DOCTORAL THESIS

Cybersecurity for Maritime Operational Technology: Challenges, Considerations and Solutions

Gábor Visky

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2025

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
71/2025

Cybersecurity for Maritime Operational Technology: Challenges, Considerations and Solutions

GÁBOR VISKY

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

The dissertation was accepted for the defence of the degree of Doctor of Philosophy in Information and Communication Technology on 19 September 2025

Supervisor: Prof. Dr. Olaf M. Maennel,
Department of Software Science, School of Information Technologies,
Tallinn University of Technology
Tallinn, Estonia

Co-Supervisor: Prof. Dr. Risto Vaarandi,
Department of Software Science, School of Information Technologies,
Tallinn University of Technology
Tallinn, Estonia

Opponents: Prof. Dr. Vasileios Gkioulos,
Department of Information Security and Communication Technology,
NTNU – Norwegian University of Science and Technology
Gjøvik, Norway

Prof. Dr. Jianying Zhou
iTrust – Centre for Research in Cybersecurity
SUTD – Singapore University of Technology and Design
Singapore, Singapore

Defence of the thesis: 22 October 2025, Tallinn, Estonia

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology, has not been submitted for any academic degree elsewhere.

Gábor Visky _____
signature

ISSN 2585-6898 (publication)
ISBN 978-9916-80-381-3 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-382-0 (PDF)
DOI https://doi.org/10.23658/taltech.71/2025

Visky, G. (2025). *Cybersecurity for Maritime Operational Technology: Challenges, Considerations and Solutions* [TalTech Press]. https://doi.org/10.23658/taltech.71/2025

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
71/2025

Merendustehnoloogia küberturvalisus: väljakutsed, kaalutlused ja lahendused

GÁBOR VISKY

TAL TECH
KIRJASTUS

Contents

List of Publications

The author authored or co-authored the following publications, which are referred to in the text using Roman numerals.

I R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi. A systematic literature review of cyber security monitoring in maritime. *IEEE Access*, 13:85307–85329, 2025

II G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam. Multi-purpose cyber environment for maritime sector. *Proceedings of the International Conference on Information Warfare and Security*, pages 349–357, Mar. 2022

III G. Visky, S. Katsikas, and O. Maennel. Lightweight Testbed for IEC61162-450-Related Cyber Security Research. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 638–643, 2024

IV G. Visky, A. Šiganov, M. u. Rehman, R. Vaarandi, H. Bahşi, H. Bahsi, and L. Tsiopoulos. Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 644–651, 2024

V G. Visky, D. Khisteva, and O. Maennel. *Technical Considerations for Open-Source Intrusion Detection System Integration in Marine Vehicles*, pages 143–160. Springer Nature Switzerland, Cham, 2025

VI G. Visky, A. Rohl, R. Vaarandi, S. Katsikas, and O. M. Maennel. Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

VII G. Visky, D. Khisteva, R. Vaarandi, and O. M. Maennel. Towards an open-source intrusion detection system integration into marine vehicles. In *2024 International Symposium ELMAR*, pages 263–268, 2024

VIII G. Visky, B. Adam, R. Vaarandi, M. Pihelgas, and O. Maennel. Open source intrusion detection systems' performance analysis under resource constraints. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, pages 201–208, 2024

IX G. Visky, A. Rohl, S. Katsikas, and O. Maennel. AIS data analysis: Reality in the sea of echoes. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

X G. Visky, R. Vaarandi, S. Katsikas, and O. Maennel. Statistical analysis-based feature selection for anomaly detection in ais dataset. In *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 159–164, 2025

XI A. S. Benterki, G. Visky, J. Vain, and L. Tsiopoulos. Using Incremental Inductive Logic Programming for learning spoofing attacks on maritime automatic identification system data. In S. Bauk, editor, *Maritime Cybersecurity*, pages 123–141. Springer Nature Switzerland, Cham, 2025

XII M. E. Orye, G. Visky, A. Rohl, and O. Maennel. Enhancing the cyber resilience of sea drones. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, pages 83–102, 2024

Author's Contributions to the Publications

I As a co-author, I actively contributed to the research and manuscript preparation. My responsibilities included conducting a comprehensive review of the relevant literature and performing in-depth analysis to support the study's findings. I played a significant role in the development and refinement of the methodological framework and statistical analysis of the papers. Additionally, I was involved in the preparation of a portion of the tables and figures. I also contributed to writing and revising the manuscript.

II As the main and leading author of this publication, I proposed a solution for the lack of a maritime-related cyber research and education environment. I developed, described and prototyped the introduced system. For the publication, I conducted the literature review, prepared the figures and wrote the research environment-related parts of the manuscript.

III As the main and leading author of this publication, I proposed a solution for the lack of maritime-specific cyber research environment. I developed, described and prototyped the introduced system, conducted all the experiments, discovered the introduced vulnerabilities, conducted the literature review, assembled the equipment, wrote the software for the experiments, conducted measurements and wrote the manuscript.

IV As the main and leading author of this publication, I led and supported the development of the research environment, provided the maritime-related theoretical background and wrote a significant part of the scripts. For the publication, I contributed to the literature review and wrote a significant part of the manuscript.

V As the main and leading author of this publication, I proposed a solution to address the lack of a comprehensive study on the aspects to be considered during an intrusion detection system integration in marine vehicles. For the publication, I contributed to the literature review, conducted the research, performed the data collection and analysis, and wrote the entire manuscript.

VI As the main and leading author of this publication, I identified the cybersecurity issues related to the proprietary developed communication protocols used on ships. I conducted the data collection in the environment introduced in II, executed the manual reverse engineering (MRE) of the discussed protocol and exploited its vulnerabilities. For the paper, I contributed to the literature review and wrote the MRE- and attack-related parts of the manuscript.

VII As the main and leading author of this publication, I identified the lack of a comprehensive study on the challenges that restrict the development of cyber defence for ships. For the paper, I contributed to the literature review, participated in the ship visits and semi-structured interviews, synthesised the results, and wrote the manuscript.

VIII As the main and leading author of this publication, I identified the need for IDS performance analysis and comparison, coordinated the development of the research environment and the method, and supervised the data collection and performance measurements and analysis. For the paper, I contributed to the literature review and wrote a significant part of the manuscript.

IX As the main and leading author of this publication, and in response to the lack of publicly available maritime-related datasets identified in I, I developed, described and prototyped the AIS data collector system, including the hardware and software, collected all the data and carried out the analysis. For the paper, I conducted the literature review, prepared all the figures and wrote the manuscript.

X As the main and leading author of this publication, and in response to the lack of maritime-related anomaly detection in OT data identified in I, I developed the method, conducted the data analysis and developed features for use in anomaly detection. For the paper, I conducted the literature review, prepared the figures and wrote the manuscript.

XI As a co-author, I pre-processed the data collected with the system introduced in IX, contributed to the feature selection and development, supervised the experiments and result validation. For the paper, I contributed to the literature review and supported the manuscript writing process.

XII As a co-author, I contributed extensively to the literature review by identifying and analysing relevant research on threat modelling methodologies, particularly in the context of sea drones. I applied the STRIDE methodology to assess vulnerabilities across various OT architectures used in different sea-drone platforms. Additionally, I supported the manuscript writing process.

List of Abbreviations

AI-PAML	Adaptive Incremental Passive-Aggressive Machine Learning
ASR	Absolute Speed Ratio
ARP	Address Resolution Protocol
ATON	Aids to Navigation
ACP	Air Condition Plant
ADNS	Automated Digital Network System
APRE	Automated Protocol Reverse Engineering
AIS	Automatic Identification System
APS	Autonomous Passenger Ships
BIMCO	Baltic and International Maritime Council
BIT	Binary Image Transfer
CCWS	Central Cooling Water System
CRP	Command-Response Pair
CIA	Confidentiality Integrity and Availability
CORS	Continuously Operating GNSS Reference Stations
CAN	Control Area Network
CNN	Convolutional Neural Networks
CSE	Critical State Estimation
CYRA-MS	Cyber Risk Assessment for Marine Systems
CTI	Cyber Threat Intelligence
CPS	Cyber-Physical System
CPU	Central Processor Unit
CRC	Cyclic Redundancy Check
DCU	Data Converter Unit
DLS	Data Link Service
DOS	Denial-of-Service
DSC	Digital Selective Calling
DSC	Digital Selective Calling
DNP3	Distributed Network Protocol 3
DSR	Dynamic Slot Reservation
ECDIS	Electronic Chart Display and Information System
EPRIB	Emergency Position Indication Radio Beacon
ESD	Emergency Shut Down
FL	Federated Learning
FMECA	Failure Mode Effects and Criticality Analysis
FWG	Fresh Water Generator
FOS	Fuel Oil System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GLONASS	Global'Naya Navigatsionnaya Sputnikovaya Sistema
HCRE	Hybrid Cyber Research Environment
HIDS	Host-based IDS
HMI	Human-Machine Interface
HVAC	Heating, Ventilation and Air Conditioning
ILP	Inductive Logic Programming
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission

IDS	Intrusion Detection System
IMO	International Maritime Organisation
INMARSAT	International Maritime Satellite Organization
CCIR	International Radio Consultative Committee
ITU	International Telecommunication Union
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
LLM	Large Language Models
LWE	Light-Weight Ethernet
LAN	Local Area Network
LSTM	Long-Short-Term Memory
LOS	Lubricating Oil System
ML	Machine Learning
MOB	Man Overboard
MITM	Man-In-The-Middle
MRE	Manual Reverse Engineering
HFO	Marine Heavy Fuel Oil
MaCRA	Maritime Cyber Risk Assessment
MAS	Multi-Agent System
MMSI	Maritime Mobile Service Identity
MSOCS	Maritime Security Operation Centres
MTS	Maritime Transportation Systems
MRD	Maximum Reception Distances
MCDM	Multi-Criteria Decision-Making Framework
MSM	Multi-Sentence Message
NMEA	National Marine Electronics Association
NM	Nautical Mile
NAVTEX	Navigation Text
NADS	Network Attack Detection
NIDS	Network-Based Intrusion Detection System
NN	Neural Network
NSE	Nmap Scripting Engine
NATO	North Atlantic Treaty Organisation
OC-SVM	One-Class Support Vector Machine
OT	Operational Technology
PPS	Packets Per Second
PMS	Power Management System
PLC	Programmable Logic Controller
PKI	Public Key Infrastructure
RADAR	Radio Detection and Ranging
RPI	Raspberry Pi 3
RE	Reverse Engineering
S-AIS	Satellite-AIS
SART	Search and Rescue Transponder
SIEM	Security Information and Event Management
SMT	Satisfiability Modulo Theories
SOLAS	International Convention for the Safety of Life at Sea
SOTDMA	Self-Organising Time Division Multiple Access
SBM	Sensor Broadcast Message

STP	Sewage Treatment Plant
SIS	Ship Information System
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
ES	Sporadic E-Layer
SCADA	Supervisory Control and Data Acquisition
SVM	Support Vector Machines
TDMA	Time-Division Multiple-Access
VHF	Very High Frequency
VND	Visual Navigation Disruption
VPN	Virtual Private Network
VTS	Vessel Traffic Service
WIDS	Water Ingress Detection System

1 Introduction

The early 2020s reminded us how fragile our global economy is: the Covid-19 pandemic had long-lasting effects on production and the supply chains [6]. Since the maritime sector has an enormous role in global transportation, disruption of maritime traffic can have serious consequences, as was proven in 2021, when the 400-metre-long container ship Ever Given blocked the Suez Channel. The ship was refloated after a six-day salvage operation. The numbers show the importance of the waterways. Approximately 12% of global trade, around one million barrels of oil and roughly 8% of liquefied natural gas pass through the canal. Each day had a severe impact on countless countries and businesses [7].

Until recently, the maritime sector was considered safe from cyberattacks due to the lack of Internet connectivity and the isolated nature of ships at sea. But now, this situation is changing. During recent years, the sector has experienced several cyber incidents, such as IT outages, ransomware attacks or data breaches [132]. There are several reasons for this. Along with increasing automation, data and navigational networks are growing more complex and becoming a critical part of ships. To optimise the resources of maritime transportation and make it economical, ships are becoming centrally controlled, meaning that they are becoming more vulnerable to cyber threats. The importance of keeping in touch with society has been growing constantly, especially during the pandemic when the crew was not allowed to leave the ships for months. The International Transport Workers' Federation reported that "Seafarers' groups had won the right to mandatory social connectivity for crews, including Internet access." To fulfil this requirement, ships will be even more vulnerable [40].

To address the problem, maritime organisations, such as shipbuilders, ship owners, the International Maritime Organisation (IMO) and classification societies in various countries, have announced laws and regulations regarding cybersecurity on ships. On 1 January 2021, the IMO released the Maritime Cyber Risk Management in Safety Management Systems to manage maritime cybersecurity [97].

Every industry has its unique features, making it difficult to defend against cyberattacks, such as in the maritime sector, where ships have high complexity and limited communication bandwidth [153]. While experts can easily access land-based IT infrastructures, the case is different on ships. Their systems are not prepared to handle remote failures, and there is no cyber expert on board to investigate an incident and introduce security measures when needed. These circumstances call for solutions that can detect cyberattacks and related system anomalies as soon as possible.

To reduce the impact of a cyber incident, it must be detected as soon as possible, which introduces the need for highly accurate incident detection systems. Regular intrusion detection systems can identify anomalies on hosts and in network traffic very efficiently but cannot deal with application-level anomalies, such as irregular sensor values or abnormal system behaviour. To address this issue, new application-level anomaly detection methods are required [191, 55].

To develop such methods, realistic maritime lab environments and real-life datasets are needed. Unfortunately, existing research has often relied on private data, and there are only a few publicly available maritime-specific datasets [189].

Vendor-developed proprietary protocols make the situation more complicated, since they are often not designed to handle cyberattacks. Moreover, proprietary protocols reduce the interoperability of devices and introduce the need to develop a custom attack-detection system for each such protocol. Furthermore, since proprietary protocols are often not sufficiently documented, understanding the nature of the

protocol requires reverse engineering. However, manual reverse engineering of these protocols is a highly complex and time-consuming procedure that should be avoided. Automated protocol reverse engineering can significantly reduce the complexity of this process [190].

Equipping ships with cyber incident detection and security monitoring solutions can be difficult, since the IT/OT infrastructure is certified by authorities, so they cannot be changed without massive administrative work. For example, the selection of the intrusion detection system (IDS) is crucial, as it involves a trade-off between component performance, system complexity, installation and cost [187]. To find the optimal solution, several aspects must be considered [186], including the performance and applicability of IDSs [184].

1.1 Research Objectives

A literature review helps to summarise and synthesise the arguments and ideas of existing knowledge in a particular field and gives direction for future research [104]. To gain a clear understanding in the field of maritime cybersecurity monitoring, our systematic literature review [180] highlighted several research gaps, which this thesis aims to bridge:

- The lack of maritime-specific lab environments.
- The absence of publicly available, maritime-related on-board communication datasets.
- The critical need for specialised on-board systems that can significantly enhance vessel cybersecurity.
- The limited availability of released algorithm implementations, which creates a need for dedicated maritime IDS solutions capable of processing both proprietary and standardised maritime protocols.
- The need for published research on the vulnerability of maritime protocols.

The thesis consists of nine chapters. After a brief state-of-the-art introduction to the maritime cyber domain, Section 4 presents the environments developed for maritime cybersecurity research and education. Section 5 details the generated publicly available datasets, which serve as an effective tool for research, testing and validation. Section 6 sheds light on the vulnerability of maritime protocols and their exploitation, highlighting the superior efficiency of automated reverse engineering compared to manual methods. Section 7 then introduces various anomaly detection methods applicable to ships' OT environments. Section 8 discusses open-source intrusion detection systems, their performance and applicability in ships' networks, and touches on related challenges.

1.1.1 Research Datasets and Environments

Improving the sector's cybersecurity requires special environments for 1) personnel education and 2) technology research. The requirements for these environments are defined by several aspects, such as purpose, flexibility, interoperability and cost.

The literature review revealed a research gap: the need for a comparative analysis of different research and educational environments from these perspectives. This analysis motivated the development of three distinct architectural options for building the maritime laboratory. Each environment was designed for different purposes, as introduced in Section 4.

Another requirement is the availability of a dataset for developing, testing and validating results. Although some publicly available data sources exist, they often serve special purposes and contain only a limited amount of data compared with the original datasets. This limitation reduces their usability. The specific research objectives related to the datasets and the research and education environment addressed in this thesis are as follows.

- **RO1:** Implementation of different architectures for research and educational laboratories.
- **RO2:** Collection, analysis and publication of maritime datasets.

1.1.2 Maritime-Specific Communication Protocol Analysis and Anomaly Detection

Like other sectors, the maritime industry uses well-documented communication protocols, and often domain-specific proprietary ones developed by individual vendors. These proprietary protocols are often ill-prepared for cyberattacks. They are vulnerable because they are either legacy systems, carry inherited weaknesses or were just optimised for a specific purpose without security features. Exploiting such weaknesses can have serious consequences, making it essential for defence solutions, such as IDSs, to be prepared to handle the situation. Special dissectors are needed for these protocols that are not easily available.

Developing dissectors requires a solid understanding of the protocols, gained either from public documentation or reverse engineering. This thesis introduces the results of the manual reverse engineering of a closed protocol and discusses an automated method that reduces human resource demands.

A thorough understanding of the protocol is also crucial for more efficient anomaly detection. Defence systems, such as IDSs, should be enhanced with capabilities that consider the specifics of the application area — in this case, the operational technology system of ships. Section 7 focuses on anomaly detection in AIS, one of the most common maritime-specific protocols.

These needs motivated the following research objectives:

- **RO3:** Maritime-specific protocol analysis and vulnerability exploitation.
- **RO4:** Data analysis and anomaly identification in the AIS dataset, including the development of new anomaly detection methods, using statistical analysis and inductive logic programming.

1.1.3 Selection and Deployment of IDS Engines into Shipboard OT Systems Networks

One key condition for reducing the effectiveness of cyberattacks, and thereby minimising the potential damage, is early detection, followed by incident management and the necessary countermeasures. However, several factors complicate detection, such as the scale of attacks, the various on-board systems, the large volume of network traffic and the closed nature of the protocols used.

Once closed communication is processed and an anomaly detection method is in place, there are two options for implementing anomaly detection on board: developing new software from scratch or extending an existing IDS solution with new features. The latter approach has the advantage of using the full range of detection logic that an IDS engine can offer, such as tens of thousands of regular signatures for detecting a large number of known attacks in the network.

The third part of the thesis investigates the selection and deployment of maritime IDSs to achieve the following research objective:

- **RO5:** Examination and introduction of key considerations for integrating IDSs into marine vehicles, including a comparative performance analysis of open-source IDSs for resource-constrained environments.

1.2 Contribution to the Field

This thesis is based on a collection of peer-reviewed scientific publications published in reputable journals and presented at international conferences. Its primary objective is to improve the cybersecurity of the maritime sector, and its main contributions to the field are as follows:

1. Development of various research and education environments to support successful and high-level cyber education and research.

2. Generation and analysis of a novel and publicly available dataset that enables the exploration of anomalies in real-world AIS data.

3. Vulnerability analysis and exploitation of standardised and proprietary protocols enabling researchers and industry to develop defence solutions for on-board communication systems.

4. Development of methods for anomaly detection in AIS data that can be used for cyber defence solutions.

5. On-board applicability and performance analysis of open-source IDSs, demonstrating their usability in shipboard environments.

For clarity, Table 1 provides a mapping of the sections to the corresponding research objectives, publications and contributions of this dissertation.

Table 1: Mapping of the thesis chapters to research objectives, publications and contributions.

Chapters	Research Objectives	Publications	Contributions
4	RO1	II, III, IV	1
5	RO2	IV, IX	2
6	RO3	III, IV, VI	3
7	RO4	IX, X, XI	4
8	RO5	V, VII, VIII, XII	5

1.3 Thesis Structure

The thesis consists of nine chapters. After a brief state-of-the-art introduction to the maritime cyber domain, Section 4 presents the environments developed for maritime cybersecurity research and education. Section 5 details the generated publicly available datasets, which serve as an effective tool for research, testing and validation. Section 6 sheds light on the vulnerability of maritime protocols and their exploitation, highlighting the superior efficiency of automated reverse engineering compared to manual methods. Section 7 then introduces various anomaly detection methods applicable to ships' OT

environments. Section 8 discusses open-source intrusion detection systems, their performance and applicability in ships' networks, and touches on related challenges.

Finally, Section 9 summarises the contributions of this research to the identified scientific challenges and outlines several future research perspectives.

2 Background

2.1 On-Board Operational Technology Systems

Various systems installed on vessels are considered part of the on-board operational technology. Farah et al. [54] described the most common examples, providing a comprehensive overview of various systems and technologies used on ships to ensure efficient operation, safety and compliance.

Power Management System (PMS). One of the key functions of the PMS is to control the diesel generator(s) on board the ship. This includes starting and stopping the generator(s) as needed, as well as adjusting their output to maintain optimal performance and efficiency. The PMS uses real-time information from sensors and monitoring systems to analyse the load on the ship's electrical system and to make decisions about how to best distribute the load among the available generators. Using an optimal equal-load division strategy, the PMS ensures that each generator operates at a consistent and efficient level while meeting the ship's overall power demand. The PMS may also adjust the operational settings of the generators based on specific conditions, such as changes in weather or sea conditions, to maintain stability and reliability.

Engine. Ships are powered by marine engines, which are specialised engines designed to provide the propulsion and electrical power needed to operate the vessel. There are several different types of marine engines, including diesel engines, gas turbine engines and steam turbines.

Diesel engines are the most common type of engine used on ships. They operate by compressing air into a cylinder and then injecting diesel fuel into the compressed air. The heat of the compressed air ignites the fuel, creating an explosion that drives a piston and turns a crankshaft. The motion of the crankshaft is then used to power the ship's propeller.

Gas turbine engines are another type of engine used on ships. They operate by compressing air, mixing it with fuel and igniting the mixture in a combustion chamber. The hot gases produced by combustion then flow through a turbine, which turns a shaft connected to the propeller.

Nuclear engines use nuclear reactors to generate heat, which is used to produce steam that drives a turbine. The heat is generated by a controlled nuclear reaction, which produces large amounts of energy from minimal fuel. Nuclear engines are primarily used on naval vessels, such as aircraft carriers and submarines, but are not commonly used in commercial shipping due to their high cost and strict regulatory requirements.

Hybrid engines use a combination of power sources to provide propulsion and electricity to the ship. For example, a hybrid engine might combine a diesel engine with an electric motor or a battery bank. The diesel engine provides primary propulsion and electrical power, while the electric motor or battery bank provides additional power during peak loads or when the ship is operating in a low-emission mode. Hybrid engines are becoming more common in commercial shipping as operators look for ways to reduce emissions and improve fuel efficiency.

Water Ingress Detection System (WIDS). This is a specialised technology used to detect the presence of water in areas where it should not be present. Each vessel must be equipped with a WIDS, in accordance with SOLAS Chapter XII, Regulation 12. The system typically consists of sensors or detectors placed in strategic locations to monitor for the presence of water. If a specific level of water is detected, an audible and visual alarm must be triggered to notify the relevant personnel. This allows for quick action to be taken to prevent damage to the structure or any equipment located in the affected

area.

Thrusters. These are a type of propulsion system that generates lateral force, enabling the ship to move sideways. They are commonly used on large vessels for efficient manoeuvring, especially during low speeds and docking. A thruster consists of a propeller mounted in a tunnel in the ship's hull and driven by an electric motor. Thrusters can be located at both the bow and the stern of a vessel, depending on the specific needs and requirements of the ship. They are often used in combination with other propulsion systems, such as main engines and rudders, to provide the necessary control and manoeuvrability for the safe and efficient operation of large vessels.

Emergency Shut Down (ESD). The ESD is a safety feature that is activated in the event of an emergency, such as a fire. It runs a sequential shutdown of pumps and valves to prevent the spread of the incident and minimise damage. The system is typically automated and can be triggered by various sensors and detectors, such as fire detection, overfilling or pressure sensors.

Once activated, the system sends signals to the control room or central monitoring station, which then initiates the shutdown of pumps and valves in a predefined sequence according to safety protocols. The shutdown process is designed to minimise the risk of further harm or damage by shutting down critical systems in a systematic and controlled manner.

Marine Heavy Fuel Oil (HFO) Treatment System. This system treats heavy fuel oil used as fuel for marine engines. The system removes impurities and contaminants that might cause engine damage and reduce engine efficiency.

The system typically consists of a series of components that work together to treat the fuel, including separators, filters and purifiers. These components remove water, dirt and other impurities from the fuel, ensuring that it meets the required specifications for use in marine engines. The HFO Treatment System is an essential component of the marine engine system, as it helps to ensure that the fuel used in the engine is of high quality and free from contaminants.

Fuel Oil System (FOS). The FOS is a critical component of a marine vessel propulsion system responsible for receiving, storing and delivering fuel oil to the propulsion system. Fuel oil is typically stored in large on-board tanks and transferred to the engine via a piping system that includes pumps, filters and other equipment. The FOS also includes fuel treatment equipment, which is used to remove impurities and contaminants from the fuel before it is used in the engine. This can include centrifugal separators, filters and purifiers, which remove water, dirt and other impurities from the fuel, ensuring that it meets the required specifications for use in marine engines. In addition to providing fuel to the engine, the FOS also includes systems to monitor and control the fuel oil supply, such as flow metres, pressure sensors and control valves. This enables the crew to monitor fuel consumption and adjust the fuel supply as needed to optimise engine performance and efficiency.

Lubricating Oil System (LOS). The LOS is a critical subsystem of a marine engine, responsible for the efficient operation and long-term reliability of the engine. It provides a continuous supply of clean oil to the engine's moving parts, which helps to reduce friction, dissipate heat, and prevent wear and tear on engine components. Typically, it includes several oil pumps, filters, coolers and reservoirs. Pumps circulate oil throughout the engine, while filters remove any impurities or contaminants. Coolers help dissipate the heat generated by the engine, which can extend the life of the lubricating oil and prevent engine damage.

The LOS also includes sensors that allow the crew to monitor the system's performance

and identify any issues or potential problems. For example, pressure sensors can detect changes in oil pressure, which may indicate a problem with the system or the engine. In addition, oil temperature can help the crew adjust the engine's operating conditions to optimise performance and efficiency.

Gyrocompass. This is a type of gyroscope commonly used for navigation. It provides information about the vessel's heading, which is the direction in which the vessel is pointing relative to magnetic north. Using the principles of gyroscopic motion, it maintains a fixed heading relative to true north, regardless of the vessel's speed or direction. This makes it a valuable tool for navigation, as it provides an accurate and reliable indication of heading, which can be used to determine the vessel's position and course.

Echo-sounder. Also known as a depth sounder or sonar, this device is used to measure the depth of water beneath a vessel. It operates by emitting a sound signal, or "ping", which travels through the water and reflects off the seabed or other underwater objects, such as rocks or wrecks. The time it takes for the sound signal to travel to the seabed and back to the echo sounder is used to calculate the depth of the water. Echo-sounders are typically mounted on the bottom of the vessel, and the collected data is displayed on a screen or monitor on the bridge or in the control room. Operators use this data to determine water depth, locate underwater hazards and map the topography of the seabed.

Cargo management system. This system supports the loading, stowage and discharge of cargo on a ship. It includes a variety of equipment and software designed to ensure the safe and efficient transport of goods by sea.

Components typically include:

- *Cargo planning software*, used to plan the loading and stowage of cargo on the ship, taking into account factors such as the weight, volume and stability of the cargo, as well as the draught, trim and stability of the ship.
- *Cargo handling equipment*, such as cranes and winches, used to load and unload cargo.
- *Cargo monitoring systems*, including sensors and instrumentation, used to monitor the condition and location of the cargo on board the ship.
- *Cargo securing systems*, used to secure the cargo in place during transit to prevent shifting or damage.
- *Ballast water management systems*, used to maintain vessel stability during loading and unloading operations.

Fresh Water Generator (FWG). This system is used to produce fresh water from seawater. It is an essential component of many vessels, particularly those operating in areas where freshwater supplies are limited or unavailable. The system typically includes several components, such as a pre-treatment unit to remove larger particles and contaminants, a high-pressure pump to push the seawater through a series of reverse osmosis membranes, and a post-treatment system to adjust the pH and mineral content of the fresh water.

Central Cooling Water System (CCWS). This system is used to cool various components of the vessel, such as the engine, the generator, the air conditioning system and other equipment that generates heat during operation. It is a closed-loop system that circulates seawater through a series of heat exchangers to remove excess heat and

dissipate it into the surrounding seawater. The CCWS is an essential component of many vessels, as it helps to regulate the temperature of the various components on board and prevent overheating, which can lead to equipment failure and other safety hazards. By using seawater as a cooling medium, the system can also conserve freshwater supplies, which is particularly important on long voyages or in areas where fresh water is scarce.

Sewage Treatment Plant (STP). This system treats wastewater generated on board before it is discharged into the sea. It is designed to remove impurities, contaminants and pathogens from wastewater, making it safe for marine discharge. The STP reduces the environmental impact of wastewater discharge and ensures compliance with regulations governing marine pollution. Treating wastewater on board helps reduce the risk of contamination and disease transmission in the marine environment.

Air Condition Plant (ACP). The refrigeration or air conditioning plant on a ship is a system used to maintain stable temperature and humidity levels in the living quarters and cargo compartments. It is designed to regulate temperature and humidity to ensure the comfort and safety of crew and passengers, as well as to preserve the quality and safety of any perishable or temperature-sensitive cargo being transported.

Anchor and Mooring Winch Control System. This system controls the operation of the anchor and anchor-lifting mechanisms. These winches are critical components of the vessel's navigation and are used to secure the vessel in place when at anchor or moored to a pier or buoy. The system includes components such as electric motors, hydraulic pumps, control panels and sensors. It provides power to the winches, which wind in or let out the anchor chain or mooring lines as required to secure the vessel.

The control system allows the operator to control the speed and direction of the winches, as well as to monitor the tension on the anchor chain or mooring lines. It may also include automatic features such as auto-tensioning or auto-winding, which help to ensure that the vessel remains securely anchored or moored, even in adverse weather or sea conditions.

Collectively, these systems support the functional and regulatory compliance of marine vessels. Unlike communication systems, they are typically monolithic, with internal control systems and limited attack vectors.

2.2 Communications Systems

The communication systems on a ship are a vital component of its navigation and operation. They enable the crew to remain connected to other vessels, shore-based facilities and emergency services, as well as to receive weather and navigation information.

2.2.1 Navigation Aids

Global navigation satellite system (GNSS) refers to a constellation of satellites that transmit positioning and timing data to GNSS receivers, which then use these data to determine location. By definition, GNSS provides global coverage. Examples include Europe's Galileo, the USA's NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) and China's BeiDou Navigation Satellite System.

2.2.2 Situational Awareness

Radio detection and ranging (RADAR) is a high-frequency electromagnetic device designed to detect air, surface and coastal targets, determine their parameters, including movement parameters, and transmit information to ship visualisation and analysis

equipment.

The automatic identification system is an essential maritime safety system. As a significant part of the thesis discusses AIS, it is introduced in detail in Section 2.3.

Navigation text (NAVTEX) is a system used to broadcast information on maritime safety, weather forecasts, navigational warnings and other important messages to ships in coastal waters and on the high seas. Under IMO regulations, NAVTEX must be installed on all passenger and cargo ships of 300 gross tonnage or more. NAVTEX is a worldwide automated system that uses NBDP technology to transmit text messages in a standardised format. The messages are broadcast on designated frequencies that are allocated for the use of NAVTEX by the International Telecommunication Union (ITU). NAVTEX messages are typically transmitted both in the language of the coastal state and in English [87].

The emergency position-indicating radio beacon (EPRIB) is an emergency device used to transmit a distress signal to search and rescue authorities in the event of an emergency at sea. When activated, the transmitter sends a distress signal via satellite, VHF or a combination, depending on the technology. EPIRBs are designed to automatically activate when a vessel experiences a critical event, such as sinking, capsizing or other distress situations [73].

The search and rescue transponder (SART) is a self-contained waterproof transponder intended for emergency use at sea. It may be either a radar-SART or a GPS-based AIS-SART (automatic identification system SART). The radar-SART helps locate a survival craft or distressed vessel by creating a series of dots on a rescuing ship's radar display. It only responds to a 9 GHz X-band (3 cm wavelength) radar and is not seen on the S-band (10 cm) or on other radars. The radar-SART may be activated by any X-band radar within a range of approximately 8 nautical miles (15 km) [36].

2.2.3 Communication

The Global Maritime Distress and Safety System (GMDSS), as defined in Chapter 5 of the International Convention for the Safety of Life at Sea (SOLAS), describes the navigational system of vessels and establishes the mandatory installation of GMDSS. Developed by the IMO in cooperation with the International Telecommunication Union (ITU), International Radio Consultative Committee (CCIR) and International Maritime Satellite Organization (INMARSAT), GMDSS is a distress and safety radio communication system. It serves as an interconnected maritime communication network that helps ships avoid maritime emergencies and alert others to bout such threats. It provides radio communication with ships in distress and transmits information related to navigation safety, including navigational and meteorological warnings [95].

A GMDSS system may include high-frequency (HF) radiotelephone and radiotelex (narrow-band direct printing) equipment, with calls initiated through digital selective calling (DSC). Maritime safety information can also be broadcast worldwide on HF narrow-band direct printing channels.

Very high frequency (VHF) radio is a short-range radio communication system used for ship-to-ship and ship-to-shore communication. Civilian marine VHF radio is used in the frequency range of 156 to 174 MHz, with a channel width of 16 kHz and a channel spacing of 25 or 12.5 kHz. For VHF maritime radio service, 56 VHF channels are used (simplex and duplex channels), among which channel 16 (156.8 MHz) is the international calling and distress channel. VHF channel 70 (156.525 MHz) is used for DSC calls, regardless of the type of call, while other VHF channels are used for other types of communication. The transmitting power is 25 W for fixed-mount devices and 1 W for handheld devices. The

expected transmitting range of the device is between 10 and 50 NM [129].

High frequency (HF) radio is an effective long-range communication paradigm that offers over-the-horizon communication capabilities, which means it can transmit signals beyond the visual range of the transmitting and receiving stations. HF communication uses radio waves in the frequency range of 3 to 30 MHz to transmit data and voice communications. Due to the properties of these frequencies, they can penetrate the ionosphere and propagate over long distances, even over the curvature of the Earth. This makes HF communication a useful tool for long-range communication, especially in areas where other forms of communication may not be available [194].

Satellite communication systems use satellites to provide long-range voice and data communication, including email, internet access, and weather and navigation information. Maritime satellite communications are based on services operating on certain frequencies (L-band, C-band, Ku-band, Ka-band and HTS). Inmarsat is an international organisation that operates the only global satellite system for mobile communications. Established in 1979, mainly on the initiative of the IMO, its initial mandate was to serve the maritime community by improving communications and radio navigation for the safety of life at sea and efficient ship management. Inmarsat provides the space segment necessary for instant, reliable distress and safety services, as well as general satellite communications for the maritime community. It offers multiple basic satellite communication systems designed to support most of the GMDSS medium- and long-range communications functions: Inmarsat-A and Inmarsat-C. Inmarsat also offers Inmarsat-E and the L-band EPIRB system [101].

Digital selective calling (DSC) is recommended by the ITU as it is responsible for issuing alerts to rescue authorities anywhere in the world. It also enables vessels to receive distress calls from others [200].

In general, communication systems on a ship are essential for ensuring the safety and efficient operation of the vessel and must be regularly maintained and inspected to ensure their proper functioning and reliability.

2.3 Automatic Identification System (AIS)

The AIS is a crucial system for ensuring situational awareness at sea [2, 14]. AIS-equipped ships continuously transmit their unique identifiers and other essential navigation details, such as position, speed and course. It helps identify vessels, assists in target tracking and simplifies information exchange. Ships send their static and dynamic data *regularly* (Table 2) over VHF AIS transceivers.

Table 2: AIS default timing [96]

Type of Ship	General Reporting Interval
Ship at anchor	180 sec
Ship 0 to 14 knots	12 sec
Ship 0 to 14 knots and changing course	4 sec
Ship 14 to 23 knots	6 sec
Ship 14 to 23 knots and changing course	2 sec
Ship >23 knots	3 sec
Ship >23 knots and changing course	2 sec

The IMO requires a specified set of ships to be equipped with AIS to improve the safety of life at sea, the safety and efficiency of navigation, and the protection of the

marine environment. It is mandatory for all vessels over 300 gross tons on international voyages, 500 gross tons on non-international voyages, and all passenger ships under IMO regulations [96].

AIS was initially designed to enable communication between ships and shore, but it has also found a role in ship-to-ship communication. The system uses VHF radio signals to send and receive information about the ship's identity, position, course, speed and other relevant details. This information can be used by other vessels, as well as by shore-based authorities, to monitor and manage maritime traffic, improve safety and prevent collisions. In addition to the mandatory installation on large vessels and passenger ships, many small vessels also use AIS voluntarily as an added safety measure. AIS is also used by search and rescue authorities to locate vessels in distress and by environmental agencies to monitor vessel traffic and prevent pollution incidents [175].

The AIS network consists of mobile stations (ships, EPIRBs, AIS-equipped satellites and aircraft) and fixed stations, such as shore stations, repeaters and aids to navigation (ATON). GPS is essential for AIS, and most transceivers have built-in GPS receivers and external GPS ports. Each AIS transceiver has a unique nine-digit maritime mobile service identity (MMSI) number, which includes a three-digit MID indicating the country of registration and a six-digit serial number, while ATON MMSIs start with "99", followed by the MID and a four-digit serial number. The MMSI is transmitted in every message to identify the sender [14].

The AIS has a data link service (DLS) sublayer, which provides the AIS frame format. Each AIS frame consists of a preamble, followed by the start flag and subsequently the data field, a 16-bit cyclic redundancy check (CRC) [17] field to detect errors in the AIS frames, and a stop flag. Finally, a 24-bit temporary buffer that supplements the frame can be used for various purposes, such as bit stuffing, distance delay, repeater delay and jitter effects [62].

