring to prevent unauthorized connections.

Back on the INS network (4), a packet capture replayed into the network showed a second RADAR spoke on the chart RADAR's display. After investigation, we found that it is actually a sub-module within the chart RADAR's casing that is connected to the antenna. This module creates two differently encoded data streams that are sent to the chart RADAR's processing unit via an additional conventional LAN cable. Without further processing, they are forwarded to the network. One stream carries the RADAR overlay data and is received by the ECDIS, whereas the other is sent back and is received by the chart RADAR itself again. We also noticed a couple of TCP packets that were falsely forwarded by the network switch to our attacking device. Their content indicated that these were control commands to the RADAR antenna following the same path as the RADAR data. The reason for that routing might be the possibility of adding additional chart RADAR terminals to the bridge with only one connected to the antenna. Because all terminals should be able to display and control the same data, this path might have simplified implementations. Fortunately for us, it also enabled us to manipulate the RADAR image on the chart RADAR, as shown by the screenshots in Fig. 5. The different encoding and processing of the data on the chart RADAR even enabled a manipulation without visible fragments of the original image (cf.Fig. 5(b)) and the specification of the echo type. For example, we added the text in Fig. 5(a) as echo trails, which is why it is displayed in blue. In combination with the modification of the overlay on the ECDIS, we had now full control of all RADAR information visible on the INS.

C. The Feasibility of External Triggering

We were able to test both GNSS triggers and the MMSI-based AIS trigger with real sensor data by choosing a certain triggering time, selecting a trigger area containing our actual position, and defining the MMSI of a nearby ship as a trigger, respectively. However, radio frequency regulations and safety concerns due to the proximity of the local harbor prohibited AIS spoofing and RADAR jamming. Therefore, we had to simulate the reception of a AIS binary broadcast messages and triggering RADAR echoes by injecting them into the network with a second laptop. We used an AIS standard conform encoding of the controlling payload and also verified that these types of AIS messages could be found in benign network traffic during normal operation. Likewise, the triggering RADAR echoes were encoded according to the RADAR protocol.



(a) Writing text into the RADAR image by adding artificial echoes.

(b) Rotation of the RADAR image by 90° counterclockwise.

Fig. 5. Screenshots taken on the bridge's chart RADAR exemplarily showing arbitrary manipulations of the RADAR image.

While the GNSS and AIS triggers worked flawlessly, we observed that our RADAR trigger agent detected a high rate of triggering signals during the normal RADAR operation caused by noise and echoes from physical objects surrounding our test space. However, the fact that the occurrence of such natural echoes heavily depend on the position of a ship and the tuning of the RADAR makes a reliable selection of a triggering echo sequence difficult. Entering a harbor or canal with activated RADAR could start the attack against the attacker's will. Changing the triggering pattern to a more distinct composition of echoes would help to prevent a false-positive triggering, but would increase the complexity of generating such a pattern with external electromagnetic pulses on the one hand and increase the detectability of the attack on the other.

D. Final Takeaways

Our final study results are summarized in Tab. I. Although INS network protocols lack of any security concepts, safety-related redundancies complicate the simultaneous manipulation of multiple systems with a network-based attack. It requires prior reconnaissance about networks and configurations of the specific bridge. The final abilities of an attacker heavily depend on the networks they are part of. Because changing the prioritization of data sources at the terminals was against the idea of this study, our initial attempts to manipulate the displayed sensor values were unsuccessful. A reconfiguration or physical manipulation was needed, which requires unprotected configuration interfaces or physical access to the serial connections that are plugged into an electronic board within the terminal casings. Since casings of operating vessels are sealed, unnoticed access to the connectors is difficult even for an attacker with physical access to the bridge.

In contrast, the only barrier to an attacker manipulating the RADAR image on this bridge is the proprietary network protocol and encoding. The combination of missing sender authentication and unusual routing of video data enabled us an INS-wide manipulation on all terminals without further preliminaries by a message injection attack. Our demonstration of the fundamental abilities to implement manipulative attacks from literature (i.e., [11], [32]) highlights this threat's severity to navigational RADAR systems.

TABLE I
FEASIBILITY OF NETWORK ATTACKS AND EXTERNAL TRIGGERS ON A REAL-WORLD SHIP BRIDGE USING DIFFERENT SENSOR INFORMATION.

Target	Position	AIS Targets	Heading	SOG	RADAR
ECDIS	◐	◐	●	◐	●
Chart RADAR	◐	◐	◐	◐	●
Attack Trigger	●	●	n/a	n/a	◔

Notation: Attack successful (●), successful only after reconfiguration (◐), reliability of trigger depends on external environmental conditions (◔).