AIS transponders mainly use two dedicated frequencies: 161.975 MHz and 162.025 MHz in the VHF band. Since AIS signals have a limited horizontal range, traffic information is only available in coastal zones or ship-to-ship range [64]. When satellites are used to receive AIS transmissions and forward them to vessel traffic services, the system is referred to as Satellite-AIS (S-AIS) [27].

AIS transponders use one of the different forms of time-division multiple access (TDMA). The self-organising time division multiple access (SOTDMA) and dynamic slot reservation (DSR) selection methods under high data link load reduce the probability of message collisions. To achieve this, transmitters must change their time slot regularly to maintain [100]. This condition makes anomaly detection more challenging and does not provide any defensive measures against spoofing or jamming.

Kessler and Zorri [107] described several attacks against AIS and identified the underlying protocol's vulnerabilities.

- It lacks validity checks: messages are assumed to be correct.
- It does not support timing checks: AIS messages contain no timestamp information.
- It does not support authentication: there is no mechanism to authenticate the sender.
- It lacks integrity checks: AIS messages are broadcast unencrypted and unsigned.

Kessler and Zorri also identified the absence of security features in the AIS protocol as the root cause of these vulnerabilities. As the system is not secured by design, malicious actors can spoof or jam the system [130] and manipulate or falsify data,

leading to the dissemination of incorrect vessel information [46, 45, 1, 181]. Amro et al. [41] further described how the AIS system can be exploited for command and control in cyberattacks.

Detecting anomalies in the transmitted data can help identify such attacks early and initiate appropriate countermeasures. This motivated the thesis to investigate new anomaly detection methods.

2.4 Marine Communication Protocols

Industrial control systems (ICSs) are required to monitor industrial processes such as logistics, manufacturing or transportation. Real-time response, high availability and reliability are the key requirements of these systems. Different industries often have unique, sector-specific protocols to meet these requirements.

The National Marine Electronics Association (NMEA) is a global organisation focused on marine electronics interface standards to improve technology and safety.

2.4.1 NMEA-0183 Protocol

In the early 1980s, the NMEA issued the NMEA-0183 standard, which defines the interface between various marine electronic equipment and navigational computers, allowing them to share vital information [116]. NMEA-0183 evolved from earlier NMEA standards (-0180 and -0182) and is based on the serial communication protocol standard RS422 (Standard: EIA-422-A). This underlying protocol supports data exchange between one talker and up to 10 listeners, using 7-bit ASCII-encoded *sentences* up to 82 characters long [49].

2.4.2 IEC61162-1 Protocol

In 1997, NMEA-0183 v.1.5 was translated into the international industrial standard IEC61162-1. The most widely used communication protocols in navigation follow the IEC61162 standard, a collection of standards from the International Electrotechnical Commission (IEC) for "digital interfaces for navigation equipment within a ship" [67].

Several standard versions were published during the long evolution of IEC61162. While the IEC61162-1 protocol was designed to work over serial lines, its gradual development led to protocols that operate over Ethernet, such as OneNet, which provides a standard method for sharing NMEA-2000 data over a local area network (LAN).

2.4.3 IEC61162-450 Protocol

Over the years, the number of on-board sensors and the complexity of ship control systems have increased. Along with this, Ethernet networks with Internet Protocols (IPs) have become predominant. As Rødseth and Christensen noted in [140], in 2007, Swedish experts proposed an Ethernet-based interface standard for maritime navigation and radio communication equipment and systems. This proposal was accepted in March 2008 by Working Group 6 (Digital Interfaces) of Technical Committee 80 of the IEC. The standard was published as IEC61162-450 [68].

Although the new protocol offers more flexible services, the data format still follows the first version, in which sensor data is transferred in the IEC61162-1 sentence format. This new protocol, referred to as light-weight Ethernet (LWE), was developed for use in instrument- or process-layer networks, designed with moderated complexity to be implementable on devices with limited resources, such as embedded computers, radios and AIS receivers.

The LWE protocol is based on the standard User Datagram Protocol (UDP), in which the talker sends multicast packets that propagate over the ship's network. IEC61162-450

supports four general communication patterns for data transmission: multi-sentence message (MSM), binary image transfer (BIT), command-response pair (CRP) and sensor broadcast message (SBM). Current research focuses on the latter.

According to [77], SBM is a standard UDP packet that enables the transmission of IEC61162-1 sentences in a network environment from multiple talkers to multiple listeners. The payload of the UDP packet contains a six-byte static header (UdPbC'0') and one or more transport, annotate and group (TAG) blocks, followed by the original data (IEC61162-1 sentence). Figure 3 shows the structure of the IEC61162-450 packet.

Table 3: IEC61162-450 packet structure

Byte Offset	Function	Example Value
00	IEC61162-450 Header	UdPbC'0'
06	Delimiter	\
07	Parameter code	s
08	Parameter code delimiter	:
09	System function indicator	SI0011
15	Parameter field delimiter	,
16	Parameter code	n
17	Parameter code delimiter	:
18	Parameter value	683
21	Checksum delimiter	*
22	Checksum value	16
23	Delimiter	\
24	IEC61162-1 data	$TIROT,123.45*hh

2.4.4 Proprietary Protocols

Vendors often develop devices using proprietary, closed communication protocols to keep their specifications secret in an attempt to provide security. However, it is common knowledge in the security community that "security by obscurity" is poor practice [44].

2.5 Cyber Situation in Maritime

The importance of local and international trade by sea is growing with the global economy. This is especially crucial in markets that prioritise sustainable development, cost-effectiveness, efficiency and environmentally friendly operations. The maritime industry is responsible for handling more than 80% of global trade [173, 146].

As technology plays an increasingly significant role in the global maritime industry, it is vital to recognise the potential risks associated with it. In recent decades, maritime systems have become more digitalised and interconnected to improve efficiency, leading to substantial cybersecurity challenges within the sector [39, 106, 57, 54].

One such risk is the threat of cyberattacks, which can have significant impacts on international shipping. Raising awareness and understanding of this risk is essential to mitigate and prevent potential damage to the industry [173].

Babineau et al. [50] discussed cybersecurity risks for shipboard system, highlighting piracy, terrorism and cyber warfare as the main domains of cybersecurity risk related to shipboard control systems.

Ten years later, a comprehensive survey by Farah et al. [54] outlined the current cyber situation in the sector. According to their work, cyber incidents can affect the entire maritime infrastructure, including ports, ships, information systems and

operational technologies. Recent examples show that maritime companies are not protected against computer viruses [156], ransomware attacks [83, 4, 34], GPS spoofing [93, 28], and navigation system attacks [66, 59, 93]. According to Per Hakon et al. [132], the maritime sector typically experiences incidents with low frequency but high impact, making them difficult to predict and prepare for.

Peng et al. [144] recently published a bibliometric analysis of maritime cybersecurity, reviewing academic publications on maritime cybersecurity and providing a comprehensive overview of research progress and focus areas. They highlight that maritime cybersecurity research mainly addresses transport-related cyberattacks, autonomous vessels, AIS, maritime communication and UAVs. Their results also point to room for improvement in maritime communication systems and overall maritime cybersecurity.

Symes et al. [169] investigated real-word cyberattacks and their consequences on autonomous vessels, finding that these vessels often have relatively easy-to-breach security systems. The consequences of cyberattacks include financial loss, loss of cargo and potential breach of oceanic airspace, which can trigger military action.

Li et al. [121] provide a comprehensive survey of maritime cybersecurity, tackling the protection of key digital assets—including AIS, GNSS, ECDIS, VDR, RADAR, VSAT and GMDSS —in interconnected shipping systems, from vessels to ports and broader supply chains. The review combines analyses of real-world incidents, technical vulnerabilities, countermeasures and emerging trends to highlight how the maritime industry can strengthen its cyber resilience.

The literature reviewed above highlights the need for improvements in the maritime sector, which motivated this thesis.

2.6 Cyber Landscape of Ship's OT Systems

Among the systems introduced in Section 2.1, Akpan et al. [40] identified the main on-board automation components targeted by malicious actors.

Electronic navigation equipment used on modern ships has undoubtedly reduced collision incidents on ships over the years [90], but it still suffers from a number of cybersecurity vulnerabilities [168, 127]. Melad et al. in [133] reviewed 46 maritime-related cyber incidents, four of which targeted ships' operational technology (OT) systems.

As discussed in Section 2.1, ships have multiple OT systems that can impact the safety and security of the vessel, its crew and its cargo. Each of these systems is typically developed and produced by different vendors, resulting in wide variation in their cybersecurity readiness.

Integrating these disparate OT systems under a common shield can significantly increase the cyber resilience of a ship and can also improve the effectiveness of security measures such as intrusion detection and incident response. By implementing a holistic cybersecurity strategy that considers the ship's systems as a whole, rather than just individual components, it is possible to identify and address potential vulnerabilities across the ship's entire cyber ecosystem.

However, OT system integration presents its own set of challenges. One of the biggest is the need to ensure compatibility between different systems, which can be particularly difficult given the wide variety of vendors and technologies involved. In addition, the integration process can be complex and time-consuming, requiring significant resources and expertise.

Ships are no longer isolated systems but are now part of a connected ecosystem that

includes multiple communication systems, as introduced in Section 2.2. These communication systems offer potential attack surfaces for cybercriminals. The increasing optimisation of marine traffic, along with the need for pre-calculated and continuously updated routes, requires ships to be online continuously. This means that they are connected to various communication systems, including satellite communication, GPS and other wireless networks.

In addition to the need for connectivity for operational purposes, the crew also requires communication systems to stay in touch with family and friends. This includes Internet access, social media and other communication channels that can be accessed via the ship's network. While these systems provide critical services to the ship and important benefits for the crew's well-being, they also represent potential attack surfaces that can be targeted by cybercriminals.

To minimise the impact of a cyberattack, early detection is essential. To support this goal, new detection methods are introduced in Section 7. For a deeper understanding of the theoretical foundation underlying the chosen approach, the following section provides a detailed explanation.

2.7 Inductive Logic Programming

Inductive logic programming (ILP) is a branch of machine learning that merges inductive reasoning with logic programming, typically using languages such as Prolog. It operates within the framework of clausal logic, where examples, background knowledge and learnt hypotheses are all represented as logical clauses. ILP systems use this consistent logical format to reason and learn. Given a set of facts representing background knowledge and labelled examples (positive and negative), an ILP system constructs a logic-based hypothesis that explains all positive examples while excluding negative ones. Formally:

- given a finite set of clauses B (background knowledge), and sets of clauses $E+$ and $E-$ (positive and negative examples, respectively),
- find a theory Σ, such that $\Sigma \cup B$ is correct with respect to $E+$ and $E-$.

By the correctness of theory Σ, we mean that $\Sigma \cup B \models e+, \forall e+ \in E+$ (*completeness*), and $\Sigma \cup B \not\models e-, \forall e- \in E-$ (*consistency*).

The process of finding a correct theory in ILP typically involves two fundamental operations: specialisation and generalisation. If the current theory, when combined with the background knowledge, incorrectly explains some negative examples, it is considered too broad and must be specialised—that is, made more restrictive—to eliminate these incorrect implications. On the other hand, if the theory fails to account for all the positive examples, it is too weak and requires generalisation; it must be expanded to ensure that all positive examples are correctly explained by it in conjunction with the background knowledge.

3 Related Work

3.1 Datasets, Testbeds and Research Environments in Maritime

A cybersecurity testbed is a controlled environment designed to simulate real-world cyber threats, attacks and defences for research, testing and training. It enables organisations, researchers and cybersecurity professionals to evaluate security measures, detect vulnerabilities and develop countermeasures without risking actual systems.

3.1.1 Testbeds and Research Environments in Maritime

These environments usually provide realistic network simulation, mimicking enterprise or critical infrastructure networks. They allow for testing malware, cyberattacks, penetration techniques and security tools in a controlled environment, ensuring that experiments do not affect live systems [134].

Recent literature introduces testbeds that can support research related to cybersecurity in the maritime field.

Conti et al. [70] provided an extensive review of testbeds and cyber ranges in their study. Their work explores the architecture of ICSs, detailing their components, common protocols and the types of attacks they face. Although the publication presents a vast array of testbeds, none specifically address marine-related systems.

Kavallieratos et al. [105] reviewed various cyber-physical testbeds that can support cybersecurity research. Their study categorises testbeds into physical, virtual and hybrid models while describing their functionalities, including vulnerability analysis, training, defensive mechanisms, impact assessment of cyberattacks, and threat analysis.

Sicard et al. [162] introduced a cybersecurity testbed designed for the naval defence sector, incorporating ICS components. Their work focuses on four primary systems: direction, energy, artillery and propulsion. The proposed testbed includes various programmable logic controllers (PLCs), human-machine interfaces (HMIs), physically simulated actuators and sensors for propulsion, direction and energy control, and artillery (76 mm main gun and motors for moving the gun turret). The system includes computers for attack generation. However, it does not cover navigational devices.

Similarly, Puys et al. [148] presented hardware-in-the-loop labs that facilitate cybersecurity awareness training and supervisory control and data acquisition (SCADA) research but also lack a focus on maritime systems.

Tam et al. [170] proposed the Cyber-SHIP platform, a sophisticated research environment for maritime cybersecurity that integrates real maritime equipment for both testing and data generation. Although this platform provides an excellent environment for penetration testing, its implementation requires substantial financial investment.

Becmeur et al. [53] presented a platform to generate propulsion, engine control and navigation data based on scenario traces for the evaluation of the intrusion detection algorithm. Their system included physical elements: a fan to simulate the propeller of the ship and a steering control to simulate the changes in direction of the ship. Their solution used common industrial communication protocols, such as Modbus, DNP3 and S7.

Raimondi et al. [150] proposed a testbed to train maritime SOC teams in cyber exercises. The testbed was implemented using Linux containerisation. It featured a ship simulator transmitting NMEA messages via a Python script to other components. Suricata IDS handled network monitoring with Lua scripting for NMEA parsing, while Splunk served as the cyber situational awareness console, forwarding data to a central

SIEM server. The authors demonstrated the training process with an exercise in which false NMEA messages disrupted the gyrocompass, requiring the trainees to detect the attack using Splunk queries.

Longo et al. [125] recently introduced a virtual testbed for maritime cybersecurity. The solution relies on open-source components and provides a testbed that includes network infrastructure and core components of the on-board cyber–physical systems. The infrastructure is easy to replicate and can be utilised as a suitable training environment for seafarers and cybersecurity operators in the maritime domain.

Basels et al. [52] discussed the Radar Cyber Security Lab, an environment to evaluate the vulnerability of navigation radars and address related network attacks. The ecosystem includes two main parts, an offensive toolkit and a defensive toolkit: with the offensive one, the network-based attacks can be executed against maritime navigation radars using various protocols, while the defensive part offers radar-specific network-based IDSs.

In March 2025, iTrust—the Centre for Research in Cyber Security at Singapore University of Technology and Design—launched MariOT, the world's first industrial-grade hybrid shipboard OT testbed for maritime cybersecurity research, education, training and cyber exercises [37].

MariOT combines physical shipboard OT and ship–shore interface systems with virtual simulations, using industry-standard communication protocols. Its open framework enables realistic cyberattack scenarios and allows researchers to test detection and defence mechanisms in a safe, controlled environment.

As the first maritime cyber-physical system testbed, MariOT strengthens iTrust's position as a global leader in cyber-physical security. It supports the research, development and validation of cybersecurity solutions for deployment in shipboard OT systems.

Beyond research, MariOT provides hands-on training for maritime stakeholders—including the MPA, port operators, cybersecurity vendors, ship owners and classification societies—and helps develop workforce expertise in maritime cybersecurity. Its remote link to CEMS' simulator further enhances training by embedding cyberattack scenarios into navigation exercises, raising crew situational and safety awareness.

3.1.2 Maritime-Related Communication Datasets

Literature also investigates the cybersecurity aspects of various on-board ship systems using different datasets.

Some sources provide publicly available historical AIS data, such as Marrinetraffic [21], Spire Global [19] or AISHub [8]. These sources are reliable, but they contain only a fraction of the content of the received messages. This is because these entities focus mainly on the ships' trajectory, position and movement, where only aggregated data is required [35]. Furthermore, these datasets are not fine-grained enough to support detailed AIS-related research.

Wolsing et al. [196] introduced various network attacks against the marine radar system. Their publication relies on real-world radar data combined with radar network attacks. They published a comprehensive dataset (RadarPWN) that can be used for cyber research.

Many research papers are based on datasets that are not publicly available [180]. For example, Ristic et al. [151] introduced the statistical analysis of vessel movement patterns in ports and waterways, using self-reported AIS data. The authors used simulated data for training and testing their anomaly detector and then tested it with datasets collected in Gulf St Vincent (Port Adelaide) and Port Jackson (Sydney Harbour). These datasets are

not publicly available.

Hadzig et al. [86] introduced a probabilistic graphical model to represent and manage the uncertainty of AIS data. The publication does not mention whether the model was validated on real or simulated data.

Shahir et al. [160] introduced an anomaly detection framework to analyse, detect, and differentiate interaction patterns and anomalies for marine vessels. Their method was validated on AIS data collected by the U.S. Coast Guard. In this dataset [20], the records are filtered to include a reduced number of samples per minute, which means that their characteristics are slightly different from the original. A ship's position should be transmitted several times a minute, but the given dataset samples the transmissions at one-minute intervals. This solution reduces the size of the data and is perfect for trajectory analysis but hides some finer details.

Amro et al. [43] presented a methodical framework for anomaly detection of sensor data in the NMEA format. Their work was validated on simulated network data, and the anomalies were created with their developed tool, the NMEA-Manipulator. As the validation data are synthetic, their features likely differ from those of data collected from real ships.

Sicard et al. in [162] introduced a maritime-specific testbed, dataset generation methods and described four possible cyberattack scenarios, but the study did not publish the relevant datasets.

Spravil et al. [166] focused on the detection of GPS spoofing with the analysis of relevant NMEA messages. To assess their framework's performance, the authors created the MARSIM dataset, which contained a large number of different GPS spoofing attacks and normal GPS data. The dataset was released into the public domain [165], making this one of the few studies to provide a publicly available maritime-specific dataset.

The limited availability of realistic and publicly accessible datasets motivated this thesis to collect, analyse and publish datasets for research purposes.

3.2 Maritime Protocol Vulnerability Analysis and Exploitation

Sections 2.3 and 2.6 shed light on cyber weaknesses in the OT systems of ships. These systems often rely on standardised communication protocols; however, vendors frequently develop proprietary protocols to find a trade-off between industry needs and the complexity of the protocol, often without adequately considering cybersecurity [140].

3.2.1 Maritime Protocol Vulnerability Analysis

The research community has shared findings that focus on vulnerabilities and weaknesses in existing navigational equipment, tracking and monitoring systems [176, 51, 82, 145]. These publications discuss external communication weaknesses rather than those linked to on-board communications.

To address this gap, Frøystad et al. in [78] offer a public key infrastructure (PKI) design to improve the cybersecurity of digital communication in the maritime sector. This solution brings reliable communication to the industry but does not aim to defend on-board communication.

The Baltic Marine Environment Protection Commission [77] focuses on a modern on-board communication protocol (IEC61162-450) [68] and offers an extension that could improve the resilience of the ships' navigational systems. The paper discusses the AIS protocol, and the recommended measures may improve the overall security of the system. It does not evaluate the general shortcomings of the protocol.

In the ICS context, Drias et al. [75] introduce an attack taxonomy model that focuses on Modbus and Distributed Network Protocol 3 (DNP3) protocols to evaluate several types of attacks that can harm ICS. Although DNP3 is commonly used in the power industry, Modbus is also widely used on board ships. Xu et al. [198] introduce several protocols and their cyber vulnerabilities in the power industry. While these works shed light on the weaknesses of ICS protocols (also used on ships), they focus on power generation systems rather than navigation. This thesis addresses this gap by focusing on navigational networks and protocols, as similar vulnerabilities may have distinct consequences for maritime safety.

Tran et al. [178] discussed the security risks of several marine network protocols, such as AIS and NMEA-0183, and newer protocols, such as OneNet, but did not focus on proprietary protocols.

Although maritime cybersecurity has gained attention, the cyber weaknesses of on-board communication protocols—especially proprietary ones—have received little attention. This may stem from the perception of ships as isolated systems with minimal attack surface, which creates a false sense of security. In reality, when ships are in port during maintenance, on-board control systems can be connected to other networks and devices, or exposed to unauthorised personnel, either accidentally or intentionally. Furthermore, the crew is likely to change over a vessel's lifetime, so a former crew member could leave behind a malicious payload.

Although new vessels are equipped with advanced automation systems to improve safety and efficiency, these systems often introduce cyber weaknesses [168, 127]. This modernisation highlights the importance of maritime protocol research. The thesis addresses the problem by introducing navigational on-board communication protocols and examining their susceptibility to cyberattacks.

3.2.2 Automated Protocol Reverse Engineering

As manual protocol reverse engineering is a laborious process, automated methods are required, especially when protocols are frequently updated. To date, no studies have evaluated the application of automated protocol reverse engineering (APRE) techniques to maritime protocols, though numerous studies have evaluated their application to *land*-vehicle Control Area Network (CAN) bus protocols [202, 182, 139].

For example, Yu et al. [202] use genetic programming to identify rules that correlate integer bytes with values found in the output of a vehicle diagnostics application. However, a limitation of their approach assumes that fields have byte-divisible lengths and known endianness. Verma et al. [182] propose a modular four-stage pipeline, *CAN-D*, that infers field boundaries, endianness, signedness and physical interpretations for each CAN message type using linear regression. Both approaches rely on a ground-truth signal generated by the vehicle's diagnostic protocol. However, maritime components do not transmit an open diagnostic protocol. In our application of linear regression to infer bits correlated with values of interest, we assume that ground-truth signals can instead be acquired from external devices (e.g. GPS) or from captured metadata (e.g. timestamps or packet lengths).

Most existing APRE techniques have been evaluated on traditional IT protocols, such as file sharing, which may not necessarily translate to maritime protocols. For some techniques, the authors have released code (Nemesys [112] and NetPlier [201]), but these techniques only infer field boundaries, whereas our security research also requires syntax and semantic information. Recent advances in APRE have used deep-learning methods to infer field semantics, but no accompanying code has been

provided [199, 204].

Our APRE method shows that basic statistical techniques, combined with contextual information, are sufficient to generate the desired outputs.

3.3 Intrusion Detection Systems

As ships are increasingly using integrated systems that rely on digitalisation and automation, the urgent need for cyber risk management has emerged. As technology continues to develop, IT and OT systems are increasingly networked and more frequently connected to the Internet, raising the risk of unauthorised access or malicious attacks on the ships' systems. In addition, risks can also arise from personnel accessing on-board systems.

The Baltic and International Maritime Council (BIMCO)—one of the largest international shipping associations representing shipowners—issued the *Guidelines on Cyber Security Onboard Ships* [56] in 2018. The guidelines highlight the differences between IT and OT systems and suggest removing the barrier between technologies through close cooperation between responsible units and management.

Cybersecurity risk management is an ongoing process to identify, analyse, evaluate and address cybersecurity threats in maritime organisations. This complex process goes far beyond the scope of this thesis, which examines only the on-board, OT-related cybersecurity solutions.

When discussing system resilience to cyberattacks, we generally refer to implemented intrusion detection or prevention mechanisms (to guard against software attacks, insider threats, external adversaries, etc.). Intrusion detection mechanisms can broadly be classified into two types: *anomaly detection* and *misuse detection*. Anomaly detection identifies system indicator deviations from predefined normal behaviour profiles, while misuse detection identifies known forms of system exploitation using predetermined adversary behaviour patterns (e.g. rules or signatures) [38].

Due to the nature of the ship bridge environment—where a complex mixture of TCP/IP and industrial protocol communications takes place—the system is exposed to both off-the-shelf, known attacks and unstudied protocol-specific attacks. This raises the importance of using a multiplex approach to detect potentially malicious activity on board.

A network-based intrusion detection system (NIDS) monitors and logs network traffic for signs of malicious activity and generates an alert when a suspicious event is discovered [48]. If configured, it will notify the designated personnel to investigate certain alerts and take further action.

In contrast, a host-based intrusion detection system (HIDS) provides a deeper, more localised level of security analysis by monitoring potential attacks on individual computers where the IDS or its agent is installed. Such software monitors computer resources, such as memory and CPU usage, running processes, and system and application logs.

Although IDSs do not prevent attacks but rather detect them, they can help avert disasters. If appropriate personnel are notified in time, malicious actions can potentially be stopped and identified before major damage is done to the ship or anyone aboard. In short, the purpose of IDSs is to monitor specified traffic on a given network and, when needed, alert professionals for review. The purpose of intrusion prevention systems (IPSs) is similar to that of IDSs; however, IPSs are also allowed to take predefined actions, such as blocking or altering specific traffic [137].

Only limited literature focuses on intrusion detection in shipboard OT systems. The following section discusses the related work.

3.3.1 Intrusion Detection for RADAR and Global Navigation Satellite Systems

Situational awareness and accurate navigation are essential for safe shipping. Several systems support navigation, among them RADAR, which provides images of surrounding objects, such as ships or land, and various GNSS that provide the precise positions of ships. GPS, Galileo, GLONASS, BeiDou and other regional systems have become indispensable for navigation, and reliance on them has increased substantially over the past decade due to their exceptional usefulness. At the same time, these systems can be attacked by malicious actors, so anomaly detection is crucial for safe sailing. Several studies have addressed this topic.

Longo et al. [126] investigated cybersecurity threats to maritime radar systems, introducing attacks capable of compromising the integrity of data displayed on a radar system and presenting a detection system to highlight anomalies in the radar video feed.

Longo et al. [124] proposed a novel threat model that exploits cyberattack capabilities against radar systems to simulate the effects of electronic countermeasures. In their work, they introduced various jamming techniques and discussed possible countermeasures.

Cohen et al. [65] introduced RadArnomaly, a deep-learning-based anomaly detection system designed to protect radar systems from data manipulation attacks. Although the model demonstrates high detection accuracy, its scope is confined to anomalies in internal data, leaving broader network-level cyber threats unaddressed. This limitation underscores the need to expand its capabilities to encompass a wider range of threats in real-world maritime environments.

Basels et al. [52] presented a maritime Radar Cyber Security Lab (RCSL), in which they addressed various network-based cyberattacks against maritime navigation radars. They also introduced network-located defence solutions: a set of rules for open-source signature-based IDS, where the IDS either uses the radar image of the previous rotation (Image-Delta) or the verified positions of landmarks on nautical charts (Chart-Diff).

Lebrun et al. [120] proposed an approach for detecting anomalous events, such as potential attack attempts, based on measurements recorded by continuously operating GNSS reference stations (CORS). Although promising, this approach is difficult to adopt on board ships.

Savolainen et al. [155] published the first unsupervised long short-term memory (LSTM)-based autoencoder for GNSS anomaly detection. Their solution successfully indicates anomalies in simulated radio frequency signals. Despite promising results, the approach cannot be implemented on all GNSS receivers used on ships.

Boudehenn et al. [61] focused on detecting GPS spoofing-induced anomalies. They analysed NMEA messages that carried GPS information and proposed a one-class support vector machine (OC-SVM). Their solution is easy to implement and requires little computational power, making it suitable for deployment on low-end hardware. Tests using both simulated and real-life data collected from a small boat showed that the OC-SVM-based anomaly detection method achieved high recall and precision.

Spravil et al. [166] also focused on the detection of GPS spoofing with the analysis of relevant NMEA messages. They developed dedicated monitoring modules that could be easily integrated into a ship's network. To demonstrate the viability of this approach, they introduced a publicly available maritime NMEA-based anomaly (MANA) detection framework, selecting five methods and combining them into an ensemble. According to their experiments, the ensemble achieved a higher recall than any individual method, as it flagged an anomaly if any of the five methods indicated one.

3.3.2 Anomaly Detection in AIS Data

In addition to the radar systems discussed above, another important system that significantly improves situation awareness is the AIS. This system, however, was not designed for attacks and can easily be hacked or falsified. Extensive literature is available focusing on anomaly detection in AIS data, with approaches including statistical, rule-based and neural-network-based machine learning methods. Several notable publications discuss this topic.

Amro et al. [43] published an overview of anomaly analysis and detection in NMEA messages generated by various on-board sensors. Their research aimed to identify potential anomalies and their malicious causes. To achieve this objective, the authors developed an anomaly detection method for NMEA messages by identifying critical message types, analysing potential anomalies and attack techniques using the MITRE ATT&CK framework and evaluating detection approaches. They found that a specification-based approach, using predefined rules to identify anomalies, was the most effective. In addition, frequency-based anomaly detection was recommended for attacks that alter message rates. Although the study examined attack scenarios, it lacked precision and recall metrics. Key limitations included false positives, undetected sophisticated attacks, incomplete protocol coverage and limited consideration of anomalies. The authors also discussed potential deployment strategies for NMEA intrusion detection systems on vessels.

Iphar et al. [99, 98] examined the weaknesses of AIS and proposed more than 900 rules and integrity items to evaluate the integrity and quality of AIS message data. These rules can be used for rule-based anomaly detection. The prototype was evaluated on about 24 million real-life AIS messages collected over 6 months; however, the study did not evaluate the system on a larger number of cases or assess the system's false positive rate.

Gamage et al. [79] provided a comprehensive survey on the applications of machine learning techniques in maritime surveillance to detect abnormal vessel behaviour.

Ristic et al. [151] analysed vessel motion patterns in ports and waterways based on transmitted positions. They extracted motion patterns from historical data and constructed models using adaptive kernel density estimation to predict vessel motion. The work focused on detecting anomalies in ship trajectories.

Hadzagic and Jousselme [86] introduced a situational analysis model for vessel tracking to support the detection of deviations from intended destinations. Their Bayesian network-based probabilistic graphical model also supported the detection of anomalies in ship trajectories.

These papers provide in-depth analyses of trajectory-related irregularities, offering a comprehensive understanding of this aspect of vessel tracking, but they do not introduce methods for detecting anomalies in AIS transmissions or data.

Campbella et al. [63] introduced machine-learning techniques for invalid AIS message detection. The study identified several features to be evaluated by the applied methods, including the standard deviation and mean time between messages and discrepancies in distance calculations.

Kontopoulos et al. [114] presented a distributed architecture for the real-time detection of spoofing and falsification attacks in AIS data streams. Their method calculated the average speed on the shortest path between the reported positions from two consecutive AIS messages. They validated their solution using data gained from a publicly available data source [21], noting that future work should focus on reducing false positives and expanding to cover more attack types.

Industrial control systems (ICS) is a term used to describe several types of systems, such as distributed control systems, supervisory control data acquisition, industrial automation systems, and industrial automation and control systems. ICSs are specialist information systems that differ significantly from traditional IT systems. As ICSs use tailored protocols that meet strict timing and reliability requirements, traditional IT systems for intrusion detection and prevention do not meet the need for monitoring malicious events in ICS environments [159].

Since a vessel can be considered a system of distributed control systems [172], much of the analysed literature on IDSs comes from the ICS field.

Several surveys are available in the field of ICS cybersecurity. A 2017 survey by Idaho National Laboratory [94] provides a good overview of security tools for the ICS environment but does not focus on the available literature on the topic. Hung-Jen et al. [122] published an overview of modern IDSs, focusing on their taxonomy but without discussing their usability in industrial environments.

Urbina et al. [179] explore physics-based attacks, offering a unified taxonomy that allows for the identification of limitations, unexplored challenges and new solutions, but limited their scope to such attacks.

Gupta et al. [84] survey the challenges in the field of communication with UAVs; while detailed, the publication only lightly touches on intrusion detection.

Khraisat et al. [109] provide a broad review of techniques, datasets and challenges related to IDSs, but do not explore ICS-specific issues in depth.

Tan et al. [174] survey recent security advances in smart grids using a data-driven approach, focusing on this emerging technology in power distribution, but cover only a fraction of the broader cybersecurity landscape.

Komninos et al. [113] discuss the same topic but explore issues related to smart grid and smart home security.

Moustafa et al. [135] provide a comprehensive review of network anomaly detection, which is an essential part of the field, but omit other important approaches.

Asharf et al. [47] recently published a comprehensive review of Internet of Things (IoT) technologies, protocols, architectures and threats, including an overview of intrusion detection models for compromised IoT devices.

According to the literature, an IDS deployed on board ships should be a hybrid solution that examines more than two characteristics of the defended systems. The solution should focus on network traffic and various sensor values, as well as their behaviour. This finding shaped the focus of the thesis.

3.3.3 Anomaly Detection in Ships' Other OT Systems

Ship control systems are a combination of cyber and physical subsystems and have inherent vulnerabilities that leave them susceptible to internal or external attacks. These attacks often cause anomalies in OT that can lead to cascading failures, making this an important topic in the literature.

Smith et al. [164] modelled a ship power system in Python using a long-short-term memory (LSTM) machine learning algorithm to detect anomalies on board OT. Their model generated predictive data to be compared with actual sensor values.

Riveiro et al. [152] published a review and highlighted the need for large volumes of heterogeneous, multidimensional and dynamic sensor data analysis for maritime anomaly detection. This need comes from the diversity of ship OT systems and their specific protocols. The research aimed to find anomalies in different systems separately.

Schroeder et al. [157] used non-intrusive load monitoring techniques and methods to

identify faults and anomalies in operational technology power systems. They tested three supervised ML algorithms—convolutional neural networks (CNN), support vector machines (SVM) and LSTM—to detect and classify various artificially generated anomalies. The algorithm used pattern recognition for the detection of anomalies in power consumption.

A recent publication by Hotellier et al. [92] discusses a behaviour-based intrusion detection approach for naval systems. Their solution, which targets process-aware attacks, uses Zeek to process network traffic captured on Ethernet networks and fieldbuses and demonstrates effective anomaly detection on Modbus RTU protocol-based communication in a realistic naval testbed.

For low-level monitoring of Modbus RTU fieldbus traffic in ship ICSs, Sicard et al. [162] propose using Zeek IDS with a specialist protocol parser and traffic capture hardware, while recommending commercial IDS sensors for regular network monitoring.

Xing, Cao and Chen [197] proposed an anomaly detection method for the ship information system (SIS) using risk data analysis. They introduced a cooperative state space control model and a critical state estimation (CSE) algorithm based on the industrial state modelling language. Simulations validated the method against sensor signal attacks, but no controller implementation details or validation data were published.

Boudehenn et al. [60] used the Teager–Kaiser operator for anomaly detection in a ship's propulsion system under cyberattacks. While the method detected anomalies during PLC attacks, the evaluation was limited to short-term analysis without the assessment of long-term detection rates, false positives or computational costs; data and code were not released.

Qiu et al. [149] proposed a particle-filter-based anomaly detection method for a ship's cyber-physical system (CPS) using propulsion system data. They trained the model during the ship's first sailing week and evaluated it over 3.5 days, but did not clarify whether the detected anomalies were due to cyberattacks or normal navigation. The study did not provide precision or recall analysis, did not report computational cost, and did not make the experimental data or implementation publicly available.

3.3.4 Anomaly Detection for Maritime Networks

Gyamfi et al. [85] developed an adaptive incremental passive-aggressive ML (AI-PAML) method for network attack detection (NADS) in IoT-based maritime transportation systems (MTS). They proposed a resource-efficient multi-access edge computing (MEC) setting to run NADS at network edges, mitigating data saturation through an advanced data updating technique. Computationally intensive tasks were deployed on MEC servers, with Markov chains optimising execution by predicting server availability. The experiments used a real IoT-MEC network and the CICDDoS2019 dataset, achieving lower latency than the benchmark models in DDoS attacks.

Liu et al. [123] introduced a CNN-MLP-based intrusion detection model for MTS, trained via federated learning (FedBatch). CNN handled feature extraction, while MLP classified attacks locally. Their method reduced computational demands and preserved data privacy by sharing only model parameters, using batch-federated aggregation to handle network constraints. Tested on the NSL-KDD dataset, the model achieved 88.1% accuracy, outperforming state-of-the-art CNNs. However, the dataset lacked maritime-specific data.

Kumar et al. [115] developed a monitoring system using cyber threat intelligence (CTI) with a long short-term memory (LSTM) variational autoencoder and Bi-GRU for IoT attack

detection. However, the system was validated using the TON-IoT dataset, which lacks maritime relevance, and no computational cost assessments were provided.

Ptasinski et al. [147] proposed a statistical ciphertext flow analysis method based on maximum entropy estimates to detect network flooding DoS attacks in the US Navy's Automated Digital Network System (ADNS) INC III. Their model defined normal traffic classes and identified anomalies by comparing the observed traffic with a baseline. Although effective, it occasionally restricted normal traffic.

Zainudin et al. [203] introduced a blockchain-based decentralised trust aggregation solution for SDN-enabled marine traffic services. Their federated IDS framework used proof-of-authority blockchain and CNN-based intrusion detection, achieving strong results on the X-IIoTID dataset.

Tiwari et al. [177] developed a lightweight security model for maritime IoT sensor networks, optimising network layer protection using Enhanced LightGBM. Their approach achieved high performance with low computational cost and bandwidth usage, but relied on the non-maritime DS2OS dataset.

Popli et al. [163] proposed a federated learning framework for intrusion detection in the distributed networks of underwater drones. Their method uses federated learning (FL) to monitor underwater IoT networks. A global model is shared with devices for local training, and updates are aggregated to refine the model. They compared FL with centralised ML using the CICIDS2017 dataset and evaluated attack detection using their lab-developed SOLIDS dataset, which simulates maritime traffic and DDoS attacks. The study also analysed computational costs, confirming the practicality of the method.

3.4 Identified Research Gaps

The growing cybersecurity challenges in the maritime sector motivated our systematic literature review, which analysed the existing body of research on monitoring systems in maritime environments [180]. It identified several critical research gaps that hinder the advancement of robust cybersecurity solutions in the maritime domain. These gaps can be categorised as follows.

- Need for a maritime cybersecurity research and education environment: There is a pressing demand for dedicated research and training platforms that simulate real-world maritime cyber threats and vulnerabilities. Such environments would enable researchers and practitioners to develop, test and refine security solutions in a controlled setting.

- Need for openly available maritime cybersecurity-related datasets: The scarcity of publicly accessible datasets presents a significant challenge for researchers working on cyber threat analysis and mitigation strategies. Without real-world data, the development of accurate and effective security solutions remains constrained.

- Understudied machine-learning-based anomaly detection methods in the field: Although machine learning has shown substantial success in cybersecurity in various domains, its application in maritime anomaly detection remains limited. More research is needed to explore and validate AI-driven approaches tailored to maritime cyber threats.

- Lack of on-board cybersecurity solutions for OT systems: Many maritime systems rely on OT, which is often outdated and vulnerable to cyberattacks. The absence of effective security solutions tailored to OT in ships and offshore platforms increases the risk of cyber incidents.

- Limited understanding of proprietary on-board communication protocols: Many maritime systems utilise proprietary communication protocols that are poorly documented or inaccessible to the research community. This lack of transparency limits efforts to analyse protocol vulnerabilities and design appropriate security measures.

3.4.1 Contribution of This Thesis

This thesis addresses these critical research gaps by proposing innovative solutions that improve cybersecurity in the maritime sector. It explores the development of open research and education platforms, investigates the creation of publicly available datasets, and advances the use of machine learning techniques for maritime anomaly detection. In addition, it contributes to the security of operational technology by designing on-board cybersecurity solutions and conducting an in-depth analysis of proprietary maritime communication protocols.

By addressing these pressing issues, this research aims to improve the resilience of maritime systems against emerging cyber threats and contribute to the broader field of maritime cybersecurity.

4 Research and Education Environments

4.1 Motivation and Novelty

As maritime operations become increasingly dependent on digital systems, the security of shipboard software and communication protocols is a growing concern. The literature review highlighted the need for a comprehensive vulnerability analysis of maritime software and protocols, as cyber threats targeting these systems pose significant risks to navigation, operational efficiency and safety.

To address these challenges, controlled research environments play a crucial role. These environments can facilitate systematic investigations by enabling the generation and collection of relevant network data. By simulating real-world maritime communication scenarios, researchers can analyse protocol behaviours, detect anomalies and uncover security weaknesses.

Special environments can also support seafarer education. Although these experts are trained for maritime operations, their education should include cybersecurity and digital hygiene. In realistic environments, they can experience the signs and consequences of attacks, which prepares them to take early action.

Although cybersecurity is a growing concern for the maritime sector, many vendors and research institutions are making significant efforts to address these challenges. To better understand maritime cyber threats and increase resilience to cybercrime, sector-specific research environments are needed.

Table 4 provides an overview of relevant publications and the main features of the environments they introduce. Most support research and, to some extent, the education of IT experts (e.g. SOC analysis) but not the training of seafarers. Only a few offer realistic environments, and only a small number address navigation devices and maritime protocols. Just a fraction of the publications introduce attacks against applications; most focus on actuators, targeting commonly used ICS protocols.

This chapter—building on the work presented in [188, 185, 193]—addresses this challenge by introducing three environments that can be used for navigation system-related research and education purposes and by discussing their advantages over existing approaches.

The main novelty lies in the involvement of maritime systems and sector-specific protocols, including standardised and proprietary ones. Section 2.4 presents vulnerability research executed in these environments, which is primarily based on various attack scenarios.

From an educational perspective, the target audience of the introduced Multi-Purpose Cyber Environment (MPCE)—presented in Section 4.2—and the Hybrid Cyber Research Environment (HCRE)—presented in Section 4.4—is seafarers. These environments offer them a space to familiarise themselves with the symptoms of an attack. Another novel feature is the integration of real-life AIS data to make the operational picture in training more realistic. Unlike previously published environments, the MPCE and HCRE also offer external access, providing services without requiring on-site presence.

Publication	Description	Platform	Form	Systems	Protocol	IDS Installed	Scalability
Sicard et al. [162]	Cybersecurity testbed for the naval sector	Physical	Warship replica	Direction, Energy, Artillery and Propulsion	ModBus RTU, Siemens S7	Yes	Low
Puys et al. [148]	Cybersecurity awareness training environment	Physical	Laboratory		Modbus, FTP, SNMP, SMTP, HTTP	Yes	Low
Tam et al. [170]	Research environment for maritime cybersecurity	Physical	Laboratory	NA	NA	Can be	Low
Becmeur et al. [53]	Testbed for propulsion, engine control, and navigation systems	Physical	Laboratory	Propulsion, Engine Control, Navigation systems	ModBus, DNP3, Siemens S7	Yes	High
Raimondi et al. [150]	Testbed to train maritime SOC teams in cyber exercises	Virtual	Laboratory	Integrated navigation system	NMEA	Yes	High
Longo et al. [125]	Virtual testbed for maritime cybersecurity	Virtual	Laboratory	Multiple ship system	ModBus, BR24	No	High
Basels et al. [52]	Radar Cyber Security Lab	Virtual	Laboratory	ECDIS	BR24, ASTERIX	Yes	High

Publication	Scenarios introduced	Cost	Main purpose	Maritime protocols Involved	Application-layer Attacks	Data	External Access
Sicard et al. [162]	Yes	Moderated	Research	No	No	Simulated	No
Puys et al. [148]	Yes	High	Training	No	Yes	Simulated	No
Tam et al. [170]	No	High	Research	NA	NA	NA	NA
Becmeur et al. [53]	Yes	Low	Research	No	No	Simulated	No
Raimondi et al. [150]	No	Moderated	Training	Yes	NA	Simulated	No
Longo et al. [125]	Yes	Moderated	Training Research	Yes	Yes	Simulated	No
Basels et al. [52]	Yes	Moderated	Research	Yes	Yes	Simulated	No

Table 4: Overview of relevant publications

4.2 Multi-Purpose Cyber Environment

Cybersecurity encompasses various domains, including application security, data protection, network security, disaster recovery and business continuity planning, operational security, cloud security, critical infrastructure security, physical security, and end-user education.

Technology, human factors and regulatory frameworks play a crucial role in addressing cybersecurity challenges. This is especially true in the maritime industry, where these elements are closely interconnected. Research can further enhance their combined effectiveness in safeguarding maritime cybersecurity. This environment can support cyber research and seafarer education by enabling realistic attack simulations in real-life settings.

4.2.1 Main features

This environment relies heavily on Transas equipment, widely used across the maritime industry. Since the vendor uses a closed communication protocol, variability testing of the product is otherwise highly restricted—a limitation this environment helps to overcome. It can be used as a network traffic source essential for gaining a deeper understanding of the closed protocol.

The setup enables penetration testing on devices, simulation of cyberattacks and analysis of scenarios in which the bridge system experiences connectivity loss, receives incorrect sensor input or suffers internal system compromises.

Since the simulator was originally designed for ship operations training, the sensor values and ship behaviour it generates are highly realistic. For example, wind direction and speed influence the ship's speed and drift. This makes it possible to generate realistic sensor data that can be used for detecting anomalies in ship behaviour.

The environment also offers valuable support for seafarers' cyber education, as it provides a realistic setting to address cyberattacks against navigation devices during simulated operations, such as mooring or sailing.

4.2.2 System Setup

This environment is built around the Transas NTPRO 5000 navigational simulator [32], which was designed specifically for seafarer training. It includes a visualisation module responsible for audio and visual output, displayed on several screens, as shown in Figure 1.

The high-level structure of the research environment is shown in Figure 2. The training environment setup includes a network, positioned on the left side, that controls the simulator based on the selected scenario.

The multi-function display (MFD) acts as the electronic chart display and information system (ECDIS) within the simulator. On this computer, two vendor-developed services (RADAR and sensor data server) run, filtering out navigation-related information from the network traffic and converting it to an ECDIS-compatible format.

Instructors can set parameters affecting the simulated ship, such as visibility, wind and weather conditions, current and tides, marine traffic and the position of other ships, all of which define the RADAR picture and NMEA messages. This feature is extremely important, as it can generate operational values similar to those of real ships.

The setup has been extended with a gateway computer, which transforms the simulator's communication into the format used on real ships. This novel solution enables communication analysis, vulnerability analysis and cybersecurity research.

Figure 1: Multi-Purpose Cyber Environment setup

4.2.3 Use Case

To create a realistic dataset, the simulator was set to different propeller speeds and, in addition to the different rudder angles and wind speeds, the ship's velocity, drift and turning speed were recorded. This highly realistic, complex data set can be used for detecting anomalous ship behaviour, as well as for model training and testing.

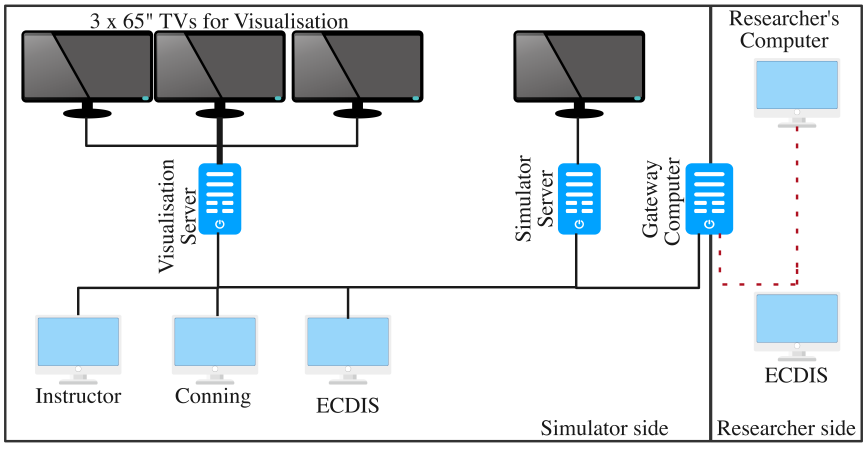


Figure 2: High-level architecture of the Multi-Purpose Cyber Environment

4.2.4 Contribution

The main contribution was the creation of a highly realistic multi-purpose cyber environment enabling the seamless execution of maritime cybersecurity research and experiments.

To achieve this, a Navi-Sailor 5000 simulator—originally designed for ship crew training in navigation and operation—was extended with additional components. The highly realistic system simulates the values of the OT process based on variables such as wind speed and direction, wave height and direction, propulsion and steering. The system uses a proprietary protocol.

The main challenge was converting this vendor- and simulation-specific communication into a ship-network-specific format. To address this, a novel solution was introduced: the original system was extended with an additional computer running a service that converts the protocols and makes network traffic available on the researcher side. This side includes the researcher's computer and an additional MFD. Both the ECDIS and the network traffic are identical to those in real integrated ship bridge systems.

These technical innovations significantly eased data acquisition during the experiments and research presented in Section 6.

4.3 Light-Weight Cyber Research Environment

The environment described above provides high-quality, realistic sensor value simulations, transmitted via a proprietary protocol, and can be extended with converters to support additional maritime protocols. However, its core infrastructure requires significant financial resources and substantial physical space for deployment. This fact motivated the development of a Light-Weight Cyber Research Environment (LWCRE) [185] that supports the vulnerability analysis of components using the IEC61162-450 standardised protocol introduced in Section 2.4.3.

4.3.1 Main Features

The LWCRE is a simple, highly cost-effective and flexible testbed, as both the researcher's machine and the ECDIS computer can run a wide range of software. The only apparent bottleneck is the chain of protocol converters, since the testbed converts IEC61162-1 sentences into IEC61162-450 format. However, this limitation can be easily handled, as the researcher's and ECDIS computers are on the same network, which allows for the use of any Ethernet-based protocol as needed.

The system is highly scalable and adaptable, since it can easily accommodate devices and services according to specific research objectives. However, the processing power and other resources for the individual components are limited by the host computers, and the simple setup accommodates only a single user at a time, leading to low shareability. Nonetheless, the straightforward design allows experienced users to easily access and use the system with minimal training.

One key limitation is the absence of external connections, which makes the environment fully isolated and limits interoperability.

4.3.2 System Setup

The high-level design of the environment is shown in Figure 3.

The setup consists of a host computer and two protocol converters, keeping costs low. The host computer runs sensor simulator software and provides a virtualisation

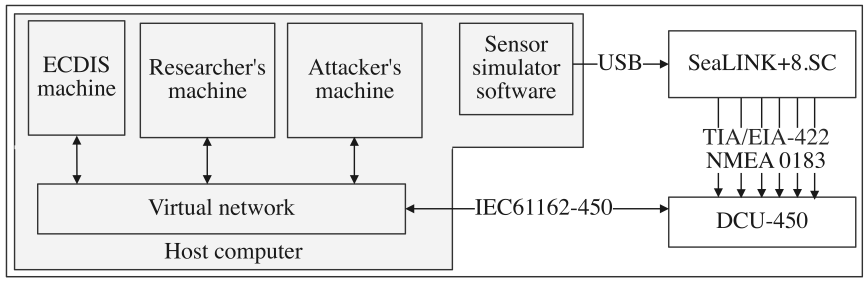


Figure 3: Structure of the Light-Weight Research Environment

environment that hosts three virtual machines: the ECDIS, the researcher's and the attacker's machine.

The host computer runs sensor simulator software [154] that can generate sensor values and send them over the USB port to the first protocol converter—the SeaLink+8.SC produced by Sealevel Ltd. [158], which has eight independent serial ports that support the TIA / EIA-422 [26] protocols. At this stage, the simulated sensor values are in IEC61162-1 format, identical to those of real-world ship systems. These signals are then passed on to a second converter, the data converter unit (DCU) DCU450 (301001), which transforms them into IEC61162-450 format. The communication at this point again matches real ship systems but now uses an Ethernet protocol. The converter sends the data through the host computer's network adapter to the virtual network that connects the three virtual machines.

The ECDIS machine runs navigational software, with the basic setup using Navi-Sailor 4000 [23] software, which is widely used in maritime transport. This software serves as the user interface and visualises data from other system components (i.e. AIS and NAVTEX messages, sensory information).

The attacker's machine, built on Kali Linux 2023.2a [15], is used to execute various attacks against the ECDIS software that uses the IEC61162-450 protocol. The malicious packets are sent over the virtual network. During our research, a serious of attacks were executed to demonstrate vulnerabilities in the software and protocol.

The researcher's machine, also running Kali Linux 2023.2a, is used to collect and analyse the network traffic.

4.3.3 Use Case

According to Kim et al. [110, 131], the STRIDE methodology, which encompasses spoofing, tampering, repudiation, information disclosure, denial of service (DoS) and elevation of privilege, is well suited for threat modelling in distributed control systems.

We used our test environment to conduct vulnerability research on a specific ECDIS device and the standardised IEC61162-450 protocol. Their vulnerabilities were successfully exploited through various attacks (spoofing, tampering, injection, and DoS) targeting the communication between the DCU and the MFD.

4.3.4 Contribution

The main contribution of this research was the design and implementation of an innovative, light-weight research environment. Compared to the MPRE—introduced in Section 4.2—this environment is more cost-effective and flexible, requires less space, is

easier to set up, and still provides effective support for maritime cyber research.

It enabled the development and execution of various cyberattacks against a Navi-Sailor 4000 ECDIS [23] by exploiting the IEC61162-450 communication protocol's weaknesses. To demonstrate the system's vulnerability, we successfully performed replay, injection, modification and eavesdropping attacks against the system. These attacks undermined the system's confidentiality, integrity and availability (CIA triad), highlighting the fragility of navigation systems.

In addition, the optimal attack rate was calculated using a Monte Carlo-like simulation [88]. Our results showed that the transmission frequency of malicious packets significantly influenced the success rate of suppressing the attacked sensor values. Specifically, the probability of a successful attack increased sharply until malicious packets were sent at less than 0.68 times the original sensor value, as shown in Figure 4. This novel finding is crucial for keeping attacks as silent as possible.

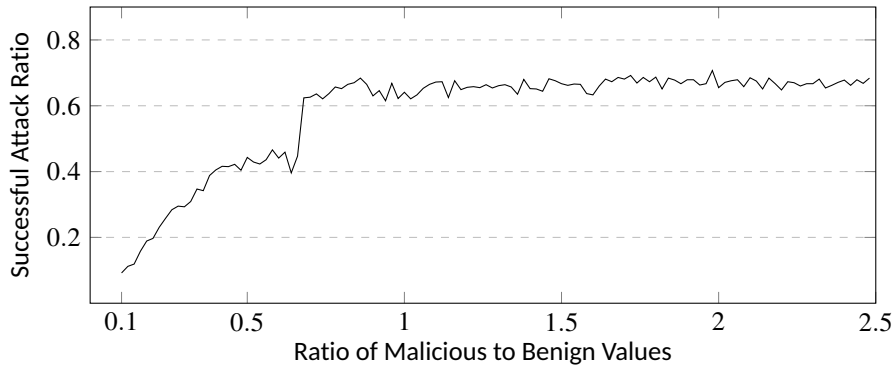


Figure 4: Probability of successful injection attack

4.4 Hybrid Cyber Research Environment

While the previously introduced research environments can support maritime cyber research, they have two main drawbacks: they handle only (highly realistic) simulated sensor values and contain hardware components, making their scaling costly. For institutions aiming to provide high-level cyber education, a realistic environment scaled to ten or twenty instances is often needed.

The innovative Hybrid Cyber Research Environment (HCRE) contains AIS data collected from real-world environments, making the operational picture in training more realistic. Another novelty is its target audience, as the HCRE is designed to specifically enhance the cyber skills of seafarers.

4.4.1 Main Features

The HCRE offers a scalable research and education platform with minimal hardware requirements, since it needs only one AIS receiver and one computer to supply real AIS data to each instance. Although the server that hosts the students' virtual machines may require a significant investment upfront, this resource can be reused for other courses, as the HCRE's virtual part is easy to rebuild. To support remote education, the system is accessible through VPN.

4.4.2 System Setup

The system architecture—divided into physical and virtual components—is shown in Figure 5. The physical layer includes the AIS receiver, the AIS relay computer, the firewall and the host computer.

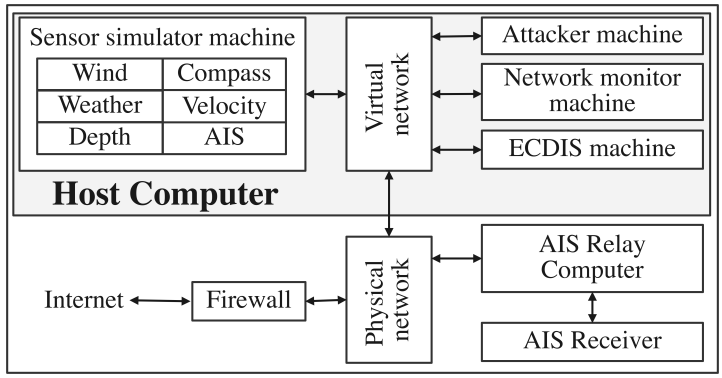


Figure 5: Structure of the Hybrid Research and Education Environment

The AIS receiver captures real-life AIS signals and, after decoding, sends them to the AIS Relay computer over TIA/EIA-422 protocol [26]. The AIS Relay computer encapsulates the messages into UDP packets and forwards them to the virtual environment. The pfSense-based [25] firewall ensures Internet communication, while providing protection against external threats by applying network-level filtering rules and by enforcing strict inbound and outbound rules.

The host Computer hosts the virtual parts of the environment.

The virtual layer consists of four virtual machines:

1. The ECDIS machine runs the ECDIS software. The basic setup uses simple OpenCPN, which is commonly used on pleasure crafts [24]. This software acts as the interface and visualises the data generated by AIS and other system components (i.e. AIS messages and sensory information).

2. The attacker machine is built on Kali Linux 2023.2a [15] and launches various attacks (e.g. network scanning, man-in-the-middle (MITM) and DoS) within the environment.

3. The network monitor machine runs Zeek [33] and Suricata [11] to store and analyse network packets regarding the normal behaviour of system components (benign traffic) and attack-related behaviour (attack traffic).

4. The sensor simulator runs NemaStudio to generate network traffic using the NMEA protocol [154]. It can simulate various source devices (e.g. AIS, RADAR or sensors) within different vessel contexts. As the environment utilises a real AIS receiver that already collects real-world data, the simulator is used to generate additional sensor data, such as wind, heading and weather information.

4.4.3 Use Case

In this setup, the sensor simulator generated various sensor values (e.g. GPS, RADAR, AIS, wind speed and direction), which were forwarded, along with real-world AIS data, to

the ECDIS machine. The ECDIS visualised these values, while the researcher or educator conducted different attacks against the system. Network traffic, both under normal conditions and during attacks, could be recorded and analysed on the network monitor machine or shared more widely.

4.4.4 Contribution

The easy-to-scale environment emulates a small-scale maritime network to facilitate research on various offensive and defensive aspects of cybersecurity. It closely replicates the communication and operational framework of real-world maritime systems, enabling in-depth analysis of vulnerabilities, attack vectors and mitigation strategies.

Within this controlled setting, a series of cyberattacks were conducted, targeting both the application and network layers. These attacks simulate real-world threats that maritime systems may face, including DoS attacks, MITM interceptions and various exploitation techniques aimed at compromising system integrity and data confidentiality.

To support further research, benign and malicious network traffic was captured, covering all system activities. These captured traces were systematically organised and published as the MarCyb dataset [192], which is publicly available in raw format. Researchers and practitioners can utilise this dataset to develop and evaluate intrusion detection mechanisms, analyse attack patterns, and improve maritime cybersecurity.

4.5 Summary

This chapter compared the features of various cyber research and educational environments, highlighting the need for new solutions that focus specifically on maritime systems and protocols and offer unique learning environments for seafarers.

Three dedicated research environments—summarised in Table 5—were introduced. These environments serve as practical platforms for both academic and industry-driven studies, facilitating hands-on experimentation and cybersecurity training. By simulating real-world maritime conditions, they enable researchers and students to analyse protocol behaviour, test security mechanisms and explore software vulnerabilities in a controlled setting.

Table 5: Summary of the main details of the environments

Environment	Multi-Function Cyber Environment	Light-Weight Research Environment	Hybrid Research Environment
Complexity	Very complex	Simple	Complex
Cost	Very high	Low	Moderate
Flexibility	Moderate	Moderate	High
Components	Physical	Mainly physical	Mainly virtual
Supported Protocols	Mainly proprietary, application level	Ethernet-based, application level, IEC61162-450	Layer 2-7, Ethernet-based protocols
Remote Access	Possible	No	Yes
Degree of Realism	High	Moderate	Moderate

Beyond vulnerability analysis, these research environments enable a wide range of cybersecurity applications. They can be used for penetration testing, IDS evaluation and

the development of defensive mechanisms tailored to maritime systems. Furthermore, their accessibility promotes knowledge sharing and education, allowing students and professionals to gain hands-on experience in analysing and securing shipboard communication networks.

The Multi-Purpose Cyber Environment offers a realistic ship bridge environment where seafarers can safely experience the signs and consequences of cyberattacks or malware. It provides a unique data source, as realistic sensor values are generated in NaviNet protocol format, which also supports research and vulnerability testing. However, this solution is less affordable, challenging to scale, and requires specialist knowledge for installation of the Transas simulator environment, although limited human effort is needed for ongoing maintenance.

The Hybrid Research Environment addresses these challenges by using only limited hardware resources and providing an easy-to-scale education environment. Despite its simple setup, this environment also enables research, network traffic generation and vulnerability testing.

The virtualisation technology limits the types of software that can be installed in this environment, as some vendors define special hardware requirements that cannot be met by virtualisation. The same applies to licensing. Vendors often sell software with individual licences, which makes scaling less affordable. Installing the system requires only moderate expertise, as the entire installation process can be scripted (this is a matter for further research).

The further needs are twofold. To scale the environment to 20 instances for a university class, a powerful server is needed, capable of running more than 60 virtual machines, possibly up to 80 or more. Therefore, it is preferable to use a cloud-based environment. Although this solution is more expensive, the environment would need to be installed and run only during class sessions, which makes it affordable.

The third introduced solution is the Light-Weight Research Environment, which relies on minimal hardware but still includes realistic components. It mainly supports, but is not limited to, research related to the IEC61162-450 protocol. Being compact, this solution supports remote work, although it is limited by its use of simulated sensor values. It is easy to install or reinstall, inexpensive to maintain and requires only basic IT knowledge. Thanks to its isolated, virtual nature, it is particularly well suited for offensive research activities.

Each environment addresses different needs. Almost fully virtual setups are best suited for training courses that involve breaking systems and where rapid redeployment of a clean environment is essential. On the other hand, labs that involve more real hardware are better suited for monitoring research and training, where systems are not broken but their behaviour is monitored in read-only mode and realism is critical.

The next chapters will detail how these environments were applied in practical cybersecurity research, specifically focusing on maritime dataset generation, protocol vulnerability analysis and exploitation.

5 Maritime Datasets

5.1 Motivation and Novelty

As highlighted in Section 1, the importance of cybersecurity is constantly growing. The previous section introduced controlled research environments that can support maritime cybersecurity research and education. Another critical challenge identified in Section 3.1.2 is the limited number of publicly available maritime datasets for cybersecurity research. Without real-world data, it remains difficult to develop and validate effective security solutions, which limits the advancement of anomaly detection and vulnerability assessment methods in the maritime domain.

Compared to other datasets, such as RadarPWN (radar-specific), MARSIM (GPS-specific) and SOLIDS (maritime IoT-specific), the dataset introduced in this thesis focuses on a different system: the AIS.

Online AIS-specific data feeds, such as Marinetraffic, Spire Global and AIS Hub, focus solely on ship positions. Unlike the AIS system, where position data are sent several times per minute, these sources distribute only a few positions per minute. Moreover, historical data are available only on a contract basis, and other types of AIS-transmitted data are not available.

To address this gap, two datasets were collected and made publicly available to support maritime cybersecurity research. These datasets provide valuable network data that can be used for protocol analysis, anomaly detection and evaluation of security measures. This section introduces these publicly available datasets and seeks to support further advancements in maritime cybersecurity, enabling the development and validation of novel security methodologies.

5.2 AIS Dataset

Section 2.3 introduced AIS, a crucial situational awareness system at sea, along with its vulnerabilities. Kessler et al. [107] describe several types of attacks against AIS and also discuss the system's vulnerabilities.

The anomaly detection solutions described in Section 3.3.2 are often validated on simulated data, which raises the need for real-life datasets. To address this need, a six-month-long dataset was collected and published.

5.2.1 Data Collection Method

The setup of the data collector system—deployed near the port of Tallinn, Estonia, at N59.462N, E24.666 40m ASL—is shown in Figure 6. It uses a ground-plane-designed base station antenna [3] tuned to the AIS transmission frequency range.

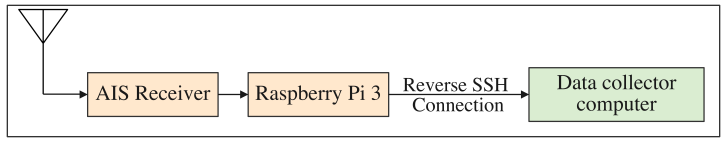


Figure 6: Structure of the Hybrid Research and Education Environment

The AIS receiver provides access to vessel information when vessels are within range. It receives AIS signals, decodes them, checks their integrity and sends the decoded data to the navigation device in NMEA0183 sentences [62]. The Comar Systems AIS receiver

(R500Ni, Comar Systems, United Kingdom) contains an AIS receiver interfaced with a Raspberry Pi 3 (RPi) computer [5]. The receiver's coverage area is shown in Figure 7.

AIS messages contain a CRC mechanism in the DLS sublayer, as introduced in Section 2.3. This mechanism supports the integrity check performed by the receiver. If the check fails, most receivers drop the packet and do not indicate the failed check or dropped message. In contrast, this receiver sends an empty NMEA sentence if a received AIS message fails the integrity check—for example, if the CRC validation is invalid or the received packet is incomplete—which helps analyse *malformed packets*. The analysis of such malformed messages is further explained in Section 5.2.4.

Sometimes packets pass the integrity check, meaning the checksum matches the payload, but the decoded data is invalid (e.g. out-of-range values). As these packets have valid CRCs and pass the integrity check, the radio cannot indicate this error; only further analysis reveals that the content is invalid. We refer to these as *error packets*.

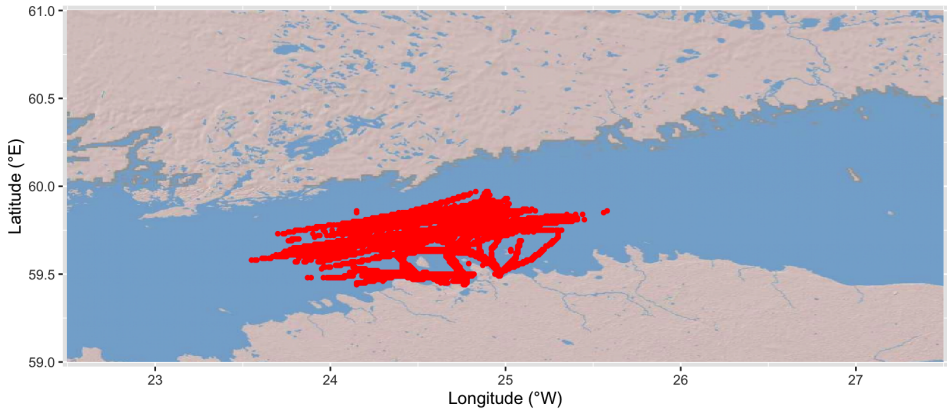


Figure 7: Receiver coverage

The radio unit of the R500Ni sends the collected data to the computer unit via a serial protocol. All decoded messages, collected by a self-developed script, are deposited hourly in separate files, and a scheduled task sends these files daily to the data collection server. This method provides safe storage for the collected data and ensures small file sizes for faster data loading.

To handle the large volume of data securely, a storage server was set up at the NATO Cooperative Cyber Defence Centre of Excellence. This server establishes a reverse SSH connection to the data collector and stores the data sent by the receiver.

5.2.2 Data Preparation

The data preparation phase involved merging the one-hour recorded files into a single file and converting timestamps to UNIX time for better dataset management. A detailed data cleaning process was then performed to identify and correct errors in the collected data.

During analysis, it was found that the receiver sometimes transmitted empty NMEA sentences due to malformed messages. These messages were systematically examined, followed by statistical analyses to identify patterns. Such anomalies were treated as distinct cases for separate analysis, as will be detailed in Section 5.2.4.

All methods ensured consistency in the handling of data anomalies, leading to a rigorous evaluation of the dataset.

5.2.3 Data Analysis

The data collection period spanned 181 days, from 8 September 2022, 00:00, to 8 March 2023, 00:00. Over this period, 71,251,552 AIS messages were collected. Within this dataset, 1,058,784 messages were identified as malformed, and 1,145 records were not supported by our parser. These unsupported records may have passed checksum validation but had incorrect bit lengths for their message type, which we classified as corrupted.

A total of 342,301 messages exhibited the presence of out-of-scope values. These could result in the issues mentioned above or may have been transmitted intentionally. Section 5.2.5 will provide a detailed explanation.

In total, 3,779 unique MMSI numbers (representing different ships) were identified. The computed mean receiver-transmitter distance was $D = 10.364$ NM, and the median was $M = 8.0$ NM.

5.2.4 Malformed Packet Analysis

We investigated the number of received packets with incorrect checksums. The null-hypothesis was that there is no correlation between the number of malformed packets and i) the maximum reception distance, ii) the median reception distance or iii) the total number of received packets during a given period. The alternative hypothesis was that there is a correlation between these variables. To test this, we aggregated the different values—such as the number of broken or malformed packets and reception distances—over four-hour periods and calculated the values. Table 6 summarises the results of the correlation analysis.

For the correlation between the broken packets received daily and the maximum reception distance, the correlation coefficient was (r) r = 9.4×10^{-2} (a very weak correlation), with p = 5.569×10^{-10}, which is below the significance level $\alpha = 0.05$. Although the correlation between the number of broken packets received daily and the MRD is statistically significant (r = 0.094, p < 0.001), the effect size is extremely small, suggesting that the maximum reception distance explains very little of the variation in the number of broken packets.

For the correlation between the number of received malformed packets and the median reception distance (MRD), we observed a negligible negative correlation (r = -0.006, p = 0.700), above the significance threshold ($\alpha = 0.05$), indicating no statistically significant linear relationship between the two variables. Given the extremely small magnitude of the correlation coefficient and the lack of statistical significance, we conclude that the median reception distance does not appear to be associated with the number of malformed packets received.

The correlation analysis between the number of received malformed packets and the total number of received packets revealed a moderate positive correlation (r = 0.446), which was statistically significant (p = 2.2×10^{-16}), well below the conventional significance threshold of $\alpha = 0.05$. The moderate effect size suggests a meaningful association between these two variables.

We can summarise the results as follows. The analysis shows that the number of malformed packets and the total number of received packets have a moderate correlation, but there is no correlation between the number of malformed packets and the reception distance, meaning that reception anomalies do not influence the number of broken packets.

Since the receiver only indicates the existence of broken packets and does not provide further information about their transmitter or why the integrity check failed, this

cannot be investigated further. We cannot prove that only messages from long distances were corrupted, but we can infer that these signals interfere with those transmitted closer, potentially causing similar results.

Table 6: Results of the correlation analysis

Values	Correlated variables		
	Maximum reception distance	Median reception distance	Number of total packets
t	6.216	-0.385	32.85
df	4343	4343	4343
p-value	5.569×10^{-10}	0.700	2.2×10^{-16}
correlation	0.094	-0.006	0.446
95% conf.	0.064	-0.036	0.422
interval	0.123	0.024	0.470

5.2.5 Error Packet Analysis

During the data collection period, we collected 342,301 error messages with correct CRCs but with invalid values—for example, latitude values exceeding 180 degrees. This can occur if a packet changes but the CRC remains correct, or if the packet is intentionally transmitted. We analysed the number of these packets, as shown in Figure 8.

Most of the packets (277,824 messages), indicated by the blue line in Figure 8, were transmitted by a manned vessel traffic service with MMSI: 2766160, located at N59.64589° / E25.49998°. The type of message transmitted was 17, which is used by base stations to transmit differential corrections for GPS. This service was started on 13 October 2022 at 10:48:18 and, in accordance with the standard, transmitted latitude and longitude values 91° and 181°, respectively.

Of the remaining 64,477 packets, 63,009 were transmitted by 120 different ships reporting positions of lat=91° and lon=181°. One of the most significant transmissions occurred on 3 November 2022, when a burst of 32,770 navigational information messages was transmitted by MMSI: 276197000, EVA320 (High-Speed Craft). However, according to its AIS messages, the ship was moored from 31 October 2022 at 11:53:41 in the port of Hundipea, Estonia (59°27'33.3"N 24°43'14.1"E), and had suspended its AIS transmissions from 1 November 2022 at 17:07:19 to 5 November 2022 at 00:38:59. These packets were transmitted intentionally or due to a transmitter failure.

The remaining 1,468 packets, with message types 1, 3 or 18, used for navigational information reporting, contained random positions. These packets were most likely corrupted due to propagation anomalies.

5.2.6 Reception Distance Analysis

The median receiver-transmitter distance in the AIS data introduced in Section 5.2 was D = 10.364 NM, while the median was M = 8.0 NM. To highlight the special characteristics of signal reception, we grouped the unique MRDs hourly and visualised them in Figure 9a.

This figure shows that the MRD was most often 7.5 NM. Most transmissions were observed for distances between 2 and 21 NM, but some transmissions were recorded at longer distances of 26 and 29 NM. During these periods, the MRD increased or doubled, and in some cases, we observed unusually long distances. We classify these occurrences as propagation anomalies caused by solar or weather-related activities.

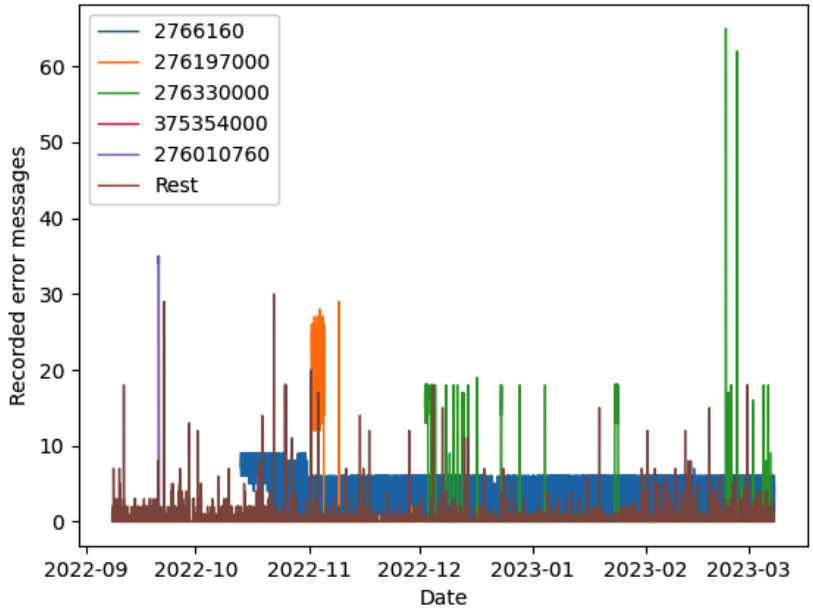
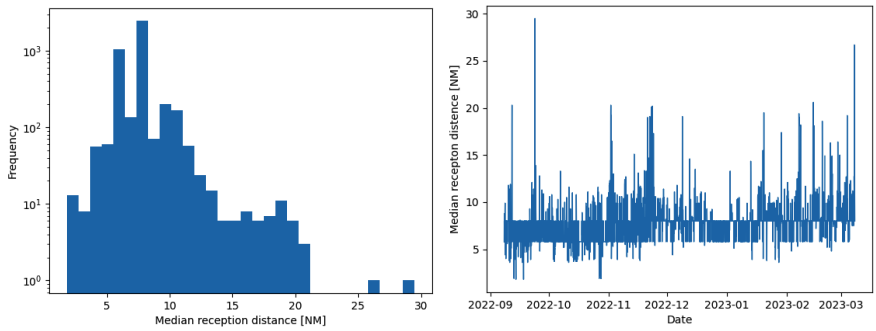


Figure 8: Number of recorded error messages



(a) Histogram of the median reception distance

(b) Median reception distance

Figure 9: Median reception distance analysis

The histogram of MRDs is shown in Figure 9a, and their values over time are shown in Figure 9b, where MRDs are calculated in hour-long intervals. In Figure 9b, peaks appear on 23 September 2022 and 7 March 2023. Our analysis indicates that these peaks were due to a single record stored during those hours, leading to a notable increase in the median value; therefore, we omitted these hours from further analysis.