The final insight is the usability of GNSS and AIS information as trigger signals or covert channels for clandestine communication under real network conditions. Although we also demonstrated the general usability of artificial RADAR echoes for this purpose, the performance depends on environmental settings and tuning of the RADAR, making our trigger agent prone to accidental triggering and thus less reliable.

VI. Conclusion

The vulnerability of navigation systems of ships has been repeatedly demonstrated by researchers, but the acceptance and preparedness of involved stakeholders and the availability of cyber-secure systems are only growing slowly. Researchers therefore have to transfer these demonstrations into the maritime world and onto real-world systems to increase the impact of their findings. In this work, we have studied the transferability of network-based attacks and covert channels from simulated research environments to a real INS. We have found network structures that complicate the proposed packet injection attacks, while showing their general feasibility and emphasizing the resulting threats. Based on our learnings, we aim to advance our threat presentations and bring them closer to real-world scenarios on a variety of different INSs to highlight the universality of the threat and demonstrate the impact on vessels operations. Furthermore, an extension of existing attack tools to other maritime communication technologies and protocols beyond Ethernet and IEC 61162-450, such as the CAN-based NMEA 2000, is desirable for future work. The overall goal shall be to provide a realistic indication of the risk of network-based attacks to study possible mitigation strategies and to improve the demonstrations of the critical importance of cyber security to maritime stakeholders.

References

[1] UNCTAD, "Review of Maritime Transport 2024: Navigating Maritime Chokepoints," *United Nations Conference on Trade and Development*, 2024. [Online]. Available: https://unctad.org/publication/review-maritime-transport-2024

[2] M.-A. Russon, "The cost of the Suez Canal blockage," *BBC News*, 2021. [Online]. Available: https://www.bbc.com/news/business-56559073

[3] SOLAS Chapter V, "Safety of Navigation," 2009, IMO.

[4] G. Kessler and S. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. Amazon Digital Services LLC – KDP Print US, 2025.

[5] Maritime Computer Emergency Response Team (M-CERT), "ADMIRAL dataset," 2025. [Online]. Available: https://www.m-cert.fr/admiral/

[6] J. Pijpker, S. McCombie, S. Johnson, R. Loves, and G. M. Makrakis, "An Open-Source Database of Cyberattacks on the Maritime Transportation System," *Preprints*, October 2024.

[7] M. Kenney and F. Macdonald, "Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity." [Online]. Available: https://cyberowl.io/resources/global-industry-report-shifting-tides-rising-ransoms-and-critical-decisions-progress-on-maritime-cyber-risk-management-maturity/

[8] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, "Maritime Cybersecurity: A Comprehensive Review," *arXiv preprint arXiv:2409.11417*, 2024.

[9] K. Munro, "Hacking, tracking, stealing and sinking ships," *PenTestPartners*, 2018. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/

[10] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: a Bridge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, 2021.

[11] 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 *Proc. of the 47th IEEE Conference on Local Computer Networks (LCN)*, Edmonton, AB, Canada, 2022.

[12] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and Defending) the Maritime Radar System," *IEEE Transactions on Information Forensics and Security*, vol. 18, 2023.

[13] A. Amro and V. Gkioulos, "From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks," in *Proc. of the 27th European Symposium on Research in Computer Security (ESORICS)*, Copenhagen, Denmark, 2022.

[14] G. C. Kessler and D. M. Zorri, "AIS Spoofing: A Tutorial for Researchers," in *Proc. of the 49th Conference on Local Computer Networks (LCN) – Special Track on Maritime Communication and Security (MarCaS)*, Caen, France, 2024.

[15] F. Klör, J. Bauer, S. Paulus, and M. Rademacher, "Dude, Where's That Ship? Stealthy Radio Attacks Against AIS Broadcasts," in *Proc. of the 49th Conference on Local Computer Networks (LCN) – Special Track on Maritime Communication and Security (MarCaS)*, Caen, France, 2024.

[16] IMO, "Guidelines on Maritime Cyber Risk Management," International Maritime Organization (IMO), MSC-FAL.1/Circ.3/Rev.3 4, Apr. 2025.

[17] DNV Cyber, "Maritime Cyber Priority 2024/2025," 2025. [Online]. Available: https://www.dnv.com/cyber/insights/publications/maritime-cyber-priority-2024/

[18] IACS, "UR-E26 – Cyber resilience of ships, UR-E27 – Cyber resilience of on-board systems and equipment," International Association of Classification Societies (IACS), Unified Requirements, Apr. 2022.