The following maximum median distances were documented: 20.6 NM between 14:00 and 15:00 on 14 February 2023; 20.3 NM between 01:00 and 02:00 on 12 September 2022; 20.3 NM between 01:00 and 02:00 on 2 November 2022; and 20.2 NM between 12:00 and 13:00 on 23 November 2022.

During these days, the MRD showed a significant increase (Figure 10, green area) compared to the regular days (Figure 10, magenta area), although no transmissions were received from extremely distant locations.

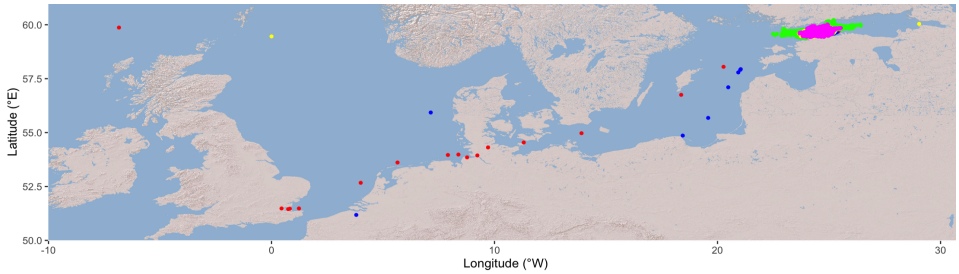


Figure 10: The position of the AIS transmitters

Figure 11 shows the histogram of the maximum reception distance grouped by hour. It indicates that, in most cases, the coverage was below 100 NM, but there were periods when coverage extended to 600, 900 and even 1200 NM.

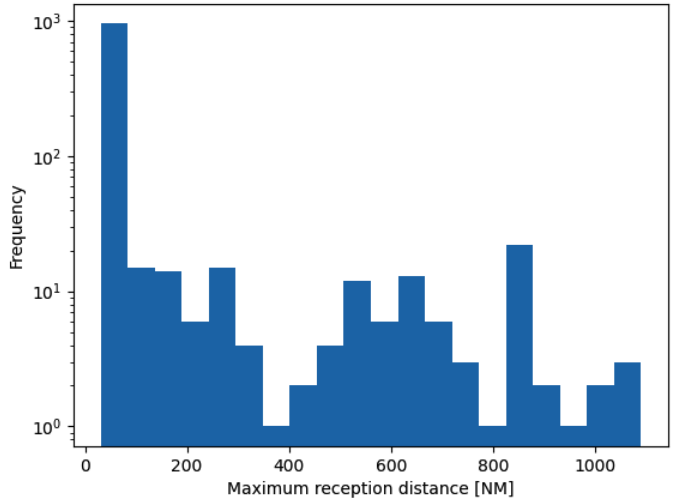


Figure 11: Histogram of the maximum reception distance

The analysis of maximum distances is summarised in Figure 10. The coverage was extremely wide on 8 October 2022: 1090.4 NM (red dots), on 10 December 2022: 993.6 NM (blue dots) and on 29 November 2022: 861.1 NM (yellow dots). However, it should be noted that numerous signals were detected from distant sources, contributing to the observed phenomena. The locations of the anomalous transmitters can also be seen in Figure 10.

No significant solar activity was recorded during the same period, which suggests that enhanced ionospheric propagation cannot be attributed to solar flares, geomagnetic storms or associated phenomena. However, atmospheric and meteorological conditions prevailing at the time may have contributed to the formation of a sporadic E layer (Es), which can significantly affect radio wave propagation.

The Es layer is a transient and irregular layer of increased ionisation that forms in the lower part of the ionosphere, typically at altitudes between 90 and 130 km. Unlike the more stable and predictable layers of the ionosphere, such as the E and F layers, the Es layer occurs unpredictably and is often influenced by wind shears, gravity waves and other

atmospheric dynamics in the mesosphere and lower thermosphere.

When present, the Es layer can reflect higher-frequency radio waves, particularly those in the VHF range, which typically includes frequencies from 30 to 300 MHz. This reflection capability allows VHF signals to travel far beyond the normal line-of-sight limits, sometimes resulting in long-distance reception over hundreds or even thousands of kilometres. Therefore, it is plausible that the observed anomalous propagation during this period was facilitated by the formation of an Es layer, enabling enhanced signal reach despite the absence of heightened solar activity.

5.2.7 Contribution

During a six-month period, we collected a publicly available AIS dataset [183], which contains more than 71 million AIS messages transmitted by 3,779 unique ships. This unique dataset can be used for research, such as verifying anomaly detection methods, as will be described in Section 7.

The high-level analysis of the dataset provided an overall picture of the behaviour of real-world AIS data. We found that 1.5% of the messages were corrupted (failed the CRC check), likely due to propagation anomalies over long distances that degrade packet integrity.

The results highlighted that reception distance can be influenced by solar and weather conditions, which are only partially predictable. This makes distinguishing between propagation anomalies and malicious activity difficult. At the same time, navigation devices can omit signals received from beyond a certain distance, limiting the impact of this phenomenon on navigation safety.

5.3 MarCyb Dataset

Section 3.1.2 introduced several publications dealing with the research environment for maritime cyber research. As summarised in Table 7, only limited literature has been published dealing with testbeds, even fewer studies provide publicly available datasets. Moreover, these datasets address only a limited range of attack types. The development and design of defensive mechanisms, such as IDSs, require public datasets with various types of attack to facilitate effective benchmarking of existing solutions. In addition, IDSs must distinguish between malicious activities and system failures, as each triggers distinct incident-handling processes involving different teams [180]. Therefore, to meet real-world requirements, datasets should include both various system failure cases and malicious activities.

The Hybrid Cyber Research Environment—introduced in Section 4.4—was used to address the need for a publicly available dataset. During the creation of the dataset, a series of the most common application- and network-layer cyberattacks [74, 91, 81] were executed within this laboratory environment, as shown in Table 8.

5.3.1 Network Attacks

MITM Attacks: In an MITM attack, an attacker secretly intercepts and potentially alters communication between two parties. In this scenario, Address Resolution Protocol (ARP) spoofing was used to intercept the data transmission between the source and the ECDIS. A self-developed script manipulated the ARP tables of the endpoints, redirecting network traffic through the researcher's computer and allowing the researcher to inspect and modify the contents of the packets before sending them to the intended recipient.

Replay attacks: A replay attack involves capturing network traffic between two

Table 7: Comparison to related works

Reference	Simulated components	Main attack scenarios	Protocols	Dataset
Longo et al. [125]	RADAR, EPFS, AIS, SDME gyroscope, compass, ship and hydraulic system, ECDIS	MITM, DoS, malware attacks	NMEA 0183, Navico BR24, ASTERIX Cat-240, MODBUS	No
Amro et al. [43]	AIS, GPS, Network simulation, OpenCPN	Network sniffing, service scanning, ARP poisoning, NMEA manipulation.	NMEA	No
Wolsing et al. [196]	Radar, IBS, GNSS, BC, AIS, OpenCPN	MITM attack on radar network	Navico BR24, AIS, ARPA	Yes
Becmeur et al. [53]	Propulsion, engine control, navigation systems	DoS, attack against navigation, propulsion and SCADA systems	ModBus, DNP3, S7	No
Raimondi et al. [150]	Ship operations and shore -side centre components, gyrocompass	NMEA packet injection, data tampering	NMEA 0183	No
Visky et al. [188]	ECDIS, RADAR, weather, operational situation, AIS, 10+ OT sensors	Network sniffing, ARP poisoning, network data manipulation.	NMEA 450, Transas proprietary protocol	No
Sicard et al. [162]	Propulsion, artillery control, trajectory generator, energy	Network attacks and process attacks	Modbus, Profibus	No

entities and retransmitting it later, sometimes with modified data. Unlike real-time MITM attacks, replay attacks do not intercept and alter live traffic but exploit previously recorded communication. During dataset creation, a replay attack was successfully carried out on the AIS messages, changing the name and location of the vessel. The Tcpdump [12] tool was used for traffic capture, Tcprewrite [31] for packet modification and Tcpreplay [30] for retransmission.

Denial of service attacks: A DoS attack aims to overwhelm a network or application

by flooding it with excessive traffic, either consuming network bandwidth or exhausting computational resources. In the lab, DoS attacks were executed using T50 [29], hping3 [13] and Metasploit [22], generating a flood of UDP packets that did not conform to the NMEA format. These attacks targeted the OpenCPN navigational application to evaluate its ability to handle high volumes of invalid packets.

Scanning attacks: Various scanning techniques were tested in the lab using nmap and masscan tools:

TCP and UDP Port scanning: This method identifies open ports and accessible network services. TCP scanning is more reliable due to its three-way handshake mechanism, which confirms whether a service is active. In contrast, UDP scanning is less conclusive, as UDP services do not establish connections and may not always respond to probes.

Scanning with Nmap Scripting Engine (NSE): NSE scripts automate vulnerability detection and collect additional information about network services, enhancing security assessments through targeted scanning.

Fuzzing attacks: Unlike the attack types mentioned above, fuzzing is a software testing technique that injects unexpected or malformed inputs to detect vulnerabilities. This method is often used in labs during the security validation of devices and software stacks.

In network security, protocol fuzzing modifies network packet fields to contain abnormal values, helping assess how well applications handle unexpected input. This technique can reveal security flaws, such as buffer overflow vulnerabilities or crashes caused by specific protocol anomalies. During dataset creation, protocol fuzzing was applied to the NMEA protocol to test the resilience of the OpenCPN navigational application.

5.3.2 Application attacks

Khandker et al. [108] conducted an in-depth study on cyberattacks targeting the AIS system. Based on their work, application-layer attacks were implemented and executed at the network level against the ECDIS within our test environment. In addition, the scope of attacks was expanded by manipulating various sensor values, including wind, velocity and depth sensors, to compromise the navigation system from multiple angles.

Man overboard (MOB) attacks simulate an emergency scenario in which a position is falsely marked as the location where an individual has fallen overboard, triggering a rescue operation. The MOB message, an AIS distress signal, includes coordinates and generates immediate alerts for nearby vessels. This attack can result in false alarms, leading to the unnecessary deployment of rescue forces and disruptions for other ships.

Spoofing involves the manipulation of AIS data transmission to mislead other vessels or monitoring systems regarding a ship's position, identity or other critical information.

Visual navigation disruption (VND) attacks occur when false targets appear on navigation displays, potentially confusing the operators of the vessels even if no alarms are triggered. We conducted extensive spoofing and MOB attacks by injecting UDP packets into the network and embedding malicious NMEA sentences to create visual navigation disruptions.

Collision alert attacks involve injecting fake ship positions into AIS signals near a target vessel. The fabricated data forces the targeted ship to take evasive manoeuvres or alter its course unnecessarily.

Logically invalid data encoding attacks exploit inconsistencies in the data of interdependent ships. For example, an unrealistic change in a vessel's position that contradicts its speed can be used to create confusion or disrupt operations.

Table 8: Malicious activity in the MarCyb dataset

Attacks	Targeted assets/protocols	Variations/types
Network attacks		
MITM	ARP tables, OpenCPN, AIS	AIS target modification (vessel name, location change)
Replay	OpenCPN, AIS	AIS target injection
Fuzzing	OpenCPN, AIS	Protocol fuzzing
DoS	OpenCPN, Network	Network flooding
Scanning	UDP, TCP, OS	Aggressive scan, fast scan
	Hidden port scan	Low-rate scan
Application attacks		
Visual navigation disruption	OpenCPN, AIS	Too many AIS and MOB targets on the screen
Spoofing	OpenCPN	Fake sensor values
AIS target flooding	OpenCPN, AIS	Fake AIS target
Man overboard flooding	OpenCPN, AIS	Fake MOB target
Collision alert	OpenCPN, AIS	Fake collision alert on the screen
Logically invalid data encoding	OpenCPN, AIS	Logically invalid sensor values

Files without attacks
48-hour capture
11.5-hour capture containing only UDP-encapsulated sensor data
48-hour capture without external communication

File with sensor failure
File with sensor malfunction

5.3.3 Contribution

The main contribution of this section is the creation and introduction of the unique MarCyb dataset [192], which represents an advancement in the domain of maritime cybersecurity, designed to support academic research and education. The dataset provides a comprehensive collection of network traffic data specific to maritime systems. MarCyb includes not only benign traffic that reflects standard operational behaviour but also data generated by a variety of malicious activities. These include simulated cyberattacks targeting key maritime components such as address resolution protocols (ARP spoofing), network bandwidth (e.g. DoS attacks) and navigation applications (e.g. manipulation or spoofing of AIS signals). By encompassing both normal and adversarial scenarios, MarCyb enables the development and evaluation of robust cybersecurity solutions, facilitates the training of machine-learning models, and fosters a deeper understanding of maritime-specific cyber threats.

5.4 Summary

In this section, two developed and published datasets were introduced to support further studies in maritime cybersecurity. These datasets provide valuable resources for on-board protocol vulnerability analysis, software security research and operational-value anomaly detection. By making these datasets publicly available, this research aims to contribute to the broader cybersecurity community, fostering collaboration and innovation to protect maritime systems against emerging threats.

The next sections will detail how these datasets were used in practical cybersecurity

research, specifically focusing on anomaly detection. By demonstrating real-world use cases, this thesis aims to highlight the effectiveness of these tools in addressing cybersecurity challenges within the maritime industry.

6 Maritime Protocol Vulnerability Analysis and Exploitation

6.1 Motivation and Novelty

As maritime operations increasingly depend on digital systems, the security of shipboard software and communication protocols is a growing concern. The literature review highlighted the need for a comprehensive vulnerability analysis of maritime software and protocols, as cyber threats targeting these systems pose significant risks to navigation, operational efficiency and safety.

Vendors rely on proprietary communication protocols to develop networked devices. During this process, they aim to find a balance between meeting the industry's needs and minimising the complexity of the protocol, often without sufficient consideration of cybersecurity [140]. The main reason for developing the protocol is to optimise the communication performance of the product. To protect market share, the communication specifications are kept closed and not made publicly available.

To reduce the attack surface of on-board control systems, the security of network services and protocols is essential, as flaws in communications can lead to system-wide vulnerabilities. To help developers with this task and ensure interoperability, a rigorous standardisation process is in place, which should also consider security. However, this is not always the case, and communication protocols used aboard ships have cybersecurity flaws.

This section contributes to the field by analysing the vulnerabilities of maritime communication protocols, particularly the proprietary NaviNet protocol and the IEC61126-450 standardised protocol.

Since NaviNet is a closed protocol, this section reveals details that can be used for defence devices, such as dissector development. Using these novel findings, various attacks were executed against an ECDIS to demonstrate weaknesses in the protocol and the device, and possible defence methods are proposed to enhance the security and resilience of shipboard communication systems.

As discussed in Section 3.2.2, automatic protocol reverse engineering (APRE) was applied to the CAN protocol, which is commonly used in the automotive industry. As a novel contribution, this section evaluates how effectively APRE can be applied to a maritime protocol, showing that the method can reduce manual labour during defence development.

6.2 The NaviNet Protocol

NaviNet is a closed proprietary protocol developed by Wärtsilä Corporation [9], a leading vendor in the maritime sector. The protocol relies on IEC61162-1 (introduced in Section 2.4.2) but uses an Ethernet network for data transfer.

6.2.1 Manual Protocol Reverse Engineering

A reverse engineering (RE) process was conducted to uncover the details of the closed protocol. To create a dataset for RE, the multipurpose research environment (introduced in Section 4.2) was used.

The manual RE process revealed that, after the successful establishment of communication, data exchange consists of two main sessions: first, a set of system-related information is exchanged; then, the data source starts sending sensor data via TCP push packets.

Since the protocol embeds structures in the form of IEC61162-1 sentences, the reverse engineering focused solely on the header generated by the DCU, as the rest of

the payload is identical to the original messages received from the sensors. This time-consuming manual process resulted in the protocol structure shown in Table 9.

Table 9: Proprietary communication packet structure

Offset	Function	Example value
00	Full length of the payload	44 00 00 00
04	Unknown/static	00
05	Timestamp Continuously increasing value	fe a7 cc 6e 9c 00 00 00
13	Sender's (DCU) IP	0a 8c 21 07
17	Message type	01
18	Channel number arrived	04
19	Length of 61162-1 data	31 00
21	Static	13 00
23	IEC61162-1 data	24 56 4d 2c 0d 0a

The efforts dedicated to manual reverse engineering highlighted the need for a cheaper solution, and the results enabled testing and validating automated protocol reverse engineering (APRE) on this protocol.

6.2.2 Automated Protocol Reverse Engineering

Reverse engineering a proprietary protocol typically involves manually identifying the structure of the protocol header. However, this process can also be automated using machine learning techniques, specifically by training a linear regression model on the bit-level representation of packet payloads. The idea is to discover which bits in the packet header are most strongly correlated with specific known fields. In this research, the payload length and the timestamp fields were tested.

In the visualisation of the results (see Figures 12, 13, 14 and 15), the regression coefficient of each bit indicates its influence on the predicted variable. The grey bars in the figures denote the ground truth (i.e. the actual location and strength of the real field), while the blue bars indicate the coefficients learned by the model. For fields expected to be unsigned, such as payload length and timestamp, the regression model was constrained to produce only non-negative coefficients, reflecting the nature of these values.

Figure 12 illustrates the application of this method to predict the length of the payload of the packet, which is a known quantity. The model identified strong coefficients at byte offset 0 and byte offset 19. However, since the payload length is represented in a single byte and the value at byte offset 0 matched the actual length, this offset was selected as the correct field. Similarly, in Figure 13, the model was trained to predict the IEC61162-1 data length and revealed a significant correlation at byte offset 19, which corresponds to the known location of this field in the proprietary format.

Both figures show that the model was successfully trained and can accurately predict the payload and data length.

We used the relative arrival time of the packet to infer the *timestamp* field in Figures 14 and 15. The timestamp field in the payload occupies 8 bytes. Linear regression cannot effectively detect patterns in lower-order bytes (bytes 5–6), as they represent milliseconds. Meanwhile, higher-order bytes (bytes 9–12) remain unobserved in the dataset because the trace only covers a duration of 100 seconds. Figure 14 shows that the timestamp value is regularly 0, as only the DCU sends the packet with valid

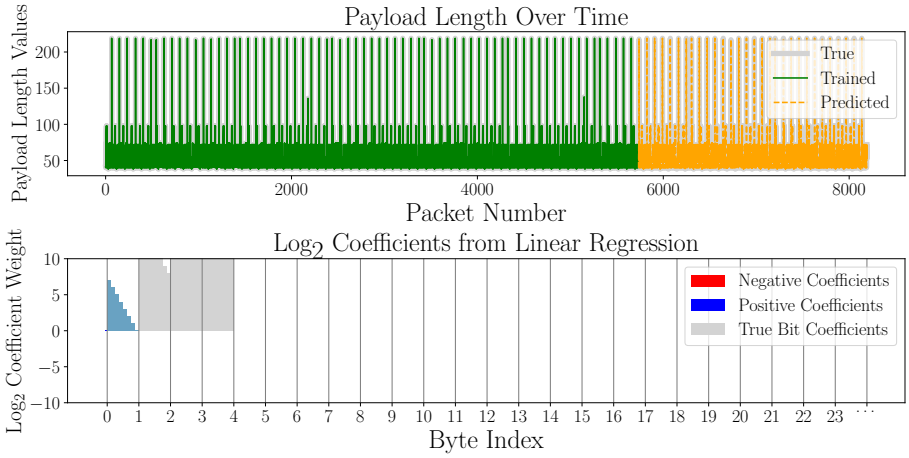


Figure 12: Inferring with payload length

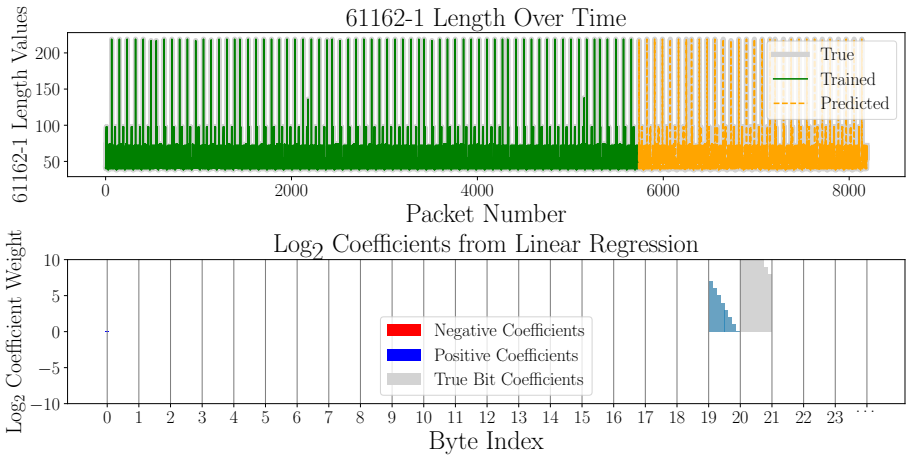


Figure 13: Inferring with payload and sentence length

timestamps, while the server sends packets with a 0 timestamp. Figure 15 shows the case where these outliers (packets with zeros in the timestamp field) are removed. Both figures show that the model was successfully trained and can accurately predict the payload and data length.

These results show that, with the help of APRE, the role of the different bits in the communication can be identified, making the reverse engineering process much easier. In addition, with these results in hand, the fields can be predicted over time, which can be used for anomaly detection.

6.2.3 Possible Mitigation Methods

Since the header of each packet includes the sender's IP address, it is essential that the receiving device performs a verification step to ensure the authenticity of the source. Specifically, the receiver should check whether the packet actually originated from the claimed IP address. This validation step helps prevent certain types of spoofing attacks, where a malicious actor could spoof the sender's IP to impersonate a trusted source. By

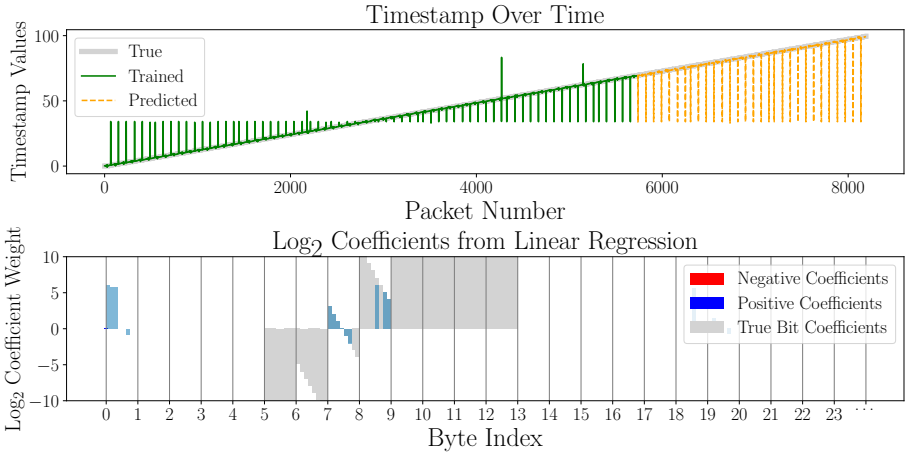


Figure 14: Inferring with the timestamp field

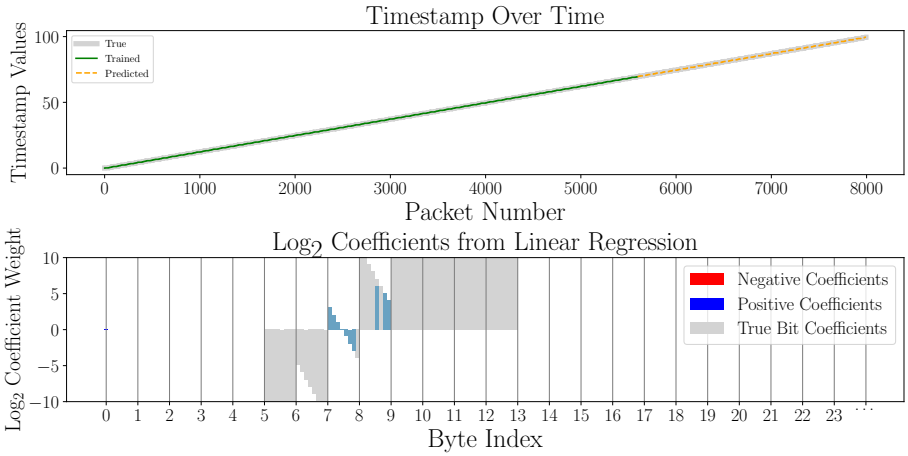


Figure 15: Inferring with timestamp field without answer packets.

confirming the match between the actual source and the declared IP in the header, the system can strengthen its security posture against unauthorised or deceptive communication attempts.

In addition to source validation, the timestamp field embedded in the packet should be leveraged for temporal verification. The receiver should assess whether the packet's timestamp falls within an acceptable time window, ensuring that only timely and relevant messages are processed. Packets with timestamps that indicate they are outdated or expired should be promptly discarded. This mechanism serves as a safeguard against replay attacks and helps maintain the integrity and freshness of communication, ensuring that stale or delayed data does not affect system behaviour.

6.2.4 Contribution

One of the main contributions of this section is the reverse engineering of the closed NaviNet protocol. This result enables the development of a dissector, which is essential for application-level anomaly detection.

The next contribution is the development of the ARPE method, which can support the dissector development or be used directly for anomaly detection. By learning which bits most strongly influence specific field values, this approach offers a valuable tool for automating the reverse engineering of unknown protocol headers. Therefore, even with limited knowledge of the communication, sensor values can be predicted, which helps with anomaly detection. The structure of the communication allowed us to confirm the effectiveness of the linear regression model in identifying field boundaries and correlating packet structure with known quantities.

The third contribution of this section is the recommendation of measures to improve the cyber resistance of the protocol.

These results allowed us to demonstrate the weaknesses of the protocol. Their exploitation will be discussed in the following section.

6.3 NaviNet Protocol's Exploitation

The NaviNet protocol, described in Section 6.2, is a vendor-specific closed protocol widely used in marine transportation. The reverse engineering process revealed the details of the protocol and showed that the vendor had extended the legacy IEC61162-1 data sentences, used to transport the sensor data, with an additional header. The combined data are transported using TCP push packets. It is worth mentioning that, since the NaviNet protocol is transmitted in plaintext over the underlying TCP protocol, it is susceptible to various cyberattacks.

6.3.1 Addressed Attacks

We successfully carried out the following attacks against an ECDIS by exploiting weaknesses in the NaviNet protocol. These attacks relied on the results from the previous section, as a successful attack requires deep knowledge about the closed protocol.

Replay attack: This type of attack involves retransmitting one or more previously captured packets. To perform the attack, relevant packets were extracted from network traffic and replayed using Tcpreplay [111]. Due to the nature of the TCP protocol, the MFD rejected the replayed packets, because Tcpreplay does not modify the headers of the packets before replaying them, preventing the formation of valid TCP sessions [111]. However, the replay attack was successfully executed using our custom-built DCU simulator application, which allowed the creation of a valid session and the replay of the original IEC61162-1 sentences.

Injection attacks: In a false data injection scenario, an attacker with sufficient knowledge of the protocol injects deceptive data. Similarly, a spoofing attack occurs when a programme or individual impersonates another entity by fabricating data to gain trust [102, 128]. During testing, specific *sensor values*—including wind speed and direction, water depth, heading, and turning rate—were changed to predefined values. Meanwhile, the *data channel* and *timestamp* fields were dynamically generated. These crafted packets were sent to the MFD, which failed to recognise the intrusion. No alerts or indications of abnormal behaviour or incorrect values were observed.

Modification: In a modification attack, data in transit is intercepted by an attacker, altered and then forwarded to the recipient. To evaluate this attack vector, we executed an MITM attack using ARP spoofing to redirect the communication through the researcher's system.

Eavesdropping: Since the protocol transmits data in plaintext without encryption, eavesdropping is straightforward. To demonstrate this vulnerability, an ARP-based MITM

attack was carried out, allowing communication interception and exposure of sensitive information.

6.3.2 Result analysis

Several threat modelling methodologies, such as the CIA triad (confidentiality, integrity and availability) [195] and STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege) [131], provide a framework for various attacks. To cover these categories, as described above, four attacks were conducted against the system: replay, injection, modification and eavesdropping.

The following explains how each attack outcome affects the relevant STRIDE categories.

Spoofing: The replay attack, which used pre-recorded network traffic, was successful. The MFD displayed the replayed data regardless of the actual sensor value. The injection attack was also successful: the MFD showed the data from the injected packets regardless of the original sensor value. When packets were injected at a rate exceeding five times a second, they *unnoticeably* suppressed the original sensor values on the ECDIS. The ECDIS injection attack was likewise successful; the MFD displayed the injected fake AIS targets, as shown in Figure 16. We can conclude that the protocol does not defend against spoofing.

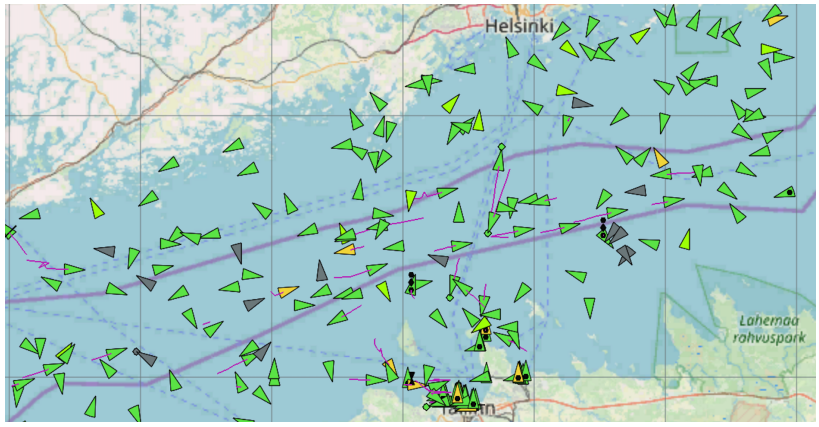


Figure 16: ECDIS screen flooded with fake AIS targets (green) caused by an injection attack

Tampering: As noted above, the protocol is defenceless against replay or spoofing attacks; it offers no protection against tampering, as data can be altered without authorisation.

Information disclosure: Eavesdropping was successful against the protocol, which means that the protocol does not meet confidentiality-related security goals. By using a network traffic analyser application, the content of the communication could be revealed, as shown in Figure 17.

Repudiation: Repudiation refers to a situation where a user denies having performed an action and there is no way to prove otherwise. This applies to the protocol under examination, as it does not support digital signatures or authentication records.

Denial of service: Although this thesis focuses on application-layer protocols, it is worth noting that the analysed proprietary protocol, while relying on TCP, operates with TCP push packets that are not buffered by TCP/IP stack. This allows an attacker to overload the application rapidly. These conditions make on-board communication

```
0000  02 00 00 00 45 00 00 5c  9e d0 40 00 80 06 00 00   ····E··\ ··@·····
0010  0a 8c 21 07 0a 8c 21 07  c3 63 ef 2c ee 6a e3 5f   ··!···!· ·c·,·j·_
0020  86 b2 b6 80 50 18 27 f6  d7 c7 00 00 30 00 00 00   ····P·'· ····0···
0030  00 72 51 d8 6e 9c 00 00  00 0a 8c 21 07 01 03 1d   ·rQ·n··· ···!····
0040  00 13 00 24 56 42 56 48  57 2c 38 39 2e 30 2c 54   ···$VBVH W,89.0,T
0050  2c 2c 2c 30 2e 31 37 2c  4e 2c 2c 2a 34 30 0d 0a   ,,,0.17, N,,*40··
```

Figure 17: Original information represented in open format

unreliable. Sensors or data aggregators cannot check the validity and reliability of the incoming data, and the same applies to the navigation system without content control: the ECDIS was flooded with packets containing modified sensor values, as shown in Figure 18, resulting in a denial of service due to the vulnerabilities described above.

Figure 18: Original information overwritten, causing a denial of service in the navigation system

6.3.3 IEC61162-450 Protocol Exploitation

Similar attacks were carried out against a navigation system that used the standardised IEC61162-450 introduced in Section 2.4.3. As shown in Figure 19, the protocol transmits sensor data in legacy format encapsulated in the UDP protocol. Compared with the previously discussed proprietary protocol, this standardised protocol is even more vulnerable [185].

```
0000  01 00 5e 40 00 01 00 01  c0 29 ae 2d 08 00 45 00   ··^@···· ·)·-··E·
0010  00 66 64 29 40 00 01 11  fa 04 0a 8c 21 0c ef c0   ·fd)@··· ····!···
0020  00 01 b4 9a ea 61 00 52  08 59 55 64 50 62 43 00   ·····a·R ·YUdPbC·
0030  5c 73 3a 53 49 30 31 30  31 2c 6e 3a 31 31 30 2a   \s:SI010 1,n:110*
0040  31 42 5c 21 41 49 56 44  4d 2c 31 2c 31 2c 2c 41   1B\!AIVD M,1,1,,A
0050  2c 31 33 38 4d 44 46 30  30 31 54 30 30 36 4a 6c   ,138MDF0 01T006Jl
0060  30 30 4c 52 32 48 51 73  3a 50 35 30 6c 2c 30 2a   00LR2HQs :P50l,0*
0070  36 33 0d 0a                                       63··
```

Figure 19: Original information represented in open format

6.3.4 Contribution

Several attacks were successfully executed against the ECDIS by exploiting vulnerabilities in both proprietary and standardised protocols, demonstrating their limited resistance to cyberattacks.

This result highlights the importance of protocol hardening, as recommended in Section 6.2.3.

Modified sensor values—regardless of the attack type—can compromise automated navigation systems, such as track and course control, which can lead to severe safety

consequences, including grounding or collision. Furthermore, altered control values can cause financial losses (e.g. through delivery delays), environmental harm (e.g. increased fuel consumption or oil spills following accidents) or safety hazards (e.g. loss of stability due to incorrect ballast management).

6.4 Summary

Ensuring the cybersecurity of shipboard communication protocols is crucial for the safe operation of modern maritime navigation systems.

This section presented a detailed analysis of the manually reverse-engineered NaviNet protocol. The protocol analysis offers a novel contribution, providing insights previously undocumented in the public domain. By systematically deconstructing the protocol's structure and behaviour, this work supplies valuable information that can support the development of network intrusion detection systems (NIDS) capable of analysing application-layer data more effectively.

A key aspect of this work is the innovative application of automated protocol reverse engineering (APRE) techniques to the NaviNet protocol. Although the protocol was primarily analysed manually, the findings were cross-validated through APRE to demonstrate its practical applicability. This dual approach not only confirms the accuracy of the reverse engineering process but also highlights how APRE methods can be leveraged to handle complex proprietary protocols like NaviNet.

The section examined the vulnerabilities of both a proprietary and a standardised shipboard protocol, demonstrating how these weaknesses can be exploited to compromise the ECDIS. The findings highlight the significant risks posed by cyber threats targeting maritime communication, as successful exploitation of these protocols can lead to navigational manipulation, operational disruptions and safety hazards.

To enhance the security of the NaviNet protocol, the sender's IP address and timestamp fields should be validated. Verifying the sender's IP helps prevent spoofing, while checking the timestamp ensures that only timely messages are accepted. Together, these checks improve resilience against unauthorised access and replay attacks.

Although anomaly detection at the network level has been widely researched and implemented, a critical gap remains in detecting anomalies in operational values, which are key parameters that directly influence ship functions and decision-making processes. Existing solutions primarily focus on identifying malicious network activity but lack the capability to assess deviations in operational data, which may indicate cyber incidents or system malfunctions.

To address this gap, the next chapter focuses on developing application-level anomaly detection methods tailored to shipboard OT systems. By analysing operational values rather than just network traffic, this research aims to improve the detection of subtle and sophisticated cyber threats that may otherwise go unnoticed. The proposed approach seeks to enhance maritime cybersecurity by providing a more comprehensive detection framework, ultimately strengthening the resilience of navigation and control systems against emerging cyber threats.

7 Anomaly Detection in Maritime Datasets

7.1 Motivation and Novelty

Maritime operations rely heavily on shipboard OT systems, which integrate navigation, communication and control processes. However, as highlighted in the related work and in the previous section, these systems remain vulnerable due to the inherent weaknesses in shipboard communication protocols and the fragile nature of navigation systems. Cyber threats targeting these systems can have severe consequences, including loss of navigation accuracy, operational disruptions and even safety hazards.

Although anomaly detection at the network level has seen significant advances, these methods often fail to address the specific challenges of OT systems in maritime environments. The unique operational constraints and data characteristics of OT systems require novel, application-level anomaly detection approaches that can effectively identify and mitigate cyber threats. Existing solutions lack the tailored detection mechanisms required for maritime OT, leaving a critical gap in securing shipboard systems.

This chapter aims to bridge this gap by developing application-level anomaly detection methods specifically designed for AIS, a key navigation system, to improve cybersecurity measures and strengthen the resilience of maritime infrastructure against emerging threats. Many papers have addressed this problem, as discussed in Section 3.3.2.

This chapter also highlights the irregularities caused by propagation anomalies, wind and weather conditions, and AIS transmission errors, which undermine the reliability of many anomaly detection methods.

While several research papers have been published proposing machine learning-based anomaly detection methods that require large datasets or logic-based rule systems built with the help of maritime experts, this chapter proposes an alternative machine learning (ML) approach using novel inductive logic programming.

The detection of anomalies in the speed and position of vessels, focusing on their voyage, is also discussed. The proposed method can highlight anomalies in the reported positions, based on calculated speed. Another novel proposal analyses the position changes of a ship at anchor. A deep understanding of these data helps improve the detection of position jamming.

As discussed in Section 2.3, the AIS is a key navigation device that improves operational awareness for the ship's crew. Its transmission covers up to 40 NM on open sea, which could help detect anomalies. To develop new detection methods, the AIS dataset introduced in Section 5.2 was used.

7.2 Inductive Logic Programming-based Anomaly Detection in AIS Data

Research literature on anomaly detection in AIS data has rapidly expanded, with new approaches ranging from statistical and rule-based methods [151, 86, 160, 43, 99] to neural network (NN)-based ML methods [63, 79]. However, an alternative group of ML methods based on ILP, first proposed by Muggleton [136] offers several advantages over other ML methods, such as the ability to generalise from a small number of training examples, natural support for lifelong learning and transfer, the ability to learn complex relational theories, and explainable of the learning results [71].

NUMSYNTH [89] is an ILP framework that learns programs combining relational logic with numerical reasoning. Unlike traditional ILP systems focused on symbolic Prolog programmes, NUMSYNTH handles both real and integer domains by learning numerical

constraints alongside logical rules. It uses a two-stage process: a programme search phase to generate partial logic programmes with numerical variables, followed by a numerical search using satisfiability modulo theories (SMT) solvers to identify values that fit the data. This approach enables the inference of constraints such as thresholds or inequalities across examples, allowing for joint reasoning over numerical relationships that standard ILP systems often miss.

NUMSYNTH is particularly well suited for anomaly detection in AIS data for several key reasons:

- AIS data are structured and mainly consist of numeric time-series data, such as speed, course, position (latitude/longitude), heading, timestamps and vessel ID.
- NUMSYNTH excels at handling structured numerical inputs and learning patterns over them.
- Vessel behaviour includes nuanced patterns (e.g. fishing loops, loitering and route deviations) that may be difficult for purely statistical models to detect.

7.2.1 Model Preparation

In the dataset used for this research, introduced in Section 5.2, vessels that crossed the edge of the AIS receiver coverage appeared only a few times in the dataset.

During the model preparation for the ILP setting, the positive examples were based on a small (but sufficient for ILP) subset of the dataset, while the negative examples were extracted from the same subset of data but selected based on violations of the accuracy constraint for consecutive vessel positions reported. In addition, fake vessels were injected into this dataset to simulate spoofing attacks.

Three key components were constructed during the preparation of the NUMSYNTH environment: the background knowledge, the examples and the bias language. The following properties were included in the *background knowledge*:

- Number of messages: The total number of AIS messages reported by a given vessel.
- Duration: The time period (in seconds) over which the vessel's AIS messages were received.
- Maximum and minimum speeds reported by the vessel.
- Mean and standard deviation of position error, calculated based on two factors: 1) the distance derived from longitude and latitude between two coordinates reported in consecutive messages, and 2) the distance computed using the reported time and speed.
- Predicate "Negative": Counts the number of messages that exceed the delta distance constraint (where the position error was higher than 20 metres).
- Predicate "Status": Indicates whether the vessel is moving or stopped, based on its reported speed (considered stopped if maximum speed is less than or equal to 0.4 knots).
- Predicate "Trajectory": Determines whether a vessel follows a straight or non-straight trajectory.

Example of background knowledge:

```
msg_nbr(sh_276636222, 66)
duration(sh_276636222, 1241.23)
max_speed(sh_276636222, 17.5)
min_speed(sh_276636222, 17.1)
mean(sh_276636222, -10000000.0)
standard_deviaton (sh_276636222, -10000000.0)
negative(sh_276636222, 66)
mean1(sh_276636222, 148.77)
standard_deviation1(sh_276636222, 2.13)
status(sh_276636222, moving)
trajectory(sh_276636222, straight)
```

During **sample preparation**, negative examples were vessels that sent data violating the accuracy constraint (i.e. a delta distance greater than 20 metres between positions reported in consecutive messages). Violations were caused by one or more of the following issues:

- Position reports outside the zone where the data were collected.
- Significant speed jumps between consecutive messages.
- Long time gaps between consecutive transmissions.
- Injected fake vessels simulating spoofing attacks.

Positive examples were vessels that did not violate any of these constraints.

The **bias language** file guided NUMSYNTH during learning by specifying which background predicates can be used, their roles (head or body clauses in the learned rules), variable types and input/output directions. It also constrained the search space by defining how predicates could be combined and how many numerical variables needed to be bounded for a valid rule.

NUMSYNTH used the "generate, test and constrain" approach [72], whereby it generated rules based on these declarations, tested them against the examples and constrained the search space iteratively. Rule size quantified the complexity of each learned logical rule or clause, impacting both interpretability and generalisation. The system started with rules of size 1 and incrementally increased rule size while respecting variable constraints. The search process continued until a valid rule was found or the maximum size limit was reached, ensuring that the system efficiently explored possible hypotheses without getting stuck in an exhaustive search.

A systematic refinement approach was used to optimise the rules generated over three learning epochs. Each epoch produced progressively more concise and accurate rules to classify vessel behaviour based on AIS data, culminating in a perfect classification. Performance metrics in the three learning epochs are summarised in Table 10.

During the epochs, the following rules were generated:

```
Epoch 1:
    vessel_id(A) :- standard_deviation1(A, C), geq(C, 0.254),
        standard_deviation(A, C).
    vessel_id(A) :- standard_deviation(A, C),trajectory(A,
        straight), geq(C, vessel_id(A) :- status(A, stop),
```

```
        mean(A, B), geq(B,  0.274).
    vessel_id(A) :- standard_deviation(A, D), leq(D, 0.439),
        status(A, stop).

Epoch 2:

    vessel_id(A) :- standard_deviation1(A, B), leq(B, 17.564),
        standard_deviation(A, C), geq(C, 0.222).
    vessel_id(A) :- standard_deviation1(A, C), status(A, stop),
        standard_deviation(A, C).

Epoch 3:
    vessel_id(A) :- standard_deviation1(A, E), mean(A, D),
        geq(D, 0.012), geq(E, 0.084), leq(E, 17.564).
```

Table 10: Summary of learning epochs: precision, recall and rule size

Epoch	Precision	Recall	TP	FN	TN	FP	Rule Size
Epoch 1	1.00	0.61	27	17	34	0	16
Epoch 2	1.00	1.00	44	0	34	0	9
Epoch 3	1.00	1.00	44	0	34	0	6

7.2.2 Results

Through iterative refinement, the rules were optimised to achieve perfect precision and recall scores (1.00). The final phase produced the most concise and effective rule set, accurately classifying vessel behaviour using key features such as trajectory, status and numerical metrics, including the mean and standard deviation of position.

7.2.3 Explainability

A key benefit of ILP is the explainability of the rules it generates based on the specified background knowledge and the language bias. These rules are human-readable and easily interpreted by domain experts. For example, rules that affect the trajectory, speed and position accuracy of the vessel naturally align with maritime operations, making them easy to review and justify. This transparency enhances trust, as users can clearly see why a vessel is flagged as behaving abnormally.

Unlike black-box ML models, the interpretability of ILP supports its use in real-world settings. It also allows for ongoing refinement, enabling experts to incorporate new data and insights over time, supporting a lifelong learning approach.

7.2.4 Contribution

The results highlight the potential of ILP to detect anomalies in AIS data that may signal spoof attacks. Applied to real-world data from the Baltic Sea, the approach successfully learned human-interpretable rules that distinguish normal from abnormal vessel behaviour. Its strength lies in generalising from limited examples while providing explainable results, which makes it well suited for operational maritime use.

The learned rules achieved perfect precision and recall on the AIS data. However, the limited geographic scope means that broader testing is needed to assess generalisability

under different maritime conditions.

7.3 Reported and Calculated Speed Difference-based Anomaly Detection

Since ships report their positions and speeds through AIS messages, a potential method for detecting anomalies is to compare the reported speed with the speed calculated from sequential position reports. Discrepancies between these two values can indicate possible errors, inconsistencies or unusual behaviour.

To explore this approach, the AIS dataset was thoroughly analysed, focusing on identifying variations between the reported speeds and those derived from geographic coordinates and timestamps.

As depicted in Figure 20, a subset of the fields was first selected, and then the data was filtered by date and message type to extract the relevant records. Only Class A messages transmitted by ships underway were processed between 8 September 2022 at 00:00 and 9 September 2022 at 00:00.

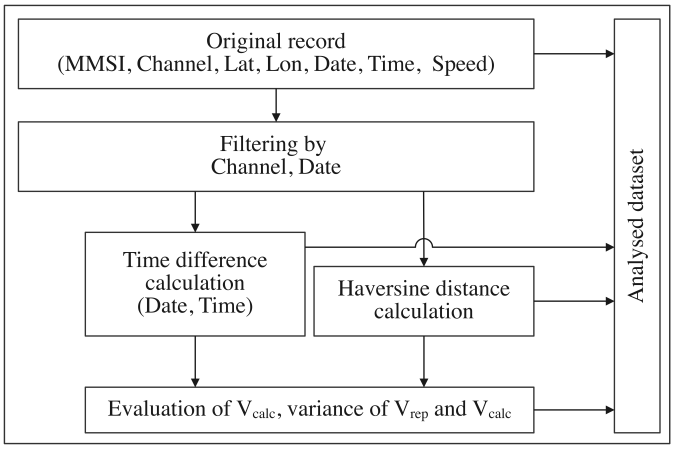


Figure 20: Flowchart of the data preparation

During preprocessing, the date and time information was converted into UNIX timestamps and appended to all records. These timestamps were then used to calculate the time differences between each pair of consecutive records, as well as the haversine distance between the corresponding positions. Based on these values, the calculated speed (V_{calc}) was determined (see Equation 1).

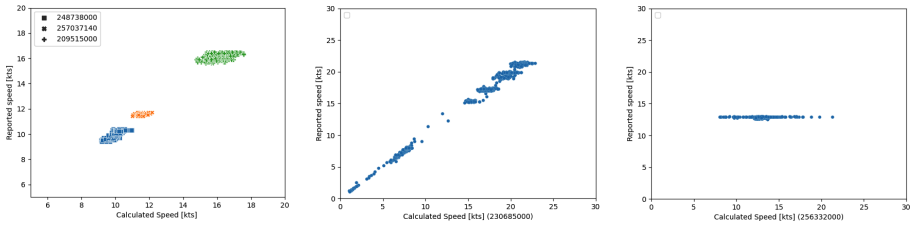
$$V_{calc}(n) = \frac{hav(loc(n+1), loc(n))}{(unix(n+1) - unix(n))} \tag{1}$$

The calculated speed (V_{calc}) was then attached to the original packets, which contained both the ship's positional data and its reported speed (V_{rep}).

With both V_{rep} and V_{calc} available, a series of tests were conducted to assess the usefulness of these data. In particular, we focused on measuring the strength of their correlation and calculating the difference between V_{rep} and V_{calc} across various time intervals and operational conditions.

Our analysis identified three clusters of ships, as shown in Figure 21. Figure 21a shows three ships moving at constant speed, while Figure 21b shows a ship with changing speed. In these cases, the reported and calculated speeds are similar. By contrast, the

ship depicted in Figure 21c reports a constant speed (12.9 kts) while the calculated speed varies.



(a) Ships with constant velocity *(b) Ship with changing velocity* *(c) Ship with anomalous reporting*

Figure 21: Ships' reported and calculated speeds

Figure 22 shows the reported positions of the ship with varying calculated speed (depicted in Figure 21c). The figure reveals two anomalies. On the left-hand side, the positions are clearly off the ship's course, possibly due to incorrect GPS position reception. On the right-hand side, the image suggests that the position was transmitted irregularly. In reality, the coordinates were reported every 20 seconds, but in a few cases, incorrect coordinates were advertised.

The anomaly detection method is based on comparing the reported and calculated speeds. When an incorrect position is transmitted, the discrepancy between the two speeds becomes significant.

The Absolute Speed Ratio (ASR) is calculated based on the ratio of V_{rep} and V_{calc} (see Equation 2).

$$ASR(n) = \begin{cases} \frac{V_{rep}(n)}{V_{calc}(n)}, & \text{if } V_{rep}(n) \geq V_{calc}(n) \\ \frac{V_{calc}(n)}{V_{rep}(n)}, & \text{if } V_{calc}(n) \geq V_{rep}(n) \end{cases} \tag{2}$$

Figure 22: Anomalously reported ship positions

Anomalous behaviour is then defined based on the ASR (see Equation 3).

$$Category(n) = \begin{cases} True, & \text{if } ASR \geq 1,5 \\ False & \text{otherwise} \end{cases} \tag{3}$$

As shown in Figure 22, this method can detect position reporting anomalies. Although simple and easy to implement, the method is applicable only if the ship's trajectory is not straight, as illustrated in Figure 23.

Figure 23: Anomalously reported ship positions

7.3.1 Contribution

The presented results show that anomalies can be identified by comparing the reported speed with the speed calculated from positional data. Theoretically, these values should be similar, but our findings revealed discrepancies between them.

Most likely, the detected anomalies were caused by irregular position transmissions due to a faulty AIS transmitter. However, similar effects can also arise from the dynamic slot reservation mechanism of the AIS.

7.4 Randomised GPS Spoofing Detection

Ships regularly report their speed and position via AIS. As discussed in the previous section, these data can be used to detect anomalies in ship behaviour. GNSSs, such as GPS, Galileo, GLONASS and BeiDou, typically provide the position data used for ship navigation.

These systems are often jammed during military operations, as jamming is a highly effective countermeasure against drones, which are increasingly used in modern warfare. Jamming can also occur for malicious purposes [167, 10].

GNSS systems are also vulnerable to spoofing [10]. Such operations can severely impact flight safety, and since these systems are also used in maritime transportation, they pose a safety risk at sea as well. As illustrated in Figure 24, falsified GPS positions are not always identical. Sometimes they remain fixed in one location, while in other cases they shift in circles, follow intricate patterns or imitate realistic movement paths.

7.4.1 Background

According to the preliminary hypothesis, the circular spoofing pattern is temporally randomised. This means that over time, the falsified GPS positions do not follow a fixed

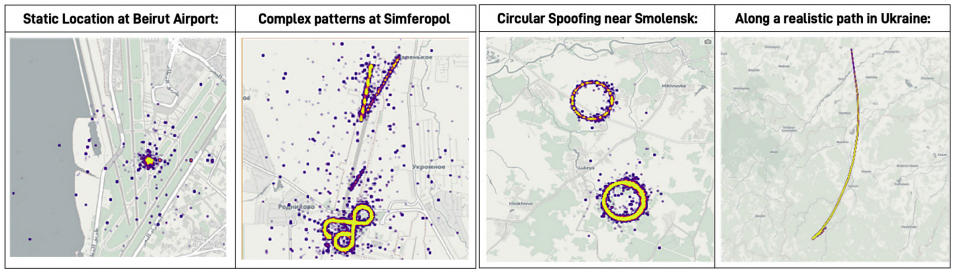


Figure 24: Various GPS spoofing patterns [10]

or linear path but instead jump between random points or trace a circular or semicircular trajectory. Such behaviour becomes more apparent when the data is observed over a long time span, allowing recurring spatial patterns to emerge despite the randomness of individual movements. This characteristic makes long-term trajectory analysis particularly effective in detecting spoofing attempts. Identifying such attacks can improve maritime safety.

7.4.2 Method

The small location errors referred to above can be simulated by adding noise to represent randomised GPS position data.

According to the hypothesis, this type of spoofing can be detected by analysing the maximum and average speeds of the ship, as the randomisation of coordinates adds extra distance between points. Since the time between the samples did not increase, the calculated speed increased.

To test the concept, the maximum and average speeds of the ships were first calculated based on their reported position. Then, the positions were randomised by no more than 100 metres, and the same values were recalculated.

7.4.3 Results

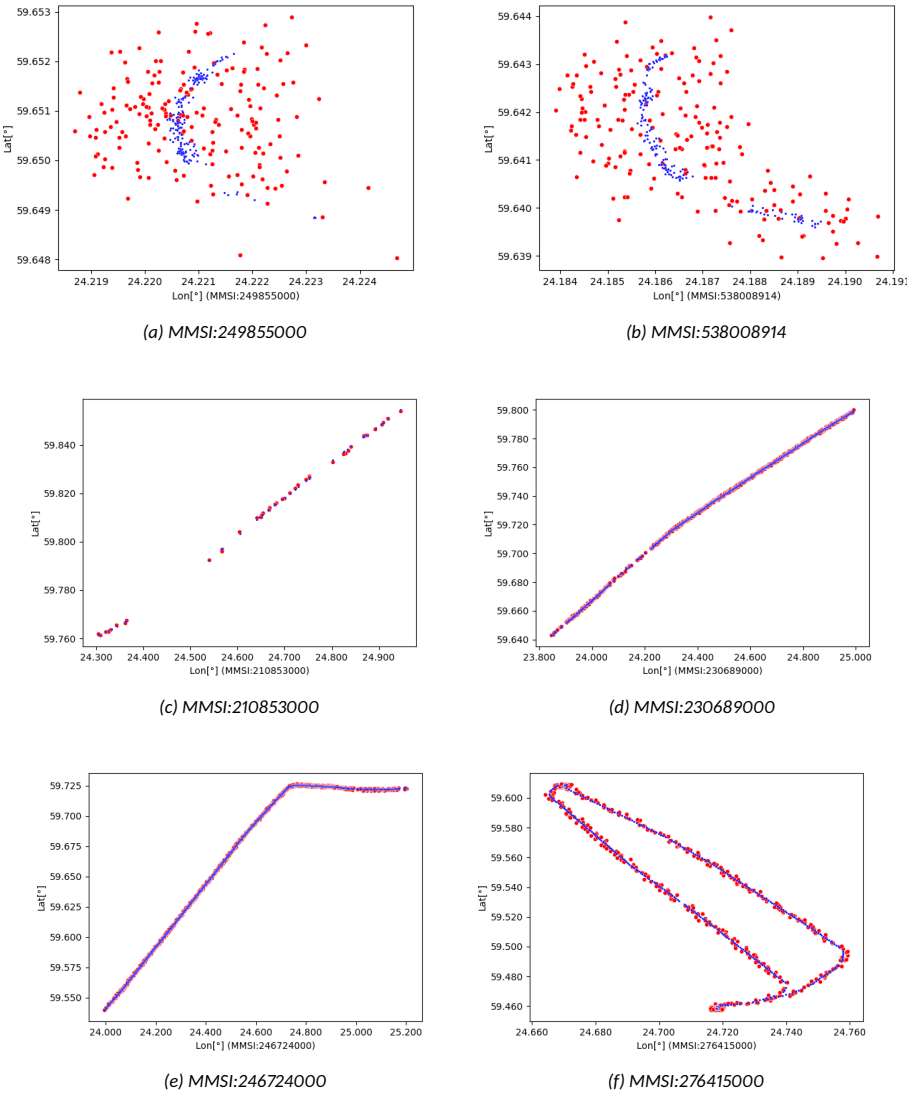
The AIS dataset described in Section 5.2 was used for this experiment.

The method was tested on both anchored ships, which transmit their positions via Type 3 AIS messages, and ships underway, which use Type 1 AIS messages.

Figures 25a and 25b illustrate examples of the positions of ships at anchor, while Figures 25c-25f show the trajectories of selected ships. The blue dots represent the transmitted positions, and the red dots represent the randomised positions.

As shown, the positions of ships at anchor followed a structured pattern: the vessel exhibited semicircular motion around the anchoring point. This pattern is consistent with natural environmental influences, particularly wind and current, which often cause anchored ships to drift within a restricted area. In this case, the trajectory suggests that the direction of the wind changed over time, gradually shifting the ship's position while it remained anchored. However, the regularity and symmetry of the movement, especially the circular component, can also indicate artificial manipulation, supporting the hypothesis of spoofing through controlled positional changes that mimic natural motion.

For the experiment, ships with different trajectories were selected. Table 11 summarises the average and maximum speeds of the ships with and without randomised GPS positions.



(a) MMSI:249855000

(b) MMSI:538008914

(c) MMSI:210853000

(d) MMSI:230689000

(e) MMSI:246724000

(f) MMSI:276415000

Figure 25: Positions of ships at anchor

7.4.4 Conclusion

As shown in Table 11, minimal randomisation of position changed the average speed by 9%, and the maximum speed by 200–300%, regardless of whether the ship was at anchor or underway. This significant difference between the changes can be used for GPS spoofing detection. Maximum and average speeds should be calculated using rolling samples, and significant deviations in their values may indicate GPS spoofing.

Table 11: Speed of ships at anchor and underway

MMSI	Status	With GPS Spoofing		Without GPS Spoofing	
		Maximum speed (kts)	Average speed (kts)	Maximum speed (kts)	Average speed (kts)
538008914	At anchor	1,07	0.48	0.16	0.04
249855000	At anchor	1.30	0.59	0.19	0.04
636021850	At anchor	1.26	0.55	0.51	0.08
276415000	On voyage	30.39	10.38	10.39	1.24
246724000	On voyage	33.53	12.51	10.89	9.94
230689000	On voyage	29.07	12.51	10.33	9.29
210853000	On voyage	25.63	13.44	13.07	12.31

7.4.5 Contribution

The results highlighted that anomalies can be identified based on the analysis of the calculated speed. The introduced method can detect position anomalies caused by randomised GPS position spoofing. One of its main advantages is that it is easy to implement and does not require extensive computational resources.

7.5 Summary

Given the critical role of AIS in maritime navigation and collision avoidance, detecting anomalies in this data stream is essential to prevent both accidental errors and deliberate cyberattacks. Integrating these anomaly detection techniques into shipboard security mechanisms can enhance real-time threat detection and response.

This chapter introduced novel anomaly detection methods applied to AIS data. It explored how inductive logic programming and statistical methods can be applied effectively to AIS data for anomaly detection, identifying unusual patterns in vessel behaviour by learning from historical data and detecting deviations from expected trajectories and operational norms. The discussion also outlined a set of potential features that could improve the accuracy of anomaly detection, such as vessel speed, heading, reported position and contextual factors such as time of day or proximity to shore.

The section further examined the inherent challenges in detecting anomalies, particularly in anchoring positions and position reporting. Anchoring anomalies can be difficult to distinguish due to natural vessel drift and varying anchoring behaviours. The research underscored that GPS spoofing attacks, which manipulate the apparent location of a vessel, can mimic natural influences such as wind or current. As a result, anomaly detection systems that rely primarily on spatial or movement patterns must also account for environmental variables, especially weather conditions, to improve robustness and avoid false positives.

In addition, the reliability of reported positional data was critically assessed. The research pointed out that even when the reported and calculated speeds appear consistent, incorrect positions can still be transmitted, either unintentionally due to sensor errors or intentionally as part of deceptive behaviour. This discrepancy can severely undermine the credibility of detection methods that assume the accuracy of positional input. Consequently, integrating cross-validated data sources and contextual reasoning is essential to enhance the trustworthiness and effectiveness of anomaly detection systems in maritime surveillance.

The next chapter will explore how these methods can be effectively applied within shipboard intrusion detection systems. By incorporating inductive logic programming and statistical models into IDS frameworks, this research aims to improve the identification of abnormal patterns in maritime operations. This approach can provide an additional layer of security, complementing network-based detection strategies and strengthening the overall cybersecurity posture of modern ships.

8 Considerations for On-board Intrusion Detection Systems for Ships' Operational Technology Systems

8.1 Motivation and Novelty

The existing literature extensively discusses IDSs and IPSs, primarily in the context of IT infrastructure. However, their application in OT environments remains relatively rare. The installation of IPSs can have serious consequences in the event of false-positive actions, where legitimate communication is blocked.

HIDSs bring other problems into the picture. OT devices, such as PLCs, RTUs, DCUs and intelligent sensors, are rarely designed to accommodate such systems. They have limited resources, run special operating systems, and do not collect system logs or data about the usage of hardware resources.

On standard computers within OT systems, vendors often prohibit the installation of software other than controller or supervisor applications. These computers frequently run obsolete operating systems that do not support the latest HIDS solutions.

In contrast, NIDSs are designed to monitor traffic and related parameters. They look for anomalous behaviour of these parameters or identify malicious communication. NIDS products are considerably easier to deploy in vessel networks than HIDS solutions because they can be connected passively to the network without modifying the systems themselves, whereas HIDSs require installation on individual systems, altering their state. Therefore, this chapter focuses primarily on network-based IDS systems, though the considerations discussed are also relevant to host-based IDSs.

Despite the importance of cybersecurity in OT environments, only a limited number of publications explore the unique challenges, requirements and constraints associated with deploying IDS and IPS solutions in such settings. The integration of these security mechanisms into OT systems, including those used in marine vehicles, requires careful consideration of factors such as cost efficiency, operational reliability and usability. Given the resource-constrained nature of many OT systems, traditional IDSs designed for IT environments may not be directly applicable without modification or optimisation.

This section provides a high-level overview of key considerations for the integration of NIDSs into marine vehicles, including the technical and operational challenges that must be addressed. As seen in Section 3.3, the literature discusses IDSs and anomaly detection methods for ship systems such as AIS and RADAR but rarely addresses considerations related to implementation and deployment.

The results presented here are novel in their contextual focus on OT networks on board ships, offering a detailed analysis of implementation challenges and adaptations for constrained, legacy-driven and safety-critical maritime environments. This section also provides a comparative evaluation of open-source IDS tools, bridging the gap between theoretical detection capabilities and practical deployment feasibility in real-world shipboard scenarios.

Some standards provide useful frameworks, such as IEC 61162-460:2024 [69]—which defines requirements and test methods for equipment to be used in compliant networks, as well as requirements for the network itself and for interconnection from the network to other networks—and IEC-62443—which outlines procedures for implementing electronically secure industrial automation and control systems. However, neither these standards nor many (academic) publications discuss the cybersecurity monitoring of ships in depth or provide detailed guidance on deployment.

The findings presented in this section aim to provide valuable insights into the practical deployment of NIDS technology in the maritime domain, contributing to

improved cybersecurity for modern marine transportation systems.

8.2 System Requirements and Objectives

8.2.1 Threat Modelling

To establish an effective IDS for a marine vehicle, it is essential to first define the security objectives. This task can be supported by several methods for modelling and risk assessment, as outlined below.

The Maritime Cyber Risk Assessment (MaCRA) threat model has been used to analyse possible attacks against manned ships [171]. Based on MaCRA, Jones et al. [103] introduced a Multi-Criteria Decision-Making Framework (MCDM) to assess cybersecurity risks in autonomous shipping. This framework offers a multifaceted approach to maintaining cybersecurity amidst the increasing complexity of advanced cyber-physical interactions in autonomous operations.

To cover a wide range of cyber threats to autonomous ships, the STRIDE threat modelling approach was developed to identify potential cyber threats and analyse them accordingly [161, 131, 143].

Kavallieratos et al. [80] leveraged the STRIDE and DREAD methodologies to qualitatively and quantitatively assess the cyber risk of cyber-physical systems on board and proposed critical cybersecurity controls to mitigate them.

Bolbot et al. [58] proposed the Cyber Risk Assessment for Marine Systems (CYRA-MS) method, which offers a quantitative risk assessment explicitly tailored for cybersecurity concerns in marine systems. This method enhances the resilience of ships against cyberattacks by helping operators identify cyber risks and systematically take effective countermeasures.

The MITRE ATT&CK framework, adapted for the maritime sector, focuses on modelling adversarial behaviour in navigation systems, as explored in [141]. This has been further integrated with failure mode, effects and criticality analysis (FMECA) for autonomous passenger ships (APS) [42].

8.2.2 Identified Obstacles

Visky et al. [187] systematically identified key challenges to cybersecurity improvements on ships:

- Limited on-board IT Staff: Due to the limited crew sizes, there are typically only a few IT experts on board, usually dedicated to temporary troubleshooting during voyages. These experts possess limited cybersecurity knowledge.

- Troubleshooting: Sailors typically resolve system failures by replacing faulty units with on-board spares. However, the limited availability of spares and the need for simple installation make it difficult to implement robust security measures. For example, unique device identifiers such as MAC addresses cannot be pre-registered in endpoint protection systems, as spare parts are often unknown until needed.

- Certification constraints: Due to certification requirements, ship control systems face strict limitations on updates. Navigation and control software developers must test their products in specific environments, which must also be present on board. These limitations hinder timely improvements needed to address evolving cyber threats.

- Legacy technologies: As of January 2023, more than 50,000 ships of this tonnage were over 15 years old [138]. These vessels use legacy technologies and outdated operating systems that are not prepared for cyber challenges.

8.2.3 Regulation Compliance

An IDS must comply with both national and international regulations. Maritime cybersecurity has gained urgency due to recent incidents, prompting the IMO to issue high-level cyber-risk management guidelines in 2017. Although these are non-binding, the Maritime Safety Committee later adopted a resolution requiring the integration of cyber risk into safety management systems by January 2021.

The ISPS Code of the IMO partially addresses cybersecurity risk assessment but lacks specific IDS requirements. Consequently, IDS implementations must also comply with relevant data protection laws, such as the EU's General Data Protection Regulation (GDPR) or California's Consumer Privacy Act (CCPA). These regulations mandate transparency, user rights regarding personal data, and, in some cases, user notification or consent before monitoring activities.

8.3 Performance Requirements

During IDS planning, it is essential to have a clear understanding of the infrastructure to be defended. This requires information about the network topology and the various systems in use.

8.3.1 Networks

Networks are the ships' communication backbone; they provide reliable communication between the subsystems. This research identified the following networks on a passenger ship [187]:

- Administrative network: Designed as a tree topology, this network is part of the company's virtual private network (VPN). It supports communication with the headquarters and administrative tasks such as reporting and map updates. It also offers monitored internet access for admin use. This network connects via Wi-Fi in port and over 4G/5G during voyages (when available).

- Navigation network: A (partially) isolated redundant ring network linking navigation devices (ECDIS, INSs, MFDs, DCUs and RADAR), it receives propulsion data from the propulsion control network via a one-way connection.

- Propulsion control network: A (partially) isolated redundant network that connects the bridge to the propulsion automation system. In emergencies, propulsion can be manually controlled from the engine room. It sends data to the Navigational Network via a one-way connection.

- Cargo handling network: An isolated wired and wireless network for cargo operations and administration. Cargo data from the coast is imported into the offline management system.

- Public Wi-Fi network: An isolated wireless network for passenger Internet access, with devices managing user separation.

- Independent support company network: An isolated wired and wireless network for ferry restaurants' operations, support orders, payments and related services.

To maximise cybersecurity, ship networks should remain physically isolated. While these networks can vary significantly across vessels, maintaining their separation is crucial to minimising the risk of lateral movement by potential attackers. The diverse and often fragmented nature of these systems further justifies the implementation of dedicated network detection solutions.

Deploying affordable open-source IDS solutions for each network segment provides a practical and scalable approach. By ensuring physical isolation and monitoring each segment independently, ships can better defend themselves against threats while accommodating their unique infrastructure constraints.

8.3.2 Systems

Section 2.1 introduced ship OT systems. Visky et al. [187] identified the administrative system, public Wi-Fi and independent company system as IT systems, while the navigation, propulsion, control (heating, ventilation and air conditioning (HVAC), security and safety, etc.), cargo handling and power generation systems were classified as OT systems. These systems typically have their own control systems and should remain isolated.

A wide range of IDS solutions is available on the market to secure IT systems. However, OT systems require a different approach that maintains a careful balance between security, safety and operational continuity. Key considerations include:

- Passive monitoring: IDS should passively monitor traffic to avoid interfering with the operation of critical systems.
- Protocol awareness: IDS must be able to process maritime-specific protocols such as IEC61162-450, BR24, ASTERIX or proprietary protocols, enabling it to detect anomalous messages or command sequences.
- Edge deployment: Due to limited and sometimes intermittent connectivity to shore-based systems, IDS should operate autonomously on board with local data processing capabilities.
- Separated approach: Different networks should remain separated to prevent lateral movement between the networks, even if a network device is compromised.

Typical data sources for IDS in maritime environments include network traffic captures, system logs and control command sequences. As introduced in Section 3.3, an on-board NIDS can trigger alerts in the event of network-related anomalies. However, such solutions do not address anomalies in operational values, such as sensor values and their behaviour. For example, a spoofed GPS signal could alter the perceived location of a ship, leading to navigational errors.

To add this capability, operational values should first be extracted from network traffic, which requires deep knowledge of the communication protocols, as discussed in Section 6, and specialist anomaly detection methods, as introduced in Section 7.

Challenges in deploying IDS on board include integration with existing infrastructure, dealing with legacy systems not designed for cybersecurity, limited on-board computing resources, and a lack of standardisation between ships and equipment. Regulatory frameworks such as the IMO guidelines and IEC62443 [16] standards are beginning to address these gaps, but implementation remains inconsistent.

8.3.3 Performance

The required processing speed is fundamentally determined by the rate of communication. To assess this, a packet capture was conducted within a ship's navigational network, which comprised a RADAR system and a data collection unit. Figure 26 illustrates the number of packets per second (PPS) over time. Analysis of the captured data revealed an average PPS of 1066.9, with an average packet size of 1035 bytes. This corresponds to an average network throughput of approximately 8831 kbit/s. Of this bandwidth, the RADAR system accounted for 8567 kbit/s, while only 263 kbit/s was attributed to the transmission of sensor data.

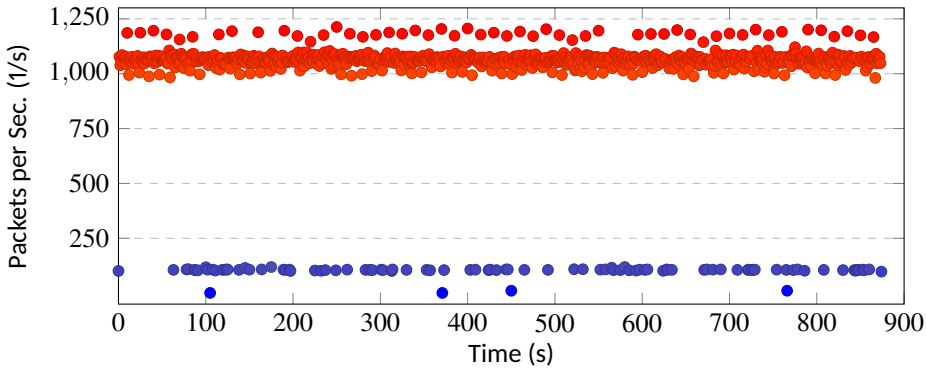


Figure 26: Speed of communication in the navigation network

A comparative performance analysis of three open-source IDSs (Zeek, Suricata and SNORT) was conducted under constrained resource conditions. The evaluated performance metrics included CPU and memory usage, kernel versus user mode time, packet drop rates, and storage requirements. The datasets used in these experiments were sourced from cyber exercises organised by the NATO Cooperative Cyber Defence Centre of Excellence and iTrust [18].

Suricata performed best in terms of packet processing without drops. Zeek was the most efficient in CPU usage but consumed significantly more memory and dropped packets under stress. Snort offered a balanced performance profile [184].

Based on these results, any of the evaluated solutions are capable of processing on-board OT communication and effectively detecting anomalies. However, due to the wide variability in network workloads among different vessel types and configurations, it is crucial to conduct similar performance evaluations under realistic operating conditions before adopting an IDS platform. This ensures that the chosen solution can handle the expected workload and traffic characteristics of the target environment without introducing latency or missing critical threats.

At the same time, these solutions must be extended with anomaly detection features in the application layer. These features can be based on the detection methods introduced in Section 7.

8.4 Architecture

8.4.1 System Architecture

Ships typically host multiple networks with varying levels of mission criticality—for example, passenger Wi-Fi is less critical than navigation or propulsion networks. This distinction must be considered when designing the network architecture.

To maintain isolation between networks, several approaches can be used:

One method is to use a single high-performance centralised IDS to monitor all traffic across networks. Although simpler in some respects, this approach compromises network isolation and may overlook network-specific anomalies.

Raimondi et al. [150] introduced another approach, in which Suricata provided intrusion detection functionality, captured NMEA traffic from the INS network and forwarded the parsed data to the shipboard security information and event management (SIEM) system. Additionally, it performed real-time detection of anomalous patterns, such as non-existent or unexpected values and conformity issues.

Splunk [76] was used for shipboard SIEM that collected and correlated data from various sources, including IDS alerts, NMEA data and logs from the workstation and ECDIS software. In addition, the shipboard SIEM can send data to a shoreside centre, selecting and aggregating it to overcome bandwidth and connectivity issues associated with satellite connections.

Although this solution allows for custom detection and lower false positive rates, it involves moderate deployment complexity and high maintenance, as each IDS requires separate updates. It also supports handling specific topologies, such as link-based layouts [186, 187].

8.4.2 NIDS Sensor Placement

The complex network structure makes the installation of IDS challenging.

Networks should be kept separated, while all alerts should be collected and displayed at a single point dedicated to the entire ship. OT networks use various protocols but differ in topology; both ring and tree topologies can be found on ships. However, the low bandwidth of the networks allows for IDS deployment using either light-weight, isolated setups or a centralised system with passive taps.

Data collection in tree topologies remains a key challenge, as segments hide their traffic. This highlights the need for a separate monitoring network to detect anomalies efficiently.

On many ferries, the navigation network uses Moxa Turbo Ring technology, which ensures fast, redundant communication with quick recovery. A dedicated switch prevents loops and can mirror traffic for IDS integration.

8.4.3 Detection Methods

In IT environments, signature-based IDSs enable misuse detection and identify intrusions by matching known attack signatures (rules) against network traffic. They rely on rule sets that define malicious traffic signatures and trigger responses when matched. This method is efficient, especially with well-known threats, and is easy to configure and understand.

Such systems can analyse network traffic and incorporate new patterns for future detection. Although fast and accurate for known attacks, they require frequent rule updates and may fail to detect novel threats. Redundant rules can also affect performance.

Unlike misuse detection, which relies on signatures that describe known cyberattacks and intrusions, anomaly detection-based IDSs learn the normal behaviour profile of the system, reporting deviations from this profile as anomalies (potential intrusions). Any significant deviation is flagged as an anomaly, allowing for the detection of unknown threats, including zero-day attacks, protocol misuse and DoS attempts.