[19] BIMCO, *The guidelines on cyber security onboard ships*. The Baltic and International Maritime Council (BIMCO), 2016.

[20] P. Rajaram, M. Goh, and J. Zhou, "Guidelines for cyber risk management in shipboard operational technology systems," in *Journal of Physics: Conference Series*, vol. 2311, no. 1. IOP Publishing, 2022.

[21] F. Macdonald, "The Lifecycle Dilemma: Navigating cybersecurity risks across designing, constructing and operating a vessel." [Online]. Available: https://cyberowl.io/resources/global-industry-report-the-lifecycle-dilemma-navigating-cybersecurity-risks-across-designing-constructing-and-operating-a-vessel/

[22] A. Raymaker, A. Kumar, M. Y. Wong, R. Pickren, A. Chhotaray, F. Li, S. Zonouz, and R. Beyah, "A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners," *arXiv preprint arXiv:2506.15842*, 2025.

[23] M. S. Lund, O. S. Hareide, and Ø. Jøsok, "An Attack on an Integrated Navigation System," *Necesse*, vol. 3, no. 2, 2018.

[24] V. Wee, "Naval dome exposes vessel vulnerabilities to cyber attack," *Seatrade Maritime News*, 2017. [Online]. Available: https://www.seatrade-maritime.com/maritime-safety/naval-dome-exposes-vessel-vulnerabilities-to-cyber-attack

[25] R. Hopcraft, A. V. Harish, K. Tam, and K. Jones, "Raising the Standard of Maritime Voyage Data Recorder Security," *Journal of Marine Science and Engineering*, vol. 11, no. 2, 2023.

[26] B. Sviličić, I. Rudan, A. Jugović, and D. Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System," *Journal of Marine Science and engineering*, vol. 7, no. 10, p. 364, 2019.

[27] IEC 61162-450:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," 2018.

[28] A. Saillard, K. Wolsing, K. Wehrle, and J. Bauer, "Exploring Anomaly Detection for Marine Radar Systems," in *Proc. of the 10th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS)*, Bydgoszcz, Poland, 2024.

[29] M. von Rechenberg, M. Schmidt, C. Hemminghaus, J. Bauer, and E. Padilla, "When a BRAT fools your bridge: A Cyber Security Test Environment for Integrated Bridge Systems," in *LCN Demos (virt.)*, Edmonton, AB, Canada, 2021. [Online]. Available: https://www.ieeelcn.org/prior/LCN46/lcn46demos/Demo_8_1570761147.pdf

[30] F. Basels, K. Wolsing, E. Padilla, and J. Bauer, "Demo: Maritime Radar Systems under Attack. Help is on the Way!" in *Proc. of the 49th Conference on Local Computer Networks (LCN)*, Caen, France, 2024.

[31] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, 2023.

[32] G. Longo, A. Merlo, A. Armando, and E. Russo, "Electronic Attacks as a Cyber False Flag against Maritime Radars Systems," in *Proc. of the 48th IEEE Conference on Local Computer Networks (LCN) – Workshop on Maritime Communication and Security (MarCaS*, Daytona Beach, FL, USA, 2023.

[33] W. C. Leite Junior, C. C. de Moraes, C. E. de Albuquerque, R. C. S. Machado, and A. O. de Sá, "A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems," *Sensors*, vol. 21, no. 9, p. 3195, 2021.

[34] K. Tam, K. Forshaw, and K. Jones, "Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities," in *Proc. of ICMET Oman*, Muscat, Oman, 2019.

[35] Fathom5, "Grace Maritime Cyber Testbed System." [Online]. Available: https://www.fathom5.co/grace

[36] P. Rajaram, R. Rajasekaran, M. Goh, J. Zhou, and K. Tan, "The Need for a Testbed for Strengthening Maritime Cybersecurity," *SNAMES 41st Annual Journal*, pp. 60–73, 2022.

[37] IMO, "Resolution MSC.252(83) Amended in 2018, Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS)," 2007.

[38] 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, p. 107, 2022.

[39] NMEA 0183, "Standard For Interfacing Marine Electronic Devices," 2023.

[40] IEC 61162-450:2024, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," 2024.

[41] IEC 61162-460:2024, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security," 2024.

[42] NMEA 2000, "Standard For Serial-Data Networking Of Marine Electronic Devices," 2022.

[43] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet Group Management Protocol, Version 3," Internet Requests for Comments, RFC Editor, RFC 3376, October 2002.

[44] J. Packer, "Bridge Command," *GitHub repository*, 2025. [Online]. Available: https://github.com/bridgecommand/bc