Some anomaly detection systems can adapt to changing environments over time, making them effective against evolving threats. As they do not rely on predefined rules,

they are particularly suitable for identifying novel attacks. However, building accurate behaviour profiles is complex, and distinguishing normal from abnormal activity can be challenging, potentially leading to false alarms.

In ship operational technologies, anomalies in system values may indicate cyberattacks. Addressing such cases requires specialist detection methods, including:

- Comparing sensor values from different sources—for example, vessel speed measured by speed sensors should be similar to GPS-derived speed data.
- Using anomaly detection methods, as discussed in Section 3.3.2.
- Identifying anomalies by comparing changes in sensor values against known patterns.

8.4.4 Data Collection, Storage and Analysis

IDSs generate large volumes of diverse data, requiring scalable storage and real-time processing. Effective management includes centralised data collection from multiple sensors using standardised protocols and formats (e.g. collecting messages in JSON format over the syslog protocol) to simplify analysis.

Given the limited communication capacity of ships, on-board storage must be efficient and scalable, using solutions suited to constrained environments. Log data should be normalised, indexed and enriched with context—such as geolocation or threat intelligence—to improve analysis and detection. Integration with SIEM systems enables real-time monitoring, correlation and threat response.

Data retention policies should balance compliance requirements, business needs and storage efficiency, including archiving older logs.

8.4.5 Alerting and Response

When an IDS detects suspicious activity—such as abnormal logins or known attack patterns—it generates alerts with relevant metadata, such as IP addresses and timestamps. Alerts should be correlated to detect coordinated attacks and prioritised by severity.

Predefined response protocols are critical for timely action. Initial analysis determines the validity of the alert, with further investigation carried out manually or through automated tools. Immediate responses may include isolating systems or blocking malicious traffic, while long-term mitigation involves patching, reconfiguring defences and updating policies.

Recovery focuses on restoring systems and preventing recurrence through improved monitoring, updated rules or staff training. An effective alert and response process ensures fast, coordinated action to protect vessel systems.

All these processes should be handled semi-automatically on board the vessels, with the assistance of a remote operator. Given the limited communication capabilities of ships, most data preparation should be performed on board.

All these tasks should be implemented in a light-weight on-board SIEM system, capable of operating efficiently with minimal resource consumption while providing real-time threat detection, log analysis, and security event correlation tailored for embedded or resource-constrained environments.

8.5 Summary

This chapter, and the publications it draws upon, emphasise the critical role of threat modelling in maritime cybersecurity. Identifying security risks and potential attack surfaces is essential for building effective defences.

The chapter examines the on-board networks of ships. While these networks can vary between vessels, it is vital to keep them segmented to reduce the risk of lateral movement by attackers. This need for separation, combined with the heterogeneous nature of shipboard networks, supports the deployment of independent network detection systems. These should consist of affordable, open-source intrusion detection systems (IDS) tailored to each network segment.

Key challenges to improving cybersecurity at sea are also explored, including the prevalence of legacy technologies, the shortage of IT and cybersecurity personnel on board, certification restrictions, and the practical limitations of troubleshooting during voyages.

As a solution, the chapter proposes the use of open-source NIDS for OT networks. These systems offer a passive, non-intrusive, certifiable and cost-effective approach suitable for maritime environments. Passive deployment through network taps makes them feasible for retrofitting onto existing ship infrastructure. A detailed benchmark of Snort, Suricata and Zeek running on low-resource hardware (Raspberry Pi 4) demonstrates their practical usability for this purpose.

The chapter provides recommendations for deploying IDS within vessels' OT networks and outlines the essential considerations necessary to ensure effective and secure integration. Due to the unique characteristics and constraints of the maritime environment—such as limited bandwidth, intermittent connectivity, legacy systems and safety-critical operations—it is important that IDS deployments are tailored specifically to vessel network architectures. A crucial preparatory step is the comprehensive evaluation and testing of IDS products to determine their suitability for the specific conditions and requirements of the target vessel environment. This includes evaluating detection accuracy, resource consumption, interoperability with existing systems and resilience against evasion techniques. To support practitioners in this process, the chapter includes case research papers that illustrate a representative testing methodology. These examples can serve as a practical reference for maritime cybersecurity professionals seeking to implement IDS solutions effectively and responsibly in operational vessel networks.

The research highlighted that separate light-weight IDSs should be deployed in the different networks to analyse network traffic and extract operational values. The detected anomalies and metric data should be sent to a light-weight on-board SIEM system to be aggregated and correlated. This solution can enhance a ship's cybersecurity without harming the critical OT systems and can also allow on-shore experts to be involved at low communication costs.

9 Conclusion and Further Work

9.1 Summary and Conclusions

This thesis addresses the cybersecurity challenges of maritime operational technologies. After a brief state-of-the-art overview of the maritime cyber landscape, it introduces five research objectives and discusses how each of these was achieved.

[RO1] Implementation of cybersecurity research and education environments for the marine sector

The first objective focuses on developing environments to support maritime cyber research and education. Section 4 introduces three such environments.

First, the Multi-Purpose Cyber Environment provides a realistic educational setting for seafarers in which they can experience the effects of cyberattacks on ship control systems. It also generates realistic sensor data, which is transferred via the proprietary NaviNet protocol.

Second, the Light-Weight Cyber Research Environment, designed with moderate cost in mind, enables research on the widely adopted IEC 61162-450 protocol. To demonstrate its practical usability, attack scripts were developed and successfully tested on the Transas Navi-Sailor 5000 ECDIS software.

A common limitation of both of these environments is their scalability. Although the light-weight solution has modest hardware requirements, scaling it still requires a separate set of hardware for each instance.

Third, the virtualisation-intensive Hybrid Cyber Research Environment addresses this challenge by using a single physical hardware instance to supply real-world data while virtualising the remaining components. This laboratory setup, built on minimal hardware, supports both research and educational applications. Its standout feature is scalability: thanks to its virtualised nature, multiple identical instances can be easily created, making it ideal for scalable cybersecurity education.

[RO2] Collection, analysis and publication of maritime datasets

As part of this thesis, two publicly available datasets were developed, as introduced in Section 5. MarCyb is a simulated dataset that reflects realistic maritime communication scenarios and includes both benign and malicious network traffic. The malicious components of the dataset comprise network-based attacks targeting the data link layer (Layer 2), the network layer (Layer 3) and specifically maritime navigation devices. The MarCyb dataset serves as a valuable resource for analysing and developing mitigation strategies against cyber-mass threats and supports reproducible experimentation in academic and applied research contexts.

In addition to the MarCyb dataset, the thesis also presents a comprehensive AIS dataset, comprising over 71 million AIS messages collected over a six-month period in Tallinn Bay. Data acquisition was carried out using a self-developed collection system that continuously recorded maritime communication signals in a real-world operational environment. This dataset provides a rich source of longitudinal vessel movement data, essential for analysing communication behaviours in maritime contexts.

Both datasets are publicly available, significantly supporting maritime cybersecurity research.

[RO3] Maritime-specific protocol analysis and vulnerability exploitation

Section 6 examines vulnerabilities in maritime communication protocols and demonstrates how these weaknesses can be exploited. The comparison of automated reverse engineering techniques with traditional manual methods is emphasised, particularly regarding speed, accuracy and scalability.

Through a series of controlled experiments, various cyberattacks were successfully executed against an ECDIS, demonstrating real-world implications. These results underscore the pressing need for improved cybersecurity measures within maritime systems and validate the effectiveness of different environments as a platform for vulnerability analysis and research on exploitation.

[RO4] Data analysis and anomaly identification in the AIS dataset

Section 7 presents various anomaly detection methods applicable to shipboard OT environments, particularly focusing on AIS data. Two approaches are introduced. The first, based on inductive logic programming, is a novel application in this context; it has not previously been used to detect anomalies in AIS data. This method offers the advantage of explainable anomaly detection, providing a clear and interpretable solution.

The thesis identifies and classifies various anomalies within the AIS dataset, with a particular focus on those arising from propagation-related phenomena. These anomalies include position reports from unexpected locations that may result from multipath propagation, atmospheric ducting, or signal obstructions caused by environmental or infrastructural factors. Understanding such irregularities is critical not only to improve the fidelity of AIS-based maritime monitoring systems but also to improve anomaly detection algorithms used in maritime cybersecurity and safety applications.

In addition to general behavioural anomalies, the study specifically addresses inconsistencies in the speed and position reported by the vessels. The proposed method compares the reported speed with the speed calculated from successive position updates to detect discrepancies. This technique was successful in identifying falsified or erroneous position reports in the AIS dataset, highlighting its potential as a robust tool for improving the reliability of maritime surveillance and threat detection.

[RO5] Examination and introduction of key considerations for integrating IDSs into marine vehicles

Section 8 examines open-source IDSs, focusing on deployment considerations within shipboard networks while also addressing the associated challenges. It highlights key obstacles to enhancing cybersecurity in maritime OT environments. The section emphasises the importance of threat modelling during system design, the complexity of ship networks and the need to maintain network isolation.

Through an analysis of shipboard network structures and the performance of various open-source IDSs, the section paves the way for their integration on ships, emphasising the need for strategic placement. In addition, it explores architectural considerations, including detection methods, data collection, storage and analysis. Finally, it discusses essential components of alerting mechanisms and incident response strategies.

9.2 Future Work

The author acknowledges that while this thesis contributes to the existing body of knowledge on maritime cybersecurity, it represents only a step towards a broader understanding that warrants continued research and development.

While the thesis offers a comprehensive exploration of maritime cybersecurity, it is subject to several notable limitations. Due to the sensitive nature of maritime operations and the proprietary design of on-board systems, access to actual shipboard data remains limited, restricting the depth and breadth of protocol vulnerability assessments.

Furthermore, the datasets collected may not fully represent the diversity of ship types and operational contexts encountered in real-world maritime environments. Future research could address these gaps by seeking collaborations with maritime stakeholders to gain access to richer and more representative datasets, including live

data streams from on-board systems. Such access would enable the development and validation of more sophisticated anomaly detection algorithms tailored to specific classes and operational profiles of vessels.

Additionally, expanding the scope of protocol analysis to include more proprietary or less documented protocols would strengthen the comprehensiveness of vulnerability assessments. However, such efforts may be constrained by practical and ethical considerations, including data privacy concerns, legal restrictions on data sharing and the risk of exposing sensitive operational information that could be exploited by malicious actors.

Another promising avenue for future work involves the design and deployment of on-board IDSs tailored to OT systems aboard ships. These systems must be light-weight, adaptive and capable of operating under the constrained computational resources typical of maritime environments. Integrating such IDS solutions with existing maritime infrastructure also presents challenges in terms of interoperability, backwards compatibility and the need to avoid interference with critical safety functions. Moreover, the dynamic and distributed nature of maritime networks may necessitate the development of decentralised detection architectures, which in turn raise new concerns related to coordination, latency and fault tolerance.

The integration of artificial intelligence and machine learning technologies—particularly state-of-the-art large language models (LLMs)—holds significant potential to enhance the cyber resilience of the maritime sector.

Building on the findings of this thesis, the author has initiated a new line of research focused on supporting maritime security operation centres (MSOCs) through the application of anomaly detection techniques in system log analysis.

List of Figures

List of Tables

References

[1] Above us only stars - C4ADS. https://c4ads.org/reports/above-us-only-stars/. (Accessed on 09/20/24).

[2] AIS for Safety and Tracking: A Brief History - Global Fishing Watch. https://globalfishingwatch.org/article/ais-brief-history/. (Accessed on 09/20/24).

[3] AV200 GPA AIS VHF Base Station Antenna - AMI Marine. https://amimarine.com/product/av200/. (Accessed on 19/03/25).

[4] China hackers steal data from US Navy contractor - reports. http://en.newsroom24.net/china-hackers-steal-data-from-us-navy-contractor-reports/. (Accessed on 02/05/23).

[5] Comar Systems Receiver: R500Ni - MarineTraffic AIS Shop. https://shop.marinetraffic.com/comar-systems-r500ni.html. (Accessed on 15/01/22).

[6] Coronavirus: How the pandemic has changed the world economy. https://www.bbc.com/news/business-51706225. (Accessed on 03/05/23).

[7] Ever Given: Ship that blocked Suez Canal sets sail after deal signed. https://www.bbc.com/news/world-middle-east-57746424. (Accessed on 03/05/23).

[8] Free AIS vessel tracking | AIS data exchange | JSON/XML ship positions. https://www.aishub.net/. (Accessed on 01/14/24).

[9] The global leader in innovative technologies and lifecycle solutions for the marine and energy markets | Wärtsilä. https://www.wartsila.com/. (Accessed on 03/03/25).

[10] GPS spoofing final report. https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf. (Accessed on 07/04/25).

[11] Home - Suricata. https://suricata.io/. (Accessed on 04/21/25).

[12] Home | TCPDUMP & LIBPCAP. https://www.tcpdump.org/. (Accessed on 23/03/25).

[13] hping3 | kali linux tools. https://www.kali.org/tools/hping3/. (Accessed on 23/03/25).

[14] IALA guideline - an overview of AIS. https://www.navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf. (Accessed on 09/20/24).

[15] Index of /kali-images/kali-2023.2/. https://old.kali.org/kali-images/kali-2023.2/. (Accessed on 15/03/25).

[16] ISA/IEC 62443 Series of Standards - ISA. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. (Accessed on 17/05/25).

[17] ISO/IEC 3309:1993 - information technology — telecommunications and information exchange between systems — high-level data link control (HDLC) procedures — frame structure. https://www.iso.org/standard/8561.html. (Accessed on 03/19/24).

[18] iTrust Labs Dataset Info - iTrust. https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/. (Accessed on 10/09/25).

[19] Marine AIS data - maritime AIS vessel tracking solutions. https://spire.com/maritime/. (Accessed on 03/18/24).

[20] Marinecadastre.gov. https://www.marinecadastre.gov/. (Accessed on 03/18/24).

[21] Marinetraffic: Global ship tracking intelligence | AIS marine traffic. https://www.marinetraffic.com. (Accessed on 01/14/24).

[22] Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. https://www.metasploit.com/. (Accessed on 23/03/25).

[23] Navi-Sailor 4000 ECDIS - Wärtsilä. https://www.wartsila.com/ancs/integrated-vessel-control-systems/navigation/navi-sailor-ecdis. (Accessed on 06/03/25).

[24] OpenCPN official site. https://opencpn.org/. (Accessed on 05/29/2024).

[25] pfSense® - world's most trusted open source firewall. https://www.pfsense.org/. (Accessed on 15/03/25).

[26] RS-422 - wikipedia. https://en.wikipedia.org/wiki/RS-422. (Accessed on 05/31/2024).

[27] Satellite – Automatic Identification System (SAT-AIS) Overview | ESA CSC. https://connectivity.esa.int/satellite-\%E2\%80\%93-automatic-identification-system-satais-overview. (Accessed on 02/02/24).

[28] Ships fooled in GPS spoofing attack suggest Russian cyberweapon. https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/. (Accessed on 02/05/23).

[29] t50 | kali linux tools. [Online]. Available from: https://www.kali.org/tools/t50/. (Accessed on 23/03/25).

[30] Tcpreplay - PCAP editing and replaying utilities. [Online]. Available from: https://tcpreplay.appneta.com/. (Accessed on 23/03/25).

[31] tcprewrite(1): Rewrite packets in PCAP file - linux man page. https://linux.die.net/man/1/tcprewrite. (Accessed on 23/03/25).

[32] Wärtsilä navigation simulator NTPRO 5000. https://www.wartsila.com/marine/products/simulation-and-training/navigational-simulators/navigation-simulator-ntpro-5000. (Accessed on 06/03/25).

[33] The zeek network security monitor. https://zeek.org/. (Accessed on 04/21/2024).

[34] Iran's top cargo shipping line says sanctions damage mounting. https://www.arabnews.com/iran\%E2\%80\%99s-top-cargo-shipping-line-says-sanctions-damage-mounting, Oct. 2012. (Accessed on 02/05/23).

[35] AIS Dispatcher: free AIS data sharing tool AISHub. https://www.aishub.net/ais-dispatcher, 07 2017. (Accessed on 14/01/24).

[36] Search and rescue transponder. https://en.wikipedia.org/wiki/Search_and_rescue_transponder, Aug. 2022. (Accessed on 03/05/23).

[37] MariOT - iTrust. https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs-mariot/, March 2025. (Accessed on 09/09/25).

[38] A. Abraham, C. Grosan, and Y. Chen. Cyber security and the evolution in intrusion detection systems. *Journal of Engineering and Technology, ISSN*, pages 0973–2632, 2005.

[39] M. Afenyo and L. D. Caesar. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean &; Coastal Management*, 236:106493, Apr. 2023.

[40] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos. Cybersecurity challenges in the maritime sector. *Network*, 2(1):123–138, 2022.

[41] A. Amro and V. Gkioulos. From click to sink: Utilizing AIS for command and control in maritime cyber attacks. In *European Symposium on Research in Computer Security*, 2022.

[42] A. Amro, V. Gkioulos, and S. Katsikas. Assessing cyber risk in cyber-physical systems using the ATT&CK framework. *ACM Transactions on Privacy and Security*, 26(2), 2023.

[43] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas. Navigation Data Anomaly Analysis and Detection. *Information*, 13(3):104, Feb. 2022.

[44] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., New York, NY, 2001.

[45] A. Androjna, I. Pavić, L. Gucma, P. Vidmar, and M. Perkovič. AIS data manipulation in the illicit global oil trade. *Journal of Marine Science and Engineering*, 12(1):6, Dec. 2023.

[46] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković. AIS data vulnerability indicated by a spoofing case-study. *Applied Sciences*, 11(11):5015, May 2021.

[47] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics*, 9(7):1177, July 2020.

[48] A. S. Ashoor and S. Gore. Importance of intrusion detection system (ids). *International Journal of Scientific and Engineering Research*, 2(1):1–4, 2011.

[49] N. M. E. Association. Nmea 0183. Standard, National Marine Electronics Association, 1987.

[50] G. L. Babineau, R. A. Jones, and B. Horowitz. A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 99–104, 2012.

[51] M. Balduzzi, A. Pasta, and K. Wilhoit. A security evaluation of AIS automated identification system. In *Proceedings of the 30th Annual Computer Security Applications Conference*, ACSAC '14, page 436–445, New York, NY, USA, 2014. Association for Computing Machinery.

[52] F. Basels, K. Wolsing, E. Padilla, and J. Bauer. Demo: Maritime radar systems under attack. help is on the way! In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–4, 2024.

[53] T. Becmeur, X. Boudvin, D. Brosset, G. Héno, B. Costé, Y. Kermarrec, and P. M. Laso. Generating data sets as inputs of reference for cyber security issues and industrial control systems. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pages 453–454, 2017.

[54] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens. Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13(1), 2022.

[55] A. S. Benterki, G. Visky, J. Vain, and L. Tsiopoulos. Using Incremental Inductive Logic Programming for learning spoofing attacks on maritime automatic identification system data. In S. Bauk, editor, *Maritime Cybersecurity*, pages 123–141. Springer Nature Switzerland, Cham, 2025.

[56] BIMCO. *The Guidelines on Cyber Security Onboard Ships*. BIMCO, 2016.

[57] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39:100571, 2022.

[58] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos. A novel cyber-risk assessment method for ship systems. *Safety Science*, 131:104908, Nov. 2020.

[59] J. Borger, M. Farrer, and O. Holmes. Pentagon orders temporary halt to US navy operations after second collision. *The Guardian*, Aug. 2017. (Accessed on 02/05/23).

[60] C. Boudehenn, J.-C. Cexus, and A. Boudraa. A data extraction method for anomaly detection in naval systems. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–4, 2020.

[61] C. Boudehenn, O. Jacq, M. Lannuzel, J.-C. Cexus, and A. Boudraa. Navigation anomaly detection: An added value for maritime cyber situational awareness. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–4, 2021.

[62] F. Cabrera, N. Molina, M. Tichavska, and V. Araña. Automatic Identification System modular receiver for academic purposes. *Radio Science*, 51(7):1038–1047, July 2016.

[63] J. N. Campbell, A. W. Isenor, and M. D. Ferreira. Detection of invalid AIS messages using machine learning techniques. *Procedia Computer Science*, 205:229–238, 2022. 2022 International Conference on Military Communication and Information Systems (ICMCIS).

[64] Y. Chen. Satellite-based AIS and its comparison with LRIT. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 8(2):183–187, 2014.

[65] S. Cohen, E. Levy, A. Shaked, T. Cohen, Y. Elovici, and A. Shabtai. Radarnomaly: Protecting radar systems from data manipulation attacks. *Sensors*, 22(11), 2022.

[66] Z. Cohen. US Navy ship collides with South Korean fishing boat | CNN Politics. `https://www.cnn.com/2017/05/09/politics/fishing-vessel-hits-us-navy-ship-south-korea/index.html`, May 2017. (Accessed on 02/05/23).

[67] I. E. Commission. Iec 61162-1 maritime navigation and radiocommunication equipment and systems - digital interfaces - part 1: Single talker and multiple listeners. In *International Standard*, Geneva, Switzerland, 2002. International Electrotechnical Commission.

[68] I. E. Commission. Maritime navigation and radiocommunication equipment and systems – digital interfaces – part 450: Multiple talkers and multiple listeners – ethernet interconnection. In *International Standard - IEC61162-450*, Geneva, Switzerland, 2018. International Electrotechnical Commission.

[69] I. E. Commission. Maritime navigation and radiocommunication equipmentand systems – digital interfaces – part 460: Multiple talkers and multiple listeners – ethernet interconnection – safety and security. In *International Standard - IEC61162-460*, Geneva, Switzerland, 2020. International Electrotechnical Commission.

[70] M. Conti, D. Donadel, and F. Turrin. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, 23(4):2248–2294, 2021.

[71] A. Cropper, S. Dumančić, R. Evans, and S. H. Muggleton. Inductive Logic Programming at 30. *Machine Learning*, 111(1):147–172, 2022.

[72] A. Cropper and R. Morel. Learning programs by learning from failures. *Machine Learning*, 110(4):801–856, 2021.

[73] M. Darcangelo. What Is An EPIRB or Emergency Position Indicating Radio Beacon? `https://www.acrartex.com/news/what-is-an-epirb/`, Mar. 2023. (Accessed on 03/05/23).

[74] R. Daş, A. Karabade, and G. Tuna. Common network attack types and defense mechanisms. In *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, pages 2658–2661, 2015.

[75] Z. Drias, A. Serhrouchni, and O. Vogel. Taxonomy of attacks on industrial control protocols. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pages 1–6, Paris, France, 2015. IEEE.

[76] R. Ducloux. Splunk | the key to enterprise resilience. https://www.splunk.com/. (Accessed on 13/06/25).

[77] E. W. G. for Mutual Exchange and D. of AIS & Data. AIS data format - IEC standard 61162-450 for ethernet interconnections, 2019.

[78] C. Frøystad, K. Bernsmed, and P. H. Meland. Protecting future maritime communication. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, New York, NY, USA, 2017. Association for Computing Machinery.

[79] C. Gamage, R. Dinalankarac, J. Samarabandu, and et al. A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors. *WMU J Marit Affairs*, 22:447–477, 2023.

[80] K. Georgios and K. Sokratis. Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*, 8(10):768, Sept. 2020.

[81] A. A. Ghorbani, W. Lu, and M. Tavallaee. *Network Attacks*, pages 1–25. Springer US, Boston, MA, 2010.

[82] A. Grant, P. Williams, N. Ward, and S. Basker. GPS jamming and the impact on maritime navigation. *Journal of Navigation*, 62(2):173–187, 2009.

[83] A. Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. (Accessed on 02/05/23).

[84] L. Gupta, R. Jain, and G. Vaszkun. Survey of Important Issues in UAV Communication Networks. *IEEE Communications Surveys & Tutorials*, 18(2):1123–1152, 2016.

[85] E. Gyamfi, J. A. Ansere, M. Kamal, M. Tariq, and A. Jurcut. An adaptive network security system for iot-enabled maritime transportation. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2538–2547, 2023.

[86] M. Hadzagic and A.-L. Jousselme. Contextual anomalous destination detection for maritime surveillance. In *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.(July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy*, pages 62–65, 2016.

[87] G. Hanchrow. Vessel traffic services: Innovation, adaptation, and continued relevance. In *Advances in Marine Navigation and Safety of Sea Transportation*, pages 73–78. CRC Press, June 2019.

[88] R. L. Harrison, C. Granja, and C. Leroy. Introduction to Monte Carlo Simulation. In *AIP Conference Proceedings*. AIP, 2010.

[89] C. Hocquette and A. Cropper. Relational program synthesis with numerical reasoning. *Proceedings of the AAAI Conference on Artificial Intelligence*, 37(5):6425–6433, Jun. 2023.

[90] S.-B. Hong. A study on the effects of e-navigation on reducing vessel accidents, 2015.

[91] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40:307–324, 2014.

[92] E. Hotellier, N. Boukhobza, F. Sicard, J. Francq, and S. Mocanu. Behavior-based intrusion detection approach deployed on a naval testbed. *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, 2024.

[93] https://newatlas.com/author/brian-dodson. University of Texas team takes control of a yacht by spoofing its GPS. `https://newatlas.com/gps-spoofing-yacht-control/28644/`, Aug. 2013. (Accessed on 02/05/23).

[94] C. M. Hurd and M. V. McCarty. A Survey of Security Tools for the Industrial Control System Environment, June 2017.

[95] IMO. *International Convention for the Safety of Life at Sea (SOLAS)*. International Maritime Organization, IMO, 1975.

[96] IMO. Resolution Resolution A.917(22) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS), 2001.

[97] International Maritime Organization. Resolution msc.428(98) - maritime cyber risk management in safety management systems. `https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf`, 7 2017.

[98] C. Iphar, A. Napoli, and C. Ray. An expert-based method for the risk assessment of anomalous maritime transportation data. *Applied Ocean Research*, 104:102337, 2020.

[99] C. Iphar, C. Ray, and A. Napoli. Data integrity assessment for maritime anomaly detection. *Expert Systems with Applications*, 147:113219, 2020.

[100] ITU-R Radiocommunication Sector of ITU. *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*, 2014. Recommendation ITU-R M.1371-5.

[101] I. Jaen. Inmarsat's role in the GMDSS. In *IEE Colloquium on Satellite Distress and Safety Systems*, pages 4/1–4/5, 1993.

[102] K. Jindal, S. Dalal, and K. K. Sharma. Analyzing spoofing attacks in wireless networks. In *2014 Fourth International Conference on Advanced Computing & Communication Technologies*, pages 398–402, Los Alamitos, CA, USA, 2014. IEEE Computer Society.

[103] K. Jones and K. Tam. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. *WMU Journal of Maritime Affairs*, 18, 01 2019.

[104] I. Karunarathna, K. Alvis, P. Gunasena, T. Hapuarachchi, U. Ekanayake, K. Gunawardana, P. Aluthge, S. Gunathilake, S. Bandara, and A. Jayawardana. *The Essentials of Conducting a Literature Review: A Guide to Effective Summary, Synthesis, and Critical Analysis*, pages 179–182. Uva-Clinical Research, 03 2024.

[105] G. Kavallieratos, S. K. Katsikas, and V. Gkioulos. Towards a cyber-physical range. In *Proceedings of the 5th on Cyber-Physical System Security Workshop*, Asia CCS '19. ACM, July 2019.

[106] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou. Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 37:100526, 2022.

[107] G. Kessler and D. Zorri. AIS Spoofing: A Tutorial for Researchers. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 10 2024.

[108] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access*, 10:29493–29505, 2022.

[109] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1):20, Dec. 2019.

[110] K. H. Kim, K. Kim, and H. K. Kim. STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*, 44(6):991–1003, Nov. 2022.

[111] F. Klassen. Tcpreplay - PCAP editing and replaying utilities, Dec 2022.

[112] S. Kleber, H. Kopp, and F. Kargl. NEMESYS: Network message syntax reverse engineering by analysis of the intrinsic structure of individual messages. In *12th USENIX Workshop on Offensive Technologies (WOOT)*, Baltimore, MD, Aug. 2018. USENIX Association.

[113] N. Komninos, E. Philippou, and A. Pitsillides. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954, 2014.

[114] I. Kontopoulos, G. Spiliopoulos, D. Zissis, K. Chatzikokolakis, and A. Artikis. Countering real-time stream poisoning: An architecture for detecting vessel spoofing in streams of ais data. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, pages 981–986, 2018.

[115] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan. Dltif: Deep learning-driven cyber threat intelligence modeling and identification framework in iot-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2472–2481, 2023.

[116] R. Langley. NNEA 0183: A GPS receiver. *GPS world*, 6(7):54–57, 1995.

[117] A. Lavrenovs and G. Visky. Exploring features of http responses for the classification of devices on the internet. In *2019 27th Telecommunications Forum (TELFOR)*, pages 1–4, 2019.

[118] A. Lavrenovs and G. Visky. Investigating HTTP response headers for the classification of devices on the internet. In *2019 IEEE 7th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pages 1–6, 2019.

[119] A. Lavrenovs, G. Visky, and O. Maennel. Status detector for fuzzing-based vulnerability mining of IEC 61850 protocol. In *Proceedings of the European Conference on Information Warfare and Security*, ECCWS 2021. Academic Conferences International Ltd, 2021.

[120] S. Lebrun, S. Kaloustian, R. Rollier, and C. Barschel. Gnss positioning security: Automatic anomaly detection on reference stations. In D. Percia David, A. Mermoud, and T. Maillart, editors, *Critical Information Infrastructures Security*, pages 60–76, Cham, 2021. Springer International Publishing.

[121] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh. Maritime cybersecurity: A comprehensive review. `https://arxiv.org/abs/2409.11417`, 2024. Accessed on 09/09/25.

[122] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[123] W. Liu, X. Xu, L. Wu, L. Qi, A. Jolfaei, W. Ding, and M. R. Khosravi. Intrusion detection for maritime transportation systems with batch federated aggregation. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2503–2514, 2023.

[124] G. Longo, A. Merlo, A. Armando, and E. Russo. Electronic attacks as a cyber false flag against maritime radars systems. In *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, pages 1–6, 2023.

[125] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo. Macyste: A virtual testbed for maritime cybersecurity. *SoftwareX*, 23:101426, 2023.

[126] G. Longo, E. Russo, A. Armando, and A. Merlo. Attacking (and defending) the maritime radar system. *IEEE Transactions on Information Forensics and Security*, 18:3575–3589, Jan. 2023.

[127] M. S. Lund, J. E. Gulland, O. S. Hareide, ø. Jøsok, and K. O. C. Weum. Integrity of integrated navigation systems. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–5, 2018.

[128] K. Manandhar, X. Cao, F. Hu, and Y. Liu. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Transactions on Control of Network Systems*, 1(4):370–379, 2014.

[129] A. Matković and A. Šarolić. Shipboard military and marine VHF and UHF communications: open sea communication range in the adriatic sea. In *2022 International Symposium ELMAR*, pages 143–148, 2022.

[130] D. McFadden, R. Lennon, and J. O'Raw. AIS transmission data quality: Identification of attack vectors. In *2019 International Symposium ELMAR*. IEEE, Sept. 2019.

[131] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamillaand, and A. M. Satyam. *Improving Web Application Security*. Microsoft Corporation, 2003.

[132] P. H. Meland, K. Bernsmed, E. Wille, Ø. Rødseth, and D. A. Nesheim. A retrospective analysis of maritime cyber security incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15:519–530, 01 2021.

[133] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim. A retrospective analysis of maritime cyber security incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3):519–530, 2021.

[134] D. Mishchenko, I. Oleinikova, L. Erdődi, and B. R. Pokhrel. Multidomain cyber-physical testbed for power system vulnerability assessment. *IEEE Access*, 12:38135–38149, 2024.

[135] N. Moustafa, J. Hu, and J. Slay. A holistic review of Network Anomaly Detection Systems: A comprehensive survey. *Journal of Network and Computer Applications*, 128:33–55, Feb. 2019.

[136] S. Muggleton. Inductive Logic Programming. *New generation computing*, 8:295–318, 1991.

[137] I. Mukhopadhyay, K. S. Gupta, D. Sen, and P. Gupta. Heuristic intrusion detection and prevention system. In *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, pages 1–7, 2015.

[138] U. Nations. Review of maritime transport 2023. `https://unctad.org/system/files/official-document/rmt2023_en.pdf`, 2023. (Accessed on 17/05/25).

[139] P. Ngo, J. Sprinkle, and R. Bhadani. CANClassify: Automated Decoding and Labeling of CAN Bus Signals. *Journal of Engineering Research and Sciences*, 1(10):5–12, Oct. 2022.

[140] M. J. C. Ørnulf Jan Rødserh. Design challenges and decisions for a new ship data network, 2011.

[141] A. Oruc, A. Amro, and V. Gkioulos. Assessing cyber risks of an INS using the MITRE ATT&CK framework. *Sensors*, 22(22), 2022.

[142] E. Orye, G. Visky, and O. Maennel. Analysing the actual use of Controller–Pilot Data Link Communications. In *OpenSky 2022*, OpenSky 2022, page 18. MDPI, Jan. 2023.

[143] M. E. Orye, G. Visky, A. Rohl, and O. Maennel. Enhancing the cyber resilience of sea drones. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, pages 83–102, 2024.

[144] P. Peng, X. Xie, C. Claramunt, F. Lu, F. Gong, and R. Yan. Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. *Transportation Research Part E: Logistics and Transportation Review*, 195:103971, 2025.

[145] M. Pini, L. Pilosu, L. Vesterlund, D. Blanco, F. Lindström, and E. Spaltro. Robust navigation and communication in the maritime domain: The TRITON project. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 331–331, The Hague, The Netherlands, 2014. IEEE.

[146] H. N. Psaraftis. *The Future of Maritime Transport*, page 535–539. Elsevier, 2021.

[147] J. N. Ptasinski, D. Wasserman, and R. Casey. Protecting QoS in the ciphertext domain. In *MILCOM 2013 - 2013 IEEE Military Communications Conference*, pages 1328–1333, 2013.

[148] M. Puys, P.-H. Thevenon, and S. Mocanu. Hardware-in-the-loop labs for SCADA cybersecurity awareness and training. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES 2021. ACM, Aug. 2021.

[149] B. Qiu, M. Wei, W. Xi, Y. Li, and Q. Li. Cps attack detection of ships using particle filter. In *2021 China Automation Congress (CAC)*, pages 4993–4998, 2021.

[150] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo. Training the maritime security operations centre teams. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 388–393, 2022.

[151] B. Ristic, B. La Scala, M. Morelande, and N. Gordon. Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction. In *2008 11th International Conference on Information Fusion*, pages 1–7, 2008.

[152] M. Riveiro, G. Pallotta, and M. Vespe. Maritime anomaly detection: A review. *WIREs Data Mining and Knowledge Discovery*, 8(5):e1266, 2018.

[153] Ø. J. Rødseth, B. Kvamstad, T. Porathe, and H.-C. Burmeister. Communication architecture for an unmanned merchant ship. In *2013 MTS/IEEE OCEANS - Bergen*, pages 1–9, 2013.

[154] sailsoft. NemaStudio from Sailsoft. `https://www.sailsoft.nl/ais_simulator.html`. (Accessed on 06/11/2022).

[155] O. Savolainen, A. Elango, A. Morrison, N. Sokolova, and L. Ruotsalainen. Gnss anomaly detection with complex-valued lstm networks. In *2024 International Conference on Localization and GNSS (ICL-GNSS)*, page 1–7. IEEE, June 2024.

[156] A. Schreck. Virus origin in Gulf computer attacks in question. `https://phys.org/news/2012-09-virus-gulf.html`. (Accessed on 02/05/23).

[157] A. Schroeder, P. McClure, and P. Thulasiraman. Anomaly detection in operational technology systems using non-intrusive load monitoring based on supervised learning. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 1–6, 2024.

[158] Sealevel. USB to 8-Port RS-232, RS-422, RS-485 (Software Configurable) DB9 Serial Interface Adapter. `https://www.sealevel.com/product/2823-usb-to-8-port-rs-232-rs-422-rs-485-software-configurable-db9-serial-interface-adapter/`, 2022. (Accessed on 06/11/22).

[159] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen. A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97:101996, Oct. 2020.

[160] H. Y. Shahir, U. Glässer, N. Nalbandyan, and H. Wehn. Maritime situation analysis: A multi-vessel interaction and anomaly detection framework. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 192–199, 2014.

[161] A. Shostack. *Threat modeling*. John Wiley & Sons, Nashville, TN, Feb. 2014.

[162] F. Sicard, E. Hotellier, and J. Francq. An industrial control system physical testbed for naval defense cybersecurity research. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 413–422, 2022.

[163] M. Singh Popli, R. P. Singh, N. Kaur Popli, and M. Mamun. A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones. *IEEE Access*, 13:12634–12646, 2025.

[164] P. F. Smith, P. Thulasiraman, G. Oriti, M. Vygoder, and J. Gudex. Anomaly detection in shipboard operational technology systems using cyber analytics. In *2024 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE)*, pages 1–7, 2024.

[165] J. Spravil, C. Hemminghaus, M. v. Rechenberg, E. Padilla, and J. Bauer. fkie-cad/mana. [Online; accessed 2025-05-14].

[166] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, and J. Bauer. Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring. *Journal of Marine Science and Engineering*, 11(5), 2023.

[167] A. K. Stine Jacobsen. Estonia says Russia violates international rules with GPS interference | Reuters. `https://www.reuters.com/world/europe/estonia-says-russia-violates-international-rules-with-gps-interference-2024-04-30/`, 4 2024. (Accessed on 07/04/25).

[168] B. Svilicic, 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*, 7(10), 2019.

[169] S. Symes, E. Blanco-Davis, T. Graham, J. Wang, and E. Shaw. Cyberattacks on the maritime sector: A literature review. *Journal of Marine Science and Application*, 2024.

[170] K. Tam, K. Forshaw, and K. Jones. Cyber-ship: Developing next generation maritime cyber research capabilities. In *Conference Proceedings of ICMET Oman*, ICMET Oman. IMarEST, Nov. 2019.

[171] K. Tam and K. Jones. Cyber-Risk Assessment for Autonomous Ships. *Cyber Security*, page 9, 05 2018.

[172] K. Tam and K. Jones. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1):129–163, Jan. 2019.

[173] K. Tam and K. D. Jones. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, 3(2):147–164, 2018.

[174] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das. Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Communications Surveys & Tutorials*, 19(1):397–422, 2017.

[175] B. Tetreault. Use of the Automatic Identification System (AIS) for maritime domain awareness (MDA). In *Proceedings of OCEANS 2005 MTS/IEEE*, pages 1590–1594 Vol. 2, 2005.

[176] B. M. Thompson. GPS spoofing and jamming, 2014.

[177] D. Tiwari, B. S. Bhati, B. Nagpal, S. Sankhwar, and F. Al-Turjman. An enhanced intelligent model: To protect marine iot sensor environment using ensemble machine learning approach. *OCEAN ENGINEERING*, 242, DEC 15 2021.

[178] K. Tran, S. Keene, E. Fretheim, and M. Tsikerdekis. Marine network protocols and security risks. *Journal of Cybersecurity and Privacy*, 1:239–251, 04 2021.

[179] D. I. Urbina, J. Giraldo, A. A. Cardenas, J. Valente, M. Faisal, N. O. Tippenhauer, J. Ruths, R. Candell, and H. Sandberg. Survey and new directions for physics-based attack detection in control systems. Technical Report NIST GCR 16-010, National Institute of Standards and Technology, Gaithersburg, MD, Nov. 2016.

[180] R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi. A systematic literature review of cyber security monitoring in maritime. *IEEE Access*, 13:85307–85329, 2025.

[181] D. M. Valentine. Now you see me, now you don't: Vanishing vessels along argentina's waters. Technical report, Oceana, 2021.

[182] M. E. Verma, R. A. Bridges, J. J. Sosnowski, S. C. Hollifield, and M. D. Iannacone. CAN-D: A Modular Four-Step Pipeline for Comprehensively Decoding Controller Area Network Data, June 2021.

[183] G. Visky. AIS dataset. `https://www.kaggle.com/ds/4703219`, 2024.

[184] G. Visky, B. Adam, R. Vaarandi, M. Pihelgas, and O. Maennel. Open source intrusion detection systems' performance analysis under resource constraints. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, pages 201–208, 2024.

[185] G. Visky, S. Katsikas, and O. Maennel. Lightweight Testbed for IEC61162-450-Related Cyber Security Research. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 638–643, 2024.

[186] G. Visky, D. Khisteva, and O. Maennel. *Technical Considerations for Open-Source Intrusion Detection System Integration in Marine Vehicles*, pages 143–160. Springer Nature Switzerland, Cham, 2025.

[187] G. Visky, D. Khisteva, R. Vaarandi, and O. M. Maennel. Towards an open-source intrusion detection system integration into marine vehicles. In *2024 International Symposium ELMAR*, pages 263–268, 2024.

[188] G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam. Multi-purpose cyber environment for maritime sector. *Proceedings of the International Conference on Information Warfare and Security*, pages 349–357, Mar. 2022.

[189] G. Visky, A. Rohl, S. Katsikas, and O. Maennel. AIS data analysis: Reality in the sea of echoes. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024.

[190] G. Visky, A. Rohl, R. Vaarandi, S. Katsikas, and O. M. Maennel. Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024.

[191] G. Visky, R. Vaarandi, S. Katsikas, and O. Maennel. Statistical analysis-based feature selection for anomaly detection in ais dataset. In *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 159–164, 2025.

[192] G. Visky, A. Šiganov, U. R. Muaan, R. Varandi, H. Bahsi, and L. Tsiopoulos. MarCyb dataset. `https://data.taltech.ee/doi/10.48726/00fa9-5xv20`, 2024.

[193] G. Visky, A. Šiganov, M. u. Rehman, R. Vaarandi, H. Bahşi, H. Bahsi, and L. Tsiopoulos. Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 644–651, 2024.

[194] J. Wang, G. Ding, and H. Wang. HF communications: Past, present, and future. *China Communications*, 15(9):1–9, 2018.

[195] M. Whitman and H. Mattord. *Principles of Information Security*. Cengage Learning, Boston, MA, USA, 2021.

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

[197] B. Xing, Y. Jiang, Y. Liu, and S. Cao. Risk data analysis based anomaly detection of ship information system. *Energies*, 11(12), 2018.

[198] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang. Review on cyber vulnerabilities of communication protocols in industrial control systems. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–6, Beijing, China, 2017. IEEE.

[199] C. Yang, C. Fu, Y. Qian, Y. Hong, G. Feng, and L. Han. Deep learning-based reverse method of binary protocol. In *Security and Privacy in Digital Economy*, pages 606–624, Singapore, 2020. Springer Singapore.

[200] L. Yang, T.-J. Su, J.-C. Cheng, Y.-C. Siao, and C.-E. Weng. The decoding method study of dsc signal. In *2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pages 1–2, 2021.

[201] Y. Ye, Z. Zhang, F. Wang, X. Zhang, and D. Xu. NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces. In *Network and Distributed System Security Symposium*, Virtual, 2021. Internet Society.

[202] L. Yu, Y. Liu, P. Jing, X. Luo, L. Xue, K. Zhao, Y. Zhou, T. Wang, G. Gu, S. Nie, and S. Wu. Towards automatically reverse engineering vehicle diagnostic protocols. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1939–1956, Boston, MA, Aug. 2022. USENIX Association.

[203] A. Zainudin, R. N. Alief, M. A. P. Putra, R. Akter, D.-S. Kim, and J.-M. Lee. Blockchain-based decentralized trust aggregation for federated cyber-attacks classification in SDN-enabled maritime transportation systems. In *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, May 2023.

[204] S. Zhao, J. Wang, S. Yang, Y. Zeng, Z. Zhao, H. Zhu, and L. Sun. ProsegDL: Binary Protocol Format Extraction by Deep Learning-based Field Boundary Identification. In *30th IEEE International Conference on Network Protocols (ICNP)*, pages 1–12, Lexington, KY, USA, Oct. 2022. IEEE.

Acknowledgements

I, the author, would like to express my deepest gratitude to my family and loved ones for their unwavering support, patience, and encouragement throughout the course of my studies. Their belief in me has been a constant source of strength and motivation, especially during the most challenging moments of this journey.

I am sincerely grateful to my supervisor, Olaf, whose steady guidance, thoughtful feedback, and constant encouragement have meant more than words can express. His mentorship has not only shaped the direction and depth of this research, but also helped me grow with greater confidence and clarity.

My heartfelt thanks also go to Risto, for generously sharing his knowledge and unique perspectives. His support and insight have opened new ways of thinking and have truly enriched this journey.

To Sanja, thank you—for being a light during the journey when everything felt dark. Your presence, understanding and advice have helped me through more than you know.

My heartfelt thanks go to all my colleagues and co-researchers. Our collaborative efforts, stimulating discussions, and mutual support have not only made complex projects manageable but also deeply rewarding. Working alongside such dedicated and brilliant minds has been both a privilege and an inspiration.

Finally, to everyone who has contributed—–directly or indirectly–—to this academic endeavour, your support has been truly appreciated, and I am profoundly grateful.

Abstract

Cybersecurity for Maritime Operational Technology: Challenges, Considerations and Solutions

The growing reliance on commercial ships, driven by their cost-effectiveness and operational versatility, has been paralleled by an increasing exposure to cyber threats that jeopardise both safety and functionality.

This thesis, based on the collection of published and cited publications, addresses the complex challenge of securing maritime operational technology systems, with a particular focus on the design of cyber defence mechanisms for navigation and control networks. It explores strategies for detecting network anomalies indicative of cyberattacks and supports decision-making for effective mitigation.

To facilitate cybersecurity research and education in the maritime domain, the thesis also introduces simulated environments and publicly available datasets—collected or generated by the author—that provide valuable resources for vulnerability analysis and training. These environments have been used to identify and exploit vulnerabilities in on-board communication protocols and navigation software, demonstrating critical weaknesses in existing systems.

Furthermore, the thesis presents how automated reverse engineering techniques can streamline the development of defence solutions, eliminating the need for labour-intensive manual processes. It also proposes novel approaches based on inductive logic programming and statistical analysis for anomaly detection in data from the Automatic Identification System, thus improving the cyber resilience of situational awareness systems.

Together, these contributions offer a comprehensive foundation for advancing cybersecurity in the maritime sector, moving the industry toward a more robust and secure future.

Kokkuvõte
Merendustehnoloogia küberturvalisus: väljakutsed, kaalutlused ja lahendused

Kasvav sõltuvus kommertslaevandusest, mille põhjuseks on selle kulutõhusus ja mitmekülgsus, on suurenenud koos küberohtudega, mis ähvardavad nii laevade ohutust kui ka funktsionaalsust.

See väitekiri, mis põhineb avaldatud ja tsiteeritud publikatsioonide kogumikul, käsitleb merenduse käidutehnoloogia süsteemide turvalisuse keerulist väljakutset, keskendudes eelkõige navigatsiooni- ja juhtimisvõrkude küberkaitsemehhanismide kavandamisele. Väitekiri uurib strateegiaid küberrünnakutele viitavate võrguanomaaliate tuvastamiseks ja toetab küberrünnakute tõhusat tõrjumist käsitlevate otsuste tegemist.

Merendusvaldkonna küberjulgeolekualaste uuringute ja õppetöö hõlbustamiseks tutvustatakse lõputöös ka simuleeritud keskkondi ja avalikult kättesaadavaid – autori poolt kogutud või loodud – andmekogusid, mis pakuvad väärtuslikke ressursse küberhaavatavuste analüüsiks ja sellealasteks koolituseks. Neid keskkondi on kasutatud sisemiste sideprotokollide ja navigatsioonitarkvara haavatavuste tuvastamiseks ja ärakasutamiseks, mis näitab olemasolevate süsteemide kriitilisi nõrkusi.

Lisaks tutvustatakse väitekirjas, kuidas automatiseeritud pöördprojekteerimise tehnikad saavad tõhustada kaitselahenduste väljatöötamist, välistades vajaduse töömahukate käsitsi läbiviidavate protsesside järele. Samuti pakutakse välja uudseid lähenemisviise, mis põhinevad induktiivsel loogilisel programmeerimisel ja statistilisel analüüsil automaatse identifitseerimissüsteemi andmetes anomaaliate tuvastamiseks, parandades seega olukorrateadlikkuse süsteemide kübervastupidavust.

Üheskoos pakuvad need panused põhjaliku aluse küberjulgeoleku edendamiseks merendussektoris, suunates tööstust kindlama ja turvalisema tuleviku poole.

Appendix 1

Publication I
R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi. A systematic literature review of cyber security monitoring in maritime. *IEEE Access*, 13:85307–85329, 2025

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 April 2025, accepted 28 April 2025, date of publication 6 May 2025, date of current version 21 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3567385

SURVEY

A Systematic Literature Review of Cyber Security Monitoring in Maritime

RISTO VAARANDI[1], LEONIDAS TSIOPOULOS[1], GÁBOR VISKY[1], MUAAN UR REHMAN[1], (Graduate Student Member, IEEE), AND HAYRETDIN BAHŞI[1,2]

[1]Centre for Digital Forensics and Cyber Security, Department of Software Science, Tallinn University of Technology, 19086 Tallinn, Estonia
[2]School of Informatics, Computing, and Cyber Systems, Northern Arizona University, Flagstaff, AZ 86011, USA

Corresponding author: Risto Vaarandi (risto.vaarandi@taltech.ee)

This work was supported by the European Union research and innovation funding programme Horizon2020, project MariCybERA (agreement 952360).

ABSTRACT In recent years, many cyber incidents have occurred in the maritime sector, targeting the information technology (IT) and operational technology (OT) infrastructure. One of the key approaches for handling cyber incidents is cyber security monitoring, which aims at timely detection of cyber attacks with automated methods. Although several literature review papers have been published in the field of maritime cyber security, none of the previous studies has focused on cyber security monitoring. The current paper addresses this research gap and surveys the methods, algorithms, tools and architectures used for cyber security monitoring in the maritime sector. For the survey, a systematic literature review of cyber security monitoring studies is conducted following the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) protocol. The first contribution of this paper is the bibliometric analysis of related literature and the identification of the main research themes in previous works. For that purpose, the paper presents a taxonomy for existing studies which highlights the main properties of maritime cyber security monitoring research. The second contribution of this paper is an in-depth analysis of previous works and the identification of research gaps and limitations in existing literature. The gaps and limitations include several dataset and evaluation issues and a number of understudied research topics. Based on these findings, the paper outlines future research directions for cyber security monitoring in the maritime field.

INDEX TERMS Cyber security monitoring in maritime, cyber security monitoring, maritime cyber security, maritime, literature review.

I. INTRODUCTION

Modern societies are heavily depending on shipping and port industries, and maritime services and infrastructures are often regarded as critically important [1]. During the recent decades, maritime systems have become increasingly digitalised and interconnected [2], [3], [4]. For example, a modern vessel network relies heavily on network technologies such as Ethernet to connect the components of the ship's navigational system. As another example, the ship's Cyber-Physical System (CPS) is similarly dependent on solutions and technologies found in traditional IT systems.

Reliance on IT technologies has introduced similar cyber security issues into the maritime domain that can be found in traditional IT systems – like organisational computer networks, maritime systems are susceptible to cyber attacks that can disrupt normal operations for longer periods, thus inflicting significant financial damage and potentially leading to catastrophic consequences. For example, in 2017, the Maersk logistics company network was attacked by NotPetya malware which brought many port terminals of the company to a halt [5]. Although the company managed to resume normal operations swiftly, it was estimated that the financial losses inflicted by the malware could have reached as high as 300 million US dollars [6].

Unfortunately, the above incident is not a rare event, but several similar cyber attacks have been conducted against maritime infrastructures. For example, in a recent paper Afenyo and Caesar describe 12 similar security incidents in 15 large ports [7], and according to their report, in 2017 large

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

ports experienced 12 cyber attacks per day. Also, the average ransom paid due to ransomware attacks against maritime systems is 3.1 million US dollars [7]. Additionally, cyber attacks directly affecting the control of ships or monitoring of ship traffic have been recently reported. For example, in 2016 a cyber attack misdirected two navy vessels in the Persian Gulf [8]. In a case from 2017, cybercriminals gained access to the navigation systems of a container vessel owned by a German company, which had a capacity of 8250 TEUs [9]. Moreover, an Italian base station of Automatic Identification System (AIS) experienced a ship spoofing incident near Elba Island, where thousands of fake ships suddenly appeared and affected vastly the accurate monitoring of the maritime traffic in the vicinity [10].

In response to the escalating cyber threats in the maritime sector, leading maritime organisations like the International Maritime Organisation (IMO) and the Baltic and International Maritime Council (BIMCO) have been proactive in developing guidelines and recommendations to bolster maritime cyber security. The IMO, in particular, has integrated cyber security into its safety management systems under the ISM Code. This integration, effective from January 2021, mandates ship owners and managers to assess cyber security risks and develop necessary countermeasures to address these risks as part of their safety management systems [11]. BIMCO, the world's largest international shipping association, has also released several guidelines on cyber security, including the 'Guidelines on Cyber Security Onboard Ships' [12]. These guidelines are designed in collaboration with other industry associations and bring forward a comprehensive framework for cyber security risks management in maritime operations. The framework covers various aspects of cyber security, from identifying threats and vulnerabilities to implementing effective risk management processes.

Despite the recent incidents and the increasing volume of recommendations and guidelines by leading maritime organisations, Kechagias et al. [2] pointed out that cyber security remains a relatively new concept for the maritime industry, with many companies having low cyber security awareness and immature cyber security risk management culture. Furthermore, Afenyo and Caesar state in their paper [7] that current study programs of maritime educational institutions offer insufficient cyber security knowledge to their students and trainees. These factors have led to low adoption of cyber attack detection and mitigation solutions in the maritime domain and to insufficient amount of academic research conducted in this field.

Cyber attack detection and mitigation is further complicated by unique features of maritime systems (see [13], [14], [15] for a more detailed discussion). Maritime systems usually consist from a number of different IT and OT networks that connect a wide variety of maritime devices which communicate over specialised protocols such as NMEA. Therefore, the detection of attacks conducted in such networks requires detailed analysis of these maritime-specific protocols by dedicated solutions. Furthermore, ships have a limited network connectivity with the shore, which leads to the need for autonomous attack detection functionality on board. Also, space limitations and other physical constraints do not often allow to operate significant computational resources (e.g., server clusters) on board of ships, introducing the need for lightweight and resource-efficient cyber security solutions.

One of the key approaches for countering cyber attacks is *cyber security monitoring* (or *security monitoring* for the sake of brevity), which aims at *detecting cyber attacks with automated methods in a timely fashion*, allowing to mitigate the attacks in a manual, semi-automated, or fully automated way. For example, network and host-based Intrusion Detection Systems (IDSs) are widely acknowledged security monitoring technologies for real-time surveillance of computer networks and individual hosts to detect cyber attacks. Also, most security-aware organisations operate a Security Operations Centre (SOC) for collecting data from security monitoring tools to a central Security Information and Event Management (SIEM) system where it is processed and then presented to human security analysts for further action [16]. In addition to existing industrial solutions, many experimental approaches like Machine Learning (ML) based algorithms have been proposed for cyber security monitoring in recent academic literature (see the domain overview paper [17] for more details).

Although security monitoring technologies have been widely adopted by traditional (i.e., non-maritime) organisations and much academic research has been conducted in this field, security monitoring remains understudied in the maritime domain. For example, detailed cyber security guidelines by BIMCO [12] touch security monitoring only briefly, mentioning the use of network IDS and malware detection for security monitoring purposes, but failing to provide more detailed implementation recommendations to build maritime SOCs and other maritime security monitoring solutions. As another example, cyber risk management guidelines by IMO [18] do not address cyber security monitoring at all. As pointed out in [13], the generic nature of existing guidelines complicates the creation of maritime security monitoring systems, and dedicated research in this domain is needed. Also, as discussed in Section IV of this paper, maritime security monitoring is a relatively new research field. Due to the novelty of this research area, no domain overview studies have been published in maritime security monitoring that would analyse existing academic literature and identify the main research topics and open challenges.

This article fills the aforementioned research gap and specifically targets the research on security monitoring in the maritime domain. The purpose of the current study is to provide a Systematic Literature Review (SLR) of research papers published in the field. Note that our study focuses

on peer-reviewed academic papers, excluding grey literature from consideration. A similar approach has been used in several recent SLRs that address maritime cyber security, risk, and safety [3], [19], [20]. Using the same approach allows us to evaluate existing literature from an academic perspective and to identify research themes and gaps in analysed papers.

Our study begins with a discussion of selection criteria for relevant research that is followed by bibliometric analysis. We continue with creating a taxonomy for maritime security monitoring research and describe the trends and common themes in this research. Finally, our study provides a thorough analysis of existing research papers and identifies open issues, outlining future research directions for addressing these research gaps.

The remainder of this article is organised as follows. Section II describes similar literature review papers, Section III formulates the research questions of our study and discusses the selection criteria for research covered by our study, and Section IV contains the bibliometric analysis of the research papers selected for the study. Section V presents the taxonomy of relevant research and provides an in-depth analysis of selected research papers. Section VI discusses open issues and research gaps in the existing research literature, and Section VII concludes the article.

II. RELATED WORK

The purpose of this section is to provide an overview of similar literature review papers in the maritime domain (see Table 1). According to Table 1, existing papers have mainly focused on the analysis of past cyber incidents and ways for mitigating cyber threats in the future. For that purpose, the authors have proposed various measures, most notably by changing existing regulations and policies, and by improving the cyber security training and cyber awareness of personnel. Only one paper [3] covers some security monitoring studies, but their treatment has remained very brief without a deeper analysis. Although the papers from Table 1 do not focus on maritime security monitoring, we will discuss these papers for the sake of the completeness of our study, and to illustrate that the treatment of maritime security monitoring has remained too brief in existing literature reviews.

The SLR paper [19] focused on cyber attacks in maritime supply chain networks (MSCN), providing recommendations on the prevention and mitigation practices. The paper introduced a comprehensive taxonomy for cyber attacks which categorised them based on a number of factors, including the hacker group, attack type, affected systems, geopolitical impact, etc. According to the study, the key cyber security threats to MCSN include malware, Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks. For prevention and mitigation, the paper proposed a number of technical and policy-level measures (e.g., the use of multi-factor authentication, standardisation of cyber security practices, etc.), and practices for increasing cyber security awareness (e.g., development of training courses about attack prevention). The study briefly mentioned some security monitoring technologies without a deeper analysis.

Symes et al. [21] reviewed the literature focusing on the cyber attacks on autonomous vessels. The paper provided an overview on cyber attack types and described a number of well-known past security incidents in the maritime sector. The paper also discussed possible cyber attack mitigation techniques, mentioning some commonly used security monitoring techniques like network traffic monitoring without a more detailed treatment. For protecting autonomous vessels from cyber attacks, the study provided a number of recommendations, including employee training, regular updating and patching of systems, the use of strong passwords and multi-factor authentication, etc.

In [22], the papers on cyber security in the maritime domain were reviewed, describing common trends in relevant literature. As commonly occurring research themes, the authors identified the impact assessment for maritime cyber threats, recognition of maritime cyber threats (e.g., through vulnerability management tools or through interviews with human personnel), and categorisation and mitigation of maritime cyber risks. The study also presented recommendations for risk mitigation, and discussed gaps in existing literature and avenues for further research. As a supplementary material to their paper, the authors published a list of 21 maritime cyber attacks that have received media coverage and public attention, providing a short description of each cyber attack. Although the study briefly mentioned couple of security monitoring approaches for cyber risk mitigation (e.g., the use of ML methods for AIS anomaly detection), these approaches were not elaborated further.

The overview paper [7] focused on maritime cyber security threats, analysing relevant literature in the field. According to the authors, existing papers do not provide enough data on past cyber security incidents and this complicates research on modelling these attacks. In addition, the authors stated that the research on maritime cyber attack data-sharing methods has received little attention so far. Furthermore, it was stated that existing studies have not focused on assessing the financial impact of cyber attacks. The authors also noted that the current educational system does not prepare maritime professionals well enough to handle cyber threats. Finally, the authors pointed out that existing governmental and international policies do not regulate maritime cyber security well enough. For example, regulations should facilitate timely reporting of cyber security incidents and cooperation between maritime companies to increase knowledge sharing on the nature and mitigation of cyber attacks.

Erbas et al. [20] performed an SLR that critically examined and compared existing threat modelling and risk assessment methods in ship cyber security, developing a taxonomy for them. The authors analysed 25 scientific papers to understand the evolving landscape of cyber security practices for manned and autonomous ships. Significant inconsistencies were observed in current approaches and key challenges were identified, underscoring the urgent need for standardised

TABLE 1. Maritime cyber security literature review papers.

Paper	Year	Topics	Analysis of Security Monitoring Research Literature
[19]	2024	cyber attacks against MSCN and practices for prevention and mitigation	missing
[21]	2024	cyber attacks on autonomous vessels and attack mitigation techniques	missing
[20]	2024	cyber threat modelling and risk assessment in the field of maritime	missing
[22]	2023	impact assessment for cyber threats, categorisation and mitigation of cyber risks	missing
[7]	2023	analysis of cyber threats, regulations and policies	missing
[23]	2023	risk management, reliability and safety of autonomous ships	missing
[3]	2022	maritime cyber security and risk management	brief treatment of some studies without a deeper analysis
[4]	2022	analysis of past cyber incidents and potential cyber attacks against maritime systems	missing

threat modelling and risk assessment frameworks that consider also the special requirements of autonomous ships. Furthermore, the authors highlighted disparities, as well as inadequacy in tool support for the reviewed threat modelling and risk assessment methods. The need for more systematic validation of expert knowledge was also deemed critical. The topic reviewed by Erbas et al. is complementary to security monitoring, as threat modelling and risk assessment can provide direct inputs for enhanced monitoring solutions.

Bolbot et al. [3] conducted an SLR for maritime cyber security. The review included a bibliometric analysis that explored the countries, authors, academic venues and prevalent topics of the publications within the scope. The research studies were categorised and reviewed under topics ranging from various technical topics (e.g., cyber risk management, design of countermeasures, penetration testing) to many interdisciplinary topics such as maritime law, training development, and cyber incident analysis. Cyber risk management constituted a significant portion of the reviewed studies. Although some security monitoring papers were discussed in the study, their treatment remained very brief, since the focus of the article was lying elsewhere.

The bibliometric review [23] analysed the research literature on the risk, reliability, and safety of autonomous ships. Whereas cyber security was not the primary focus of this paper, it was identified as an important part of the ship's safety. Also, the study indicated that the cyber security of autonomous vessels has started to receive more attention from researchers recently. However, the paper did not include the treatment of cyber security monitoring topics.

Another study by Ben Farah et al. [4] reviewed cyber incidents in the maritime domain and provided a concise bibliographic analysis. The authors provided an extensive elaboration of maritime sub-systems located in vessels and ports, in addition to a review of the potential cyber attacks targeting these systems. Similarly to previous studies described in this section, the authors did not focus on cyber security monitoring issues.

Our article addresses a gap in the existing SLR literature on the cyber security of the maritime sector. Unlike previous analyses that have largely focused on the cyber threats and risks, our contribution specifically delves into maritime security monitoring systems, an area that has not been adequately covered thus far.

III. METHODOLOGY

In this section, the systematic literature review process will be discussed, describing the undertaken methodological approach together with the inclusion and exclusion criteria for relevant research, as well as the overarching review objectives.

A. AIMS AND RESEARCH QUESTIONS

An SLR is a methodological approach for collecting studies that constitute the research literature in the given field, systematically investigating this research field, answering focused research questions, and identifying the research gaps and research directions in the field [24]. Concretely, this article provides answers to the following research questions:

RQ1: What are the statistical characteristics of the papers that constitute the relevant literature? Analysing the literature through bibliometric methods will provide insights on the publication timeline, the types of venues in which the works were presented, and other properties of related work. RQ1 is answered by the discussion in Section IV.

RQ2: What research themes and topics are the papers focusing on, and what is the nature of research presented in the papers? The in-depth analysis of the paper topics will be supported by the paper taxonomy created by us, which is essential for facilitating a meaningful discussion. RQ2 is answered by the analysis in Section V.

RQ3: What are the main shortcomings and limitations of the papers? A thorough examination of the papers will reveal potential research gaps that can be addressed in future studies. RQ3 is answered by the discussion in Section VI.

B. SURVEY METHOD

During the development of this literature review the PRISMA protocol [25], [26] was followed. PRISMA is a widely used protocol for conducting an SLR and has been employed by several maritime cyber security literature review papers discussed in Section II [3], [19], [20], [21]. According to the PRISMA protocol, an SLR should have clearly defined objectives or research questions (see Section III-A), eligibility criteria for relevant literature (discussed in Section III-B1), a search strategy for finding relevant studies and selection process (discussed Section III-B2), and data extraction process (discussed in Section III-B3).

1) ELIGIBILITY CRITERIA

Initially, criteria need to be set that guide the search process and help to filter out irrelevant works. In this article, papers written in English and published in peer-reviewed journals and conference/workshop proceedings were included. When searching for relevant papers, we did not set an age limit for publications (i.e., we did not exclude papers published before a specific date). Papers that did not focus on maritime cyber security monitoring were excluded, just like papers focusing on non-IT-related methods from the fields of electrical engineering, physics, and other fields not related to IT. Editorials, opinions, keynotes, abstracts, tutorial summaries, position papers, panel discussions, technical reports and posters were also excluded. The duplicated publications because of different versions were eliminated from consideration, with only the most recent version being included. Since this SLR considers peer-reviewed academic papers, grey literature was not covered in this research.

Inclusion and exclusion criteria are summarised below. For a paper to be included, *all* inclusion criteria described in Section III-B1a must be met. On the other hand, a paper is excluded if it matches *any* of the exclusion criteria from Section III-B1b.

a: INCLUSION CRITERIA

- Studies that are peer-reviewed journal and conference papers.
- Studies in the domain of cyber security in the maritime sector with a focus on security monitoring and intrusion detection.
- Studies that propose novel cyber security monitoring and intrusion detection algorithms and technologies, and provide details about their application in the maritime domain.

b: EXCLUSION CRITERIA

- Studies that do not explicitly focus on cyber security monitoring and intrusion detection.
- Studies without any connection to maritime.
- Studies that are not peer-reviewed papers.
- Grey literature.
- Studies not written in English.
- Studies with their full texts not available.
- Studies that deal with electrical engineering, physics, and other fields not related to IT.

It should be pointed out that due to aforementioned criteria, a number of seemingly relevant maritime cyber security papers were excluded, because they did not focus on cyber security monitoring by contributing novel algorithms and technologies in this area. To provide a few examples of excluded papers, [27], [28] described maritime testbeds in the context of cyber attack tools and vulnerability testing without proposing new security monitoring approaches for detecting cyber attacks. In [29], a survey was conducted among maritime SOC experts to identify challenges in maritime SOCs without proposing novel security monitoring methods for addressing these challenges. In other words, the inclusion and exclusion criteria set the focus of the current study specifically to maritime cyber security monitoring papers with original algorithmical and technological contributions.

2) SEARCH STRATEGY

The studies were searched according to the following steps.

a: SEARCH FOR RELATED PUBLICATIONS

An initial search was applied to determine the current maritime SLR papers and to identify other significantly related publications. The most notable papers that we found have been described in Section II.

b: KEYWORD SELECTION

The selection of keywords heavily influences the results of the search. During the search phase, several keywords and their combinations were tried on search engines for electronic libraries. All the search engines that we used supported the creation of search queries with Boolean operators (AND, OR and NOT), which helped to narrow the focus of the search and limit the number of hits. Also, the engines allowed to apply the search expression on the title, abstract, keywords, metadata, etc. of the papers. The time frame of the search was also definable, and the wildcard characters (such as asterisk (*) and question mark (?)) allowed further flexibility during the search.

In the first phase of keyword selection, the keywords related to the maritime sector, like ''marine'', ''ship'', and ''navy'' were selected to define the sector. These keywords combined with the OR-operator led to too many generic papers about marine systems. Then, the focus was narrowed by cyber security monitoring-specific keywords and phrases, like ''monitoring'', ''intrusion detection'', ''IDS'', ''attack detection'', etc. The queries which combined these keywords yielded many publications, but the majority of them remained out of scope. By adding ''cyber'' to these keywords, the focus was narrowed down further.

c: AUTOMATED SEARCH ON BIBLIOGRAPHICAL SOURCES

During the initial stage of the automated search on bibliographical sources several trials were applied, using different combinations of keywords according to the main objectives of the review, with the aim to construct an optimal keyword set. The final keyword set was then used to construct the search query to be executed in various search engines of electronic libraries. The following electronic libraries were used to identify the publications relevant for the study: ACM Digital Library, IEEE Xplore, Elsevier Scopus, and Web of Science. Relevant publications were searched with the following query from all libraries: *cyber AND (monitoring OR "intrusion detection" OR "anomaly detection" OR "attack detection" OR ids) AND (maritime OR navy OR ship OR marine OR sea OR ais)*

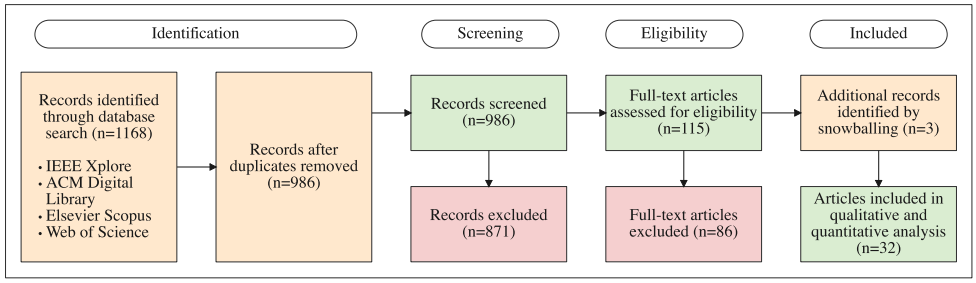


FIGURE 1. The use of PRISMA protocol for identifying relevant publications.

d: PAPER SELECTION PROCESS

The paper selection process has been summarised in Figure 1. The automated search from all libraries resulted in 1168 papers. After the library search, the four co-authors processed one library each in the form of independent work, and the findings were added to a shared database that helped to indicate the duplicated items. After the removal of the duplicates, 986 papers remained for further analysis.

The next step in the selection of relevant papers was the analysis of the title and the abstract. If a paper was irrelevant based on the title and/or the abstract, it was excluded (In case of doubt, the researcher read the full text). If the title and abstract were in the scope, the paper became a candidate. This part of the selection resulted in 115 candidates.

If a paper remained relevant, its main properties were noted to support our findings. After the full-text reading of the candidates, we had a set of papers conforming to the inclusion criteria. The procedure ended in 29 papers and snowballing identified 3 additional studies, yielding 32 publications for a detailed analysis. At this point, the bibliometric analysis was written, and the methodology for analysis was developed.

3) DATA EXTRACTION AND ANALYSIS

Following the SLR protocol, at this stage, the papers were fully assessed and relevant data were extracted relating to:

- Publication venue (e.g., name of the journal).
- Publication time and detailed author information.
- Research topic of the publication.
- The nature of the proposed security monitoring method.
- The nature of the maritime environment the proposed method was designed for.
- The nature of the data processed by the proposed method.
- The nature of the cyber attacks and anomalies detected by the proposed method.
- Performance evaluation details for the proposed method.
- The nature of the performance evaluation dataset and its availability information.
- Computational cost analysis for the proposed method.
- Availability information for the implementation of the proposed method.

IV. BIBLIOMETRIC ANALYSIS

To answer RQ1 (see Section III-A), this section presents the bibliometric analysis of relevant research.

In Figure 2, the annual distribution of the identified papers is shown, which does not reveal a clear pattern. However, an interesting observation can be made: the number of publications started rising after the major cyber incidents in 2017 within the maritime sector (e.g., the cyber attack against Maersk described in Section I). As can be seen from Figure 2, 30 research papers out of the 32 originate from 2018–2025, whereas only two research papers have been published before 2018. In other words, *maritime security monitoring is a relatively new research domain* which has started to receive more attention during the last 6–7 years.

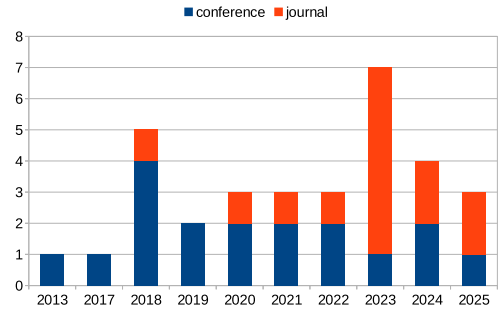


FIGURE 2. Publications per year.

According to Table 2, conference papers form a slight majority of the literature. On the other hand, journal articles are dominant among recent papers from 2023–2025. This indicates the increasing quality of relevant research. The most prominent publisher is IEEE with 24 papers (i.e., 75% of the analysed literature). As for conference papers, the vast majority of them (17 out of 18) have been published by IEEE, whereas only one paper originates from an ACM conference. When investigating the conference venues more closely, we found that three papers were published at the *International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, whereas each remaining conference accounted for one paper. As for journal papers,

three papers appeared in *IEEE Transactions on Intelligent Transportation Systems* and two papers in *IEEE Access*. Remaining journals published one paper each.

TABLE 2. Publications per publisher.

Publisher	Journal article	Conference paper
IEEE	7	17
ACM	-	1
Elsevier	3	-
MDPI	3	-
Springer	1	-
Total	14	18

The 32 research papers were authored by 126 researchers, and we also tried to identify more prolific authors in the field. For that task, we used a frequent itemset mining algorithm to identify all authors who have published at least two papers. Since the purpose of the frequent itemset mining algorithm is to identify associations, that allowed us to detect not just single authors, but also prolific co-author groups. According to our findings, no author has published more than three papers in this research domain, and a small minority of authors (16 out of 126 or 12.7%) have published more than one paper. That indicates that for the majority of authors, maritime security monitoring has not been a persistent focus area with a larger number of peer-reviewed academic publications. In a recent SLR paper by Bolbot et al. [3], a similar phenomenon has been reported – only 17% of authors have published more than one paper in the field of maritime cyber security. Also, we identified one co-author group with three publications, with the co-authors coming from the same country. This illustrates the fact that *maritime security monitoring has received limited attention so far*, and well-established prolific research groups specifically focusing on this particular field have not yet emerged.

V. ANALYSIS

A. TAXONOMY

To answer RQ2 (see Section III-A), we have created a taxonomy for existing research literature that is presented in Figure 3. Table 3 provides detailed information about the selected 32 research papers and how they map to different taxonomy categories. As Figure 3 illustrates, the research papers can be categorised by the environment they target, the type of data the proposed methods analyse, the type of the proposed methods, and the type of cyber attacks and anomalies that the proposed methods are able to detect. Note that these four categorisations from Figure 3 correspond to the "Targeted Environment", "Monitored Data", "Method Type", and "Detected Attacks and Anomalies" columns in Table 3.

When using Table 3 for analysing the mapping of papers to taxonomy categories in Figure 3, we discovered four non-overlapping clusters of closely related papers. The clusters cover 30 papers out of 32, and have been highlighted with different colours (red, blue, green, and orange) in Figure 3. If the majority of papers in some category belong to a single cluster, the category is highlighted with the colour of the respective cluster in Figure 3. Note that the "Unsupervised" and "Other methods" categories in Figure 3 are not highlighted with any colour, since there is no cluster which would cover the majority of papers in these categories. The four clusters from Figure 3 are summarised below:

- Studies on security monitoring for navigational systems [15], [30], [33], [37], [41], [45], [50], [54] (red cluster in Figure 3) – papers which propose the analysis of application layer protocol data for detecting AIS and GPS spoofing attacks, radar image manipulation attacks, and anomalies in navigational systems.
- Studies on security monitoring for CPSs [46], [48], [49], [51], [56] (blue cluster in Figure 3) – papers which propose the analysis of OT data for detecting attacks against vessel and canal CPSs.
- Studies on security monitoring for distributed maritime systems and networks [31], [34], [35], [39], [40], [42], [43], [58] (green cluster in Figure 3) – papers which propose the analysis of network traffic for detecting attacks against maritime IoT networks, maritime Software Defined Networks (SDNs), maritime wireless networks, and navy networks.
- Studies on security monitoring architectures and testbeds [13], [14], [36], [38], [44], [52], [53], [55], [57] (orange cluster in Figure 3) – papers which have not proposed one particular security monitoring method like the studies from previous clusters, but rather a security monitoring architecture or testbed.

The identified clusters in Figure 3 reveal some associations between taxonomy categories which describe the nature of existing research. First, studies on security monitoring for navigational systems (red cluster) have focused on the analysis of relevant application layer protocols, and rule-based security monitoring approaches have been usually applied in the context of navigational systems. Furthermore, studies on security monitoring for distributed maritime systems and networks (green cluster) have focused on network traffic analysis, and such studies tend to employ supervised ML methods. Also, studies on security monitoring for CPSs (blue cluster) have proposed the analysis of OT data, and there is no particular method category strongly associated with this cluster. Unlike papers from other clusters, the studies on security monitoring architectures and testbeds (orange cluster) propose a range of different methods and their simultaneous use with the ability to process different types of input data and detect different attacks and anomalies.

It should be pointed out that two papers, [32], [47], which are not covered by the above clusters are fairly close to one of them. Although these two papers focus on the analysis of application layer data instead of network traffic, they propose security monitoring methods for maritime IoT systems, and are thus closely linked to the green cluster in Figure 3. In the

TABLE 3. Overview of research papers.

Paper	Year	Paper Type	Targeted Environment	Monitored Data	Method Type	Monitoring Method	Detected Attacks and Anomalies
[30]	2025	M	navigational system	application layer protocol (Navico BR24 and NMEA)	supervised	deep learning	spoofing and data manipulation
[31]	2025	M	distributed maritime system/network	network traffic	supervised	deep learning	IoT attacks
[32]	2025	M	distributed maritime system/network	application layer protocol (NMEA)	other	stochastic semi-Markov processes	IoT attacks
[33]	2024	M	navigational system	application layer protocol (Navico BR24 and NMEA)	other	semi-supervised learning	spoofing and data manipulation
[34]	2024	M	distributed maritime system/network	network traffic	supervised	CatBoost	network layer attacks
[35]	2024	M	distributed maritime system/network	network traffic	supervised, unsupervised	deep learning, Isolation Forest	network layer attacks
[36]	2024	T	navigational system	application layer protocol (Navico BR24 and NMEA)	testbed	various (different types of IDS)	spoofing and data manipulation
[37]	2023	M	navigational system	application layer protocol (ASTERIX)	rule-based	policy enforcement	spoofing and data manipulation
[38]	2023	T	distributed maritime system/network	various (network traffic, NMEA, etc.)	testbed	various (IDS signatures, SIEM queries, etc.)	various
[39]	2023	M	distributed maritime system/network	network traffic	supervised	deep learning	IoT attacks
[40]	2023	M	distributed maritime system/network	network traffic	supervised	passive aggressive machine learning	IoT attacks
[41]	2023	M	navigational system	application layer protocol (NMEA GPS)	unsupervised	ensemble of unsupervised methods	spoofing and data manipulation
[42]	2023	M	distributed maritime system/network	network traffic	supervised	deep learning	IoT attacks
[43]	2023	M	distributed maritime system/network	network traffic	supervised	deep learning	network layer attacks
[14]	2022	T	distributed maritime system/network	various (network traffic, NMEA, etc.)	testbed	various (IDS signatures, SIEM queries, etc.)	various
[44]	2022	T	vessel CPS	various (network traffic, fieldbus traffic)	testbed	various (IDS signatures, etc.)	CPS attacks
[45]	2022	M	navigational system	application layer protocol (NMEA)	rule-based	predicate logic rules	navigational anomalies
[15]	2021	M	navigational system	application layer protocol (NMEA GPS)	unsupervised	One-Class Support Vector Machine	spoofing and data manipulation
[46]	2021	M	vessel CPS	OT (ship propulsion system)	supervised	Particle Filter	CPS attacks
[47]	2021	M	distributed maritime system/network	application layer protocol (IoT device events)	supervised	Light Gradient Boosting Machine	IoT attacks
[48]	2020	M	vessel CPS	OT (ship propulsion system)	unsupervised	Teager-Kaiser operator for time series analysis	CPS attacks
[49]	2020	M	vessel CPS	OT (ship propulsion system)	other	graph-based method	CPS attacks
[50]	2020	M	navigational system	application layer protocol (AIS)	rule-based	description logic rules	navigational anomalies
[51]	2019	M	canal CPS	OT (canal lock device)	supervised	deep learning	CPS attacks
[52]	2019	A	port infrastructure	various (network traffic, event logs, etc.)	architecture	various (IDS and antivirus signatures, event correlation rules, etc.)	various
[13]	2018	A	distributed maritime system/network	various (network traffic, event logs, etc.)	architecture	various (IDS signatures, event correlation rules, etc.)	various
[53]	2018	A	distributed maritime system/network	various (network traffic, OT systems, etc.)	architecture	various (agents with different functionality)	various
[54]	2018	M	navigational system	application layer protocol (AIS)	rule-based	distributed rule-based processing	spoofing and data manipulation
[55]	2018	A	distributed maritime system/network	various (ship navigational data, environment data, etc.)	architecture, unsupervised	Isolation Forest	various
[56]	2018	M	vessel CPS	OT (ship SCADA network)	rule-based	mathematical control theory integrated with rules	CPS attacks
[57]	2017	T	vessel CPS	OT (ship ICS and SCADA network)	testbed	dataset generation platform without any specific method	-
[58]	2013	M	distributed maritime system/network	network traffic	unsupervised	Maximum Entropy Estimation	network layer attacks

Paper Type: M – proposes a monitoring method; A – proposes an architecture; T – proposes a testbed

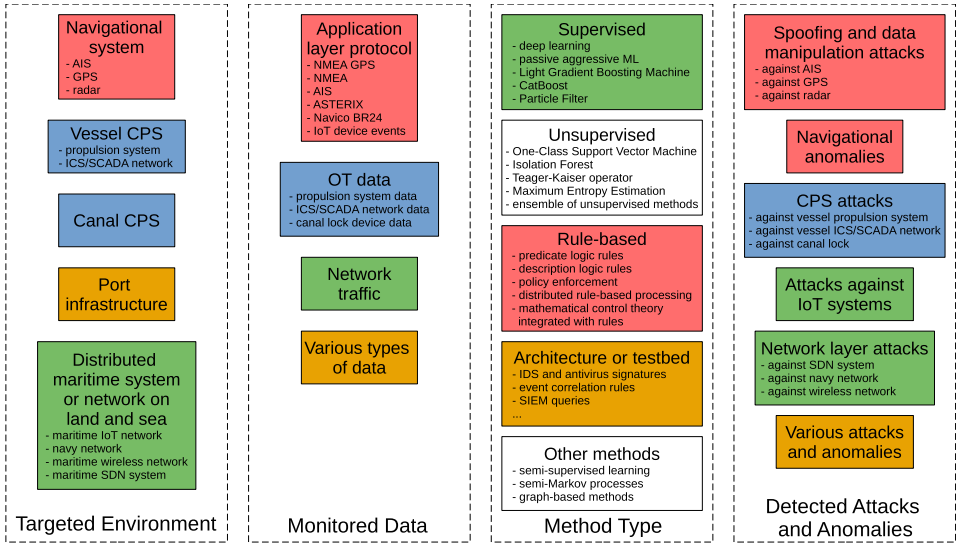


FIGURE 3. Taxonomy for existing research literature.

remainder of our study, we will consider these two papers together with their closest cluster.

In order to distinguish papers that have proposed security monitoring methods from the papers that have described architectures and testbeds, we divided all papers by their type (see the "Paper Type" column in Table 3). Letter *M* denotes the papers that discuss specific security monitoring methods, letter *A* the papers which describe the architecture of the entire security monitoring system, and letter *T* the papers that discuss testbeds designed for security monitoring data collection, testing, and exercises. As can be seen from Table 3, 23 papers have focused on specific security monitoring methods [15], [30], [31], [32], [33], [34], [35], [37], [39], [40], [41], [42], [43], [45], [46], [47], [48], [49], [50], [51], [54], [56], [58], while 4 papers have described architectures [13], [52], [53], [55] and 5 papers have described testbeds [14], [36], [38], [44], [57], respectively. Most papers that concern architectures and testbeds [13], [14], [36], [38], [44], [52], [53], [57] have not proposed any novel security monitoring algorithms for analysing specific data (e.g., network traffic), but have rather employed various well-known industrial security monitoring technologies such as signature-based network IDS, antivirus, etc., which monitor a wide range of different data types (see the "Monitored Data" and "Monitoring Method" columns in Table 3). Therefore, we have set the "Method Type" to *architecture* or *testbed* for these papers in Table 3, because the focus of these papers lies on the entire architecture or testbed, not on one security monitoring method. The only exception is the work by Jia et al. [55] which describes the use of an Isolation Forest-based algorithm within the proposed architecture.

As can be seen from Table 3, security monitoring architectures received a significant amount of attention until 2019 (all 4 relevant papers were published in 2018–2019, constituting almost half of the 9 papers published before 2020). In contrast, during the more recent years after 2019, the research focus has shifted towards security monitoring methods and testbeds, with the majority of the papers (19 out of 23) discussing security monitoring methods. This finding illustrates the fact that during the earlier research period before 2020, scholars preferred to focus on the architecture of the entire security monitoring system, studying the unique challenges that arise in maritime environments. After the architectural issues and solutions for them were identified, the attention moved to particular security monitoring methods which constitute the building blocks of security monitoring system architectures.

The "Targeted Environment" column in Table 3 indicates that most papers have proposed methods, architectures, and testbeds for addressing the needs of vessels or a distributed environment which involves vessels and land-based objects. In contrast, a small fraction of works target land-based environments only [51], [52].

As for the nature of monitored data (see the "Monitored Data" column in Table 3), we have used the term *network traffic* for studies which have proposed network monitoring methods without considering the application layer protocol in network packets. In the rest of the article, we will call such methods network traffic monitoring methods. Almost all the studies published until 2022 were not focusing on monitoring network traffic, with the work [58] being the only exception. Starting from 2023, a new trend can be observed where a significant proportion of papers have

described such methods [31], [34], [35], [39], [40], [42], [43]. However, these studies have been limited to specific environments like maritime IoT networks. Also, according to Figure 3, the majority of papers that have proposed the analysis of application layer data have employed it for security monitoring of navigational systems, whereas the analysis of OT data is generally used in the context of CPS.

As for the types of security monitoring methods (see the "Method Type" column in Table 3), supervised and unsupervised ML approaches are the most common, while some papers have also described rule-based and other approaches. As for supervised ML, deep learning (DL) based approaches have been the most widely employed [30], [31], [35], [39], [42], [43], [51], whereas no unsupervised ML method has seen more frequent use than the others. As Figure 3 illustrates, more than half of the papers which have proposed supervised ML approaches have applied them for maritime network security monitoring, whereas rule-based approaches tend to be applied for navigational systems.

Note that unlike the papers on architectures and testbeds, the studies of security monitoring methods involve thorough evaluations of particular algorithms on dedicated datasets. In order to get more insights into the relevant literature, Table 4 provides an overview of 24 papers that propose security monitoring methods (i.e., the papers from Table 3 with the "Method Type" column containing other values than *architecture* or *testbed*). Similarly to Table 3, Table 4 contains the "Detected Attacks and Anomalies" column, but provides more detailed information about the nature of attacks and anomalies. As this column indicates, some studies have proposed methods for detecting specific attack types. For example, whereas methods from [39], [42], [43] can detect network attacks of various types, algorithms from [31], [32], [35], [40], [58] are focusing on DDoS/DoS and network flooding attacks only. As another example, [45] proposes generic anomaly detection for NMEA messages, while [15], [41] focus on processing NMEA messages for the detection of GPS spoofing. Other methods described in papers from Table 4 include detection of radar image manipulation attacks [30], [33], [37], AIS anomaly detection [50], detection of AIS spoofing [54], detection of application layer attacks against maritime IoT systems [47], anomaly detection in the state and trajectory of uncrewed surface vehicles [55], detection of attacks against canal lock CPS [51], and detection of attacks and anomalies in the CPSs of ships [46], [48], [49], [56].

Table 4 also provides some insights into the evaluation process of the proposed security monitoring methods. In older studies which used maritime-specific data for evaluations, datasets were generally private (i.e., not publicly available). Also, whenever a public dataset was utilised, it was generally not maritime-specific. However, recent studies have started a new trend of creating and using publicly available maritime-specific datasets for evaluations, and examples of such public datasets include MARSIM [41], SOLIDS [31], and RadarPWN [59], which have been utilised in [30], [31], [33], [41].

Table 4 also reveals several other aspects of method evaluations – not all studies have published widely acknowledged performance metrics like *precision*, *recall*, and *F1-score* which provide a realistic picture of the method performance (for such studies, the "Performance Evaluation" column in Table 4 contains *no*). Also, many studies have not released the implementation of the method (see the "Is Code Publicly Available" column in Table 4) and have not assessed the computational cost of the method (see the "Computational Cost Assessment" column in Table 4).

The following sections provide a more detailed discussion of all papers from Table 3. For structuring the discussion, we have closely followed the aforementioned clustering of the selected research papers into four clusters based on the taxonomy presented in Figure 3. The papers on security monitoring architectures and testbeds (with the "Paper Type" column set to *A* or *T* in Table 3) are covered in Sections V-E and V-F, respectively (note that such papers correspond to the orange cluster in Figure 3). The discussion of the remaining papers on security monitoring methods (with the "Paper Type" column set to *M* in Table 3) has been divided into three subsections by the targeted environment (represented by red, blue, and green clusters in Figure 3) – the papers concerning security monitoring methods for distributed maritime systems and networks are covered in Section V-B, papers on security monitoring methods for navigational systems are covered in Section V-C, and papers on security monitoring methods for maritime CPSs are covered in Section V-D.

B. SECURITY MONITORING METHODS FOR DISTRIBUTED MARITIME SYSTEMS AND NETWORKS

Gyamfi et al. [40] developed an adaptive incremental passive-aggressive ML (AI-PAML) method for a network attack detection system (NADS) in an IoT-based Maritime Transportation System (MTS) environment. A resource-efficient multi-access edge computing (MEC) setting was proposed to execute the system at network edges. To avoid data saturation problems of online learning models and facilitate the updating of the detection system, the authors provided an enhanced approximate linear dependence and advanced data updating technique to remove the irrelevant data. For efficient execution, the computation-hungry algorithms of NADS were deployed through MEC servers located on the ship or onshore. The experimental results were obtained by using a PC running a layer 7 DDoS simulator named DDOSIM. This was used to execute DDoS attacks against IoT devices with the aim being to achieve real-time responses from the developed NADS. The CICDDoS2019 dataset[1] was used to train the AI-PAML model. Although this dataset is quite recent and relevant for the IoT domain, it is not directly connected to the maritime domain. The authors also benchmarked the proposed model against the "Perceptron"

[1] https://www.unb.ca/cic/datasets/ddos-2019.html

TABLE 4. Overview of research papers on security monitoring methods.

Paper	Year	Evaluation Data	Is Data Maritime Specific	Is Data Publicly Available	Is Code Publicly Available	Performance Evaluation	Computational Cost Assessment	Detected Attacks and Anomalies
[30]	2025	RadarPWN	yes	yes	no	yes	no	radar image manipulation attacks
[31]	2025	SOLIDS	yes	yes	no	yes	yes	DDoS attacks against maritime underwater IoT systems
[32]	2025	internal	yes	no	no	yes	no	DDoS attacks against maritime IoT systems
[33]	2024	RadarPWN	yes	yes	no	yes	no	radar image manipulation attacks
[34]	2024	internal	yes	no	no	yes	yes	network attacks against navy satellite networks
[35]	2024	WSN-DS	no	yes	no	yes	no	DoS attacks against maritime wireless networks
[37]	2023	internal	yes	no	no	yes	yes	radar image manipulation attacks
[39]	2023	NSL-KDD	no	yes	no	yes	no	network attacks against maritime IoT systems
[40]	2023	CICDDoS2019	no	yes	no	yes	yes	DDoS attacks against maritime IoT systems
[41]	2023	MARSIM	yes	yes	yes	yes	no	GPS spoofing
[42]	2023	TON-IoT	no	yes	no	yes	no	network attacks against maritime IoT systems
[43]	2023	X-IIoTID	no	yes	no	yes	no	network attacks against maritime SDN-based systems
[45]	2022	internal	yes	no	no	no	no	anomalies in NMEA messages
[15]	2021	internal	yes	no	no	yes	yes	GPS spoofing
[46]	2021	internal	yes	no	no	no	no	attacks against ship's CPSs
[47]	2021	DS2OS	no	yes	no	yes	no	application layer attacks against maritime IoT systems
[48]	2020	internal	yes	no	no	no	no	attacks against ship's CPSs
[49]	2020	internal	yes	no	no	yes	no	attacks against ship's CPSs
[50]	2020	internal	yes	no	no	no	no	anomalies in AIS messages
[51]	2019	internal	yes	no	no	no	no	attacks against canal lock CPS
[54]	2018	MarineTraffic AIS	yes	no	no	yes	no	AIS spoofing
[55]	2018	internal	yes	no	no	no	no	anomalies in the state and trajectory of unmanned surface vehicle
[56]	2018	internal	yes	no	no	no	no	anomalies in ship's CPSs
[58]	2013	internal	yes	no	no	no	no	network flooding attacks against navy networks

and "Stochastic Gradient Descent" models regarding the training and prediction runtime and its latency was found to be better than the benchmark models after all models run against the DDOSIM attack.

In [42], a monitoring system was proposed that used Cyber Threat Intelligence (CTI) extracted with the DL-based method, Long Short-Term Memory (LSTM) based Variational Autoencoder. The system applied the Bi-directional Gated Recurrent Unit (Bi-GRU) method for detecting attacks addressing IoT devices. According to the authors, the proposed system featured a high performance, having a better accuracy than several other similar methods from non-maritime research literature. The main drawback of the study is the fact that no maritime-specific dataset was used for the validation of the method, but rather the TON-IoT dataset[2] which contains network traffic of consumer IoT devices. As one of the limitations, the study mentioned that the proposed DL-based method is computationally more expensive than traditional ML algorithms.

Liu et al. [39] proposed a CNN-MLP based Intrusion Detection model for MTSs which was trained via Federated Learning (FL), also called FedBatch by the authors. In the mentioned model, a Convolutional Neural Network (CNN) was utilised for data feature extractions, while Multilayer Perception (MLP) was used for attack classification to locally detect intrusion on each vessel. The study targeted IoT-based MTSs and endeavoured to address the limitations inherent in conventional learning algorithms, which consume an amount of computing resources that can not be provided in resource-constrained IoT environments. The study aimed to protect data privacy by not sharing the training data obtained locally in vessels with the cloud. Instead, the models were induced locally in the remote devices, and their parameters were shared with the cloud. The authors proposed a robust and efficient model for MTS security monitoring by training and testing their model on the generic NSL-KDD dataset.[3]

In [58], a method for detecting network flooding attacks was presented which harnessed a Maximum Entropy Estimation based statistical ciphertext (CT) flow analysis

[2]https://research.unsw.edu.au/projects/toniot-datasets

[3]https://www.unb.ca/cic/datasets/nsl.html

mechanism. The authors specifically focused on protecting Quality of Service (QoS) in the CT domain against DoS attacks in the context of the Automated Digital Network System (ADNS) INC III, a critical network system of the US Navy for unclassified and secret information exchange. The proposed approach detected anomalies in the network by using anomaly-free packets as training data and estimated their distribution as a baseline which represented normal traffic. For anomaly detection purposes, the network traffic was observed and its distribution was compared with the baseline distribution. Furthermore, the study provided an attack response mechanism by limiting network traffic. However, in some cases, normal traffic flow was also unnecessarily limited.

Zainudin et al. [43] introduced a decentralised trust aggregation solution which used blockchain to provide a secure and trusted federated IDS infrastructure. The solution offered a federated intrusion classification framework for SDN enabled marine traffic services. The scheme utilised an interplanetary file system with a network that used blockchain for proof-of-authority (PoA). An IDS model that used FL-based collaboration was also proposed, together with the lightweight intrusion detection and classification model. The solution, leveraging CNN, surpassed other comparable implementations. The effectiveness of this model was evaluated using the X-IIoTID dataset,[4] specifically curated for IoT-related research but not being maritime-specific.

In [47], a supervised ML approach was proposed to secure sensor networks against cyber attacks and adversarial activities. The work focused on maritime IoT-based systems, addressing the attack detection in the network layer of such infrastructures. The paper introduced the data collection, pre-processing, model training, method optimisation, testing and its results. According to the results, the Enhanced Light Gradient Boosting Machine (Light-GBM) technique delivered excellent results on low computational cost and network bandwidth usage, which is essential in the complex marine IoT environment, that is also limited from the communication bandwidth's viewpoint. The experiments and the IoT attacks classification were conducted on the Distributed Smart Space Orchestration System (DS2OS) dataset,[5] an open-source but not maritime-related dataset.

Algarni et al. [35] explored the use of both supervised (LSTM-based DL) and unsupervised (Isolation Forest) ML methods for detecting network layer attacks in maritime wireless networks. The methods relied on the edge computing paradigm, i.e. processing data locally on network nodes. For comparative evaluation of supervised and unsupervised methods, the authors employed the WSN-DS dataset,[6] which is not maritime specific. According to the study, LSTM-based DL outperformed Isolation Forest, demonstrating a significantly higher F1-score when detecting network attacks.

Agnew et al. [34] proposed a supervised method for monitoring naval submarine satellite communication networks. For creating the model of the satellite network, the authors utilised queuing theory. The method employed the CatBoost ML algorithm for detecting zero-day cyber attacks, training the algorithm on the data obtained from queuing analysis. For evaluation, simulations were used, and according to the authors, the method yielded a high precision, recall, and F1-score metric values. In addition, the study provided a computational cost analysis, indicating that the proposed approach is cost efficient and requires a minimal amount of CPU time.

The paper [32] suggested the use of stochastic semi-Markov processes for monitoring NMEA messages in maritime IoT networks, so that DDoS attacks in such networks could be identified in a timely fashion. The system proposed by the authors involved data collection from IoT devices and the detection of device states which reflect the likelihood of a security incident. Also, Markov chains were used to model state transitions in the network for identifying anomalies which can indicate DDoS attacks. The proposed system was evaluated by simulating normal traffic and DDoS attacks in maritime IoT systems, and according to the authors, the system demonstrated excellent performance with a low rate of false positives and false negatives.

Singh Popli et al. [31] proposed a DL-based method for monitoring underwater IoT networks which involved FL. With this distributed learning approach, a pretrained global ML model was shared with devices for further local training on local data, updating the global model with parameters received from devices. For comparative evaluation of FL with traditional centralised ML, the authors employed a non-maritime-specific CICIDS2017 dataset.[7] However, for evaluating the attack detection capabilities of the proposed approach, the authors used a publicly available SOLIDS dataset[8] developed in their lab, which is reflecting normal traffic and DDoS attacks in maritime underwater IoT networks. The study also involved the computational cost analysis for the proposed method, demonstrating its suitability for real-life networks.

Discussion: According to the analysis of 10 papers in this section, the current research on security monitoring methods for maritime networks has focused on specialised networks – IoT networks have been studied in 6 papers [31], [32], [39], [40], [42], [47], whereas two papers have targeted military networks [34], [58]. Moreover, one paper on monitoring SDN networks [43] considered an IoT-specific dataset during evaluations, making IoT networks a dominant theme in relevant research. Therefore, the monitoring of

[4]https://ieee-dataport.org/documents/x-iiotid-connectivity-and-device-agnostic-intrusion-dataset-industrial-internet-things
[5]https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces
[6]https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds
[7]https://www.unb.ca/cic/datasets/ids-2017.html
[8]https://drive.google.com/drive/u/0/folders/1IjFET0QOOZ4foEG-qzBLzTQKag6cUdiy

other maritime network types than IoT has not received enough attention and constitutes an understudied research area. As for the network monitoring methods, supervised ML methods have been the most frequently employed (proposed in 8 papers [31], [34], [35], [39], [40], [42], [43], [47]), with DL-based approaches being the most prominent of them [31], [35], [39], [42], [43]. On the other hand, as argued in a recent domain overview study [17], the superiority of DL over traditional ML methods is not yet proven in the field of network intrusion detection, and DL involves a significantly higher computational cost which might not always justify its use for network monitoring (only one study [31] provided the relevant cost analysis). These considerations are even more pronounced for maritime systems which are often resource constrained. Therefore, the research on lightweight ML methods suitable for maritime networks is another understudied area.

Finally, the use of supervised ML for network security monitoring is known to suffer from the issue of *concept drift* [17] – since the surrounding environment changes over time, a supervised ML model will become obsolete, requiring retraining on new labeled datasets which are expensive to create. Existing works have not addressed this issue on datasets which cover longer time frames (e.g., several months), and studying ML methods for tackling concept drift (such as active learning) is a highly relevant future research direction. To this end, only the work by Gyamfi et al. [40] touched on this issue by providing a technique to keep only relevant data used for the dynamic updating of the learned model, although specific validation for this aspect of the work was not provided. Another interesting direction is further study of unsupervised ML methods, which do not need labeled data.

C. SECURITY MONITORING METHODS FOR NAVIGATIONAL SYSTEMS

In [54], a distributed architecture was presented for detecting spoofing and falsification attacks in streams of AIS data in real time. Average speed was measured on the shortest path between positions obtained from two consecutive AIS broadcast messages. Then, this value constituted the basis of the spoof detection approach implemented in the study. The architecture was of the Master-Workers type, with the Master distributing the AIS messages to Workers for analysis in an efficient manner incorporating load balancing techniques. The approach was validated by generating a 43,912,236 AIS messages dataset from *marinetraffic.com* and performing simulations by attacking the dataset in various ways. The validation dataset has not been made public. The reduction of false positives as well as the extension to more attack types was mentioned to be part of future work.

Amro et al. [45] proposed a method for analysing navigational NMEA-0183 messages that communicate the data of the various onboard sensors. The objective was to identify possible anomalies and their malicious causes. For this, relevant anomaly detection algorithms were developed. To facilitate the analysis the authors employed a maritime cyber security testing environment that they previously developed [60] which included the NMEA-Manipulator tool enabling the generation of the anomalies by attacking sensor data. To develop the anomaly detection method, the authors first identified NMEA message types that affected navigation together with relevant message fields and their values. Potential anomalies that can appear in NMEA messages and attack techniques which can trigger these anomalies were studied using the MITRE ATT&CK framework.[9] Finally, the authors investigated different approaches for implementing attack and anomaly detection for NMEA messages. According to the authors, specification-based approach was best suited for that purpose, which involved the use of rules that described the normal behaviour of the system (i.e., any violation of these rules indicated an anomaly). Also, for some specific attacks that involved changing the arrival rate of NMEA messages to the system components, the authors recommended frequency-based anomaly detection that involved checking if the message rate remained within the expected boundaries.

Iphar et al. [50] analysed the weaknesses of AIS in their study. Since these weaknesses allow falsifying and spoofing AIS messages, a rule-based system was developed for anomaly detection from AIS messages. The authors proposed over 900 rules or *integrity items* for assessing the integrity of AIS messages. The first order assessment rules considered only one field from a single AIS message, while the second order rules analysed several fields from a single message. The third order rules considered fields from several AIS messages of the same type, whereas the fourth order rules analysed several AIS messages of all types. Based on the truth values of rules and external contextual information, flags were set that were further used for calculating ship-related risks and their levels. For evaluating the proposed method, a Python-based prototype was created which utilised a database for storing AIS data, intermediate results from computations, and contextual data. The prototype was evaluated on about 24 million real-life AIS messages collected over 6 months. In the study [50], the authors provided a detailed description of risk evaluation for 4 cases involving anomalous AIS messages (the study considered 13 cases in total). In all 4 cases, the prototype raised one or more flags. However, the study did not evaluate the system on a larger number of cases, including the assessment of a false positive rate of the system (reflected by the precision metric in ML literature).

The study [15] focused on the detection of GPS spoofing. For that purpose, an anomaly detection approach was proposed which employed a One-Class Support Vector Machine (OC-SVM) and analysed NMEA messages that carried GPS information. The authors selected OC-SVM because it was easy to implement and did not require much computational resources, making it suitable for deployment

[9] https://attack.mitre.org/

on low-end hardware. During the experiments, the authors trained OC-SVM on data collected from a maritime simulator and also on real-life data collected on a small boat. For implementing GPS spoofing during the experiments, the authors utilised a device which generated a GPS signal carrying wrong GPS information. According to the experiments, the OC-SVM based anomaly detection method featured a high recall and precision. To demonstrate the lightweight nature of the method and its low computational cost, the authors implemented the method on a Raspberry Pi based monitoring device that was suitable for deployment on real-life ships. Such evaluation of the actual computational cost of the proposed method and its suitability for real-life deployment sets this study apart from many other works.

Similarly to the previous paper [15], the study by Spravil et al. [41] focused on the detection of GPS spoofing with the analysis of relevant NMEA messages. According to the authors, the analysis of NMEA messages allowed for the development of dedicated monitoring modules which could be easily integrated into the ship's network. To demonstrate the viability of that approach, the authors publicly released the implementation of the MANA (MAritime Nmea-based Anomaly detection) framework. The framework combined unsupervised anomaly detection methods into an ensemble, and to identify suitable methods, the authors investigated various GPS spoofing methods, with a number of methods originating from other domains than maritime (e.g., aviation and mobile phone networks). As a result of the investigation, five methods were selected for the ensemble. To assess the performance of the MANA framework, the authors created the MARSIM dataset which contained a large number of different GPS spoofing attacks and normal GPS data. Also, the dataset was released into the public domain.[10] According to the experiments, the ensemble of five methods featured a higher recall than each method (the ensemble regarded the anomaly as detected if any of the five methods provided a relevant indication). As one of the limitations of their approach, the authors identified the need for well-chosen thresholds for each method to avoid false positive alerts.

Hossain et al. [33] proposed a semi-supervised ML approach for detecting attacks against maritime radar systems which involve manipulations of the radar image (e.g., freezing or rotating the image, adding an object to the image, etc.). One of the main purposes of semi-supervised ML is to lower the data labelling workload of human experts [61]. For the experiments, the authors used the RadarPWN dataset[11] which is maritime specific and publicly available (more details on the dataset can be found in [59]). For semi-supervised ML, the authors utilised the Random Forest classifier which was initially trained on a small dataset labelled by a human expert. The classifier was then used to predict the labels for unlabelled training data, and samples with the most certain predictions were added to training data. After that, the classifier was trained again on the labelled training dataset extended with newly added samples. The whole training process consisted of 10 such training iterations, extending the training dataset during each iteration with automatically labelled samples, which reduces the workload of human experts. According to the authors, the final classifier achieved a high precision, recall, and F1-score metric values.

The study [37] described a number of attack scenarios for manipulating the maritime radar image which involved the misuse of the ASTERIX protocol. For detecting these attacks, the authors proposed a rule-based system which utilised candidate policies, where each candidate policy described the normal operating conditions of a radar. For making candidate policies adjustable for specific environments, the policies contained variables which were automatically set by the system. Also, if some candidate policies were not applicable in the given environment, they were automatically excluded from consideration. Selected policies were used for the real-time analysis of ASTERIX messages, and alerts were raised on policy violations. According to the study, the proposed system featured a high attack detection rate with a small number of false positives. In addition, the computational cost of the system was low, making it suitable for resource-constrained maritime environments. The experiments conducted in the study were supported by the MaCySTe testbed [38], which will be described in Section V-F.

To avoid data privacy issues of conventional ML and DL approaches that typically require centralising data on a single server, Hossain et al. [30] presented an FL-based approach with the aim to enhance the detection and classification of cyber attacks against marine radar systems. The method constructed a global model by utilising the collective learning ability of several distant clients, which involved local training at clients without sharing sensitive data. For evaluation, the RadarPWN dataset was used and partitioned into numerous subsets to represent different data sources in a collective learning environment. The authors provided a comprehensive evaluation of their approach, with high values reported for each performance metric. Additionally, the authors evaluated several DL-based approaches for the attack detection component of their system, choosing CNN as the best fit. The authors stated some limitations of their study, e.g., the need for reliable communication between clients and the central server, which might not always be practical in maritime operations due to connectivity issues.

Discussion: All 8 papers discussed in this section have focused on the analysis of application layer data (e.g., NMEA or AIS messages) in order to detect AIS spoofing, GPS spoofing, image manipulation attacks against maritime radars, and navigational anomalies. As for the used methods, rule-based approaches are the most common and have been suggested in four papers [37], [45], [50], [54], whereas

[10] https://github.com/fkie-cad/mana
[11] https://doi.org/10.5281/zenodo.6805559

remaining four papers have suggested unsupervised ML [15], [41], semi-supervised ML [33], and DL [30]. When employed for security monitoring, rule-based approaches are known to be very precise [17] and are thus used by many industrial security monitoring products (such as commonly used network IDS platforms like Suricata). However, creating a rule-based system requires domain experts and is a time-consuming process. One open research area is the use of rule mining algorithms in order to speed up the rule creation process.

Also, the current research has largely focused on rule-based and unsupervised ML-based approaches, whereas only two papers analysed in this section have suggested the use of supervised and semi-supervised ML for the detection of navigational attacks and anomalies. Therefore, further study of these approaches is another open research area, as is dealing with advanced ML issues like concept drift. Finally, as mentioned in [17], rule-based and ML-based security monitoring systems are complementary, with both of them having unique advantages. Therefore, building and evaluating such hybrid systems for navigational security monitoring is another future research direction. Inductive logic programming [62] is a potential hybrid approach which could be applied to automate the rule learning process in a supervised ML manner.

D. SECURITY MONITORING METHODS FOR MARITIME CPS

In [49], graph-based models were utilised for the detection of attack propagation in CPSs. A graph model that represented the digital and physical system layers was proposed in the paper, considering the interdependencies between CPSs by using the system variables. The model was applied in a case study that involved a small-scale system consisting of a ship with a fuel tank, valve, motor and propeller which were monitored through a PLC. One scenario of normal system usage and four attack scenarios including port scan, closing the PLC and man-in-the-middle attacks were simulated in the study. According to the authors, the method did not produce a false positive alert for the normal scenario, whereas one attack scenario out of four remained undetected (i.e., precision and recall were 100% and 75%, respectively). However, the evaluation of the method was limited to the aforementioned five scenarios without testing the method on a larger dataset.

Yoginath et al. [51] proposed a Recurrent Neural Network (RNN) based Digital Twin (DT) model to simulate an operational CPS of a Canal Lock. Their model performed real-time analysis to detect anomalies at the earliest, specifically anomalous changes in water levels within chambers through which ships pass. The study [51] used an actual PLC, sensors, valves and pumps to emulate the behaviour of the Canal Lock CPS physically. The authors identified all the possible scenarios, i.e., the ship's up and down movements, performed by Canal Lock CPS and trained a set of RNN models using the emulation data as input. Anomaly detection was performed through a difference-based method (analysis of PLC and DT predicted values). The previously DT predicted value was compared with the current PLC read value and the deviation was captured, with the larger value being regarded as an indication of the attack. Furthermore, to evaluate the RNN model, the authors performed live validation of the system. However, no specific CPS attacks were executed to test the accuracy of the DT concept for anomaly detection.

Xing et al. [56] presented an anomaly detection method for the Ship Information System (SIS) based on risk data analysis. Since SIS is a typical SCADA system, the authors first elaborated on all the different operational and networking components of the SIS SCADA system and then they proceeded with presenting the data anomaly detection approach based on a cooperative state space control mathematical model, for the data propagated between the sensors, the distributed controller units and the actuators. A so-called Critical State Estimation (CSE) Algorithm was proposed based on the Industrial State Modelling Language (ISML). Detection rules were formulated as ''condition *implies* action'' with the condition being a boolean formula composed by various predicates indicating values that are expected by system components. The approach was validated by simulations on the ship dynamics under heading sensor signal attacks.

The study [48] focused on the use of Teager-Kaiser operator for time series analysis to detect anomalies in a ship's propulsion system in the case of cyber attacks. During the experiments, the authors collected the following time series data – oil consumption, fuel consumption, propeller speed, and valve opening. The following attacks were conducted for evaluating the anomaly detection methods – port scanning with *nmap* tool, DoS attack with *hping* tool, and exploiting the vulnerability of the ship's propulsion PLC for stopping and starting the PLC. Port scanning and DoS attacks did not influence the propulsion system, and only the attack against the PLC had a significant impact. According to the experiments, the Teager-Kaiser operator managed to identify sudden changes in the ship's propulsion system time series data. However, the evaluation results were presented in the form of graphs only for the 5-minute time period which involved a single attack against the PLC. Therefore, it is difficult to assess what would be the detection rate for many attacks of different types against the propulsion system during a longer time frame (e.g., several days or weeks), and a more detailed analysis of the proposed method was identified as future work in the study.

The study [46] proposed the use of a Particle filter-based anomaly detection method for time series data collected from a ship's CPS to detect cyber attacks. In the study, the authors focused on data collected from the ship's propulsion system – the temperature of the cylinder exhaust, cooling water pressure, and the speed of the fuel flow. For training the anomaly detection system, the authors used data collected

from a new cargo ship during its first sailing week, assuming that the probability of cyber attacks during this week is very low. For evaluating the anomaly detection algorithm, data from the second half of the first sailing year was employed. For discussing the anomaly detection rate of the algorithm, the authors presented graphs for the 5,000-minute time frame (about 3.5 days) in the study. Although the graphs displayed some fluctuations in the time series data for the propulsion system, the study did not detail whether these sudden changes were the result of a cyber attack or rather a side effect of normal navigation.

Discussion: As for the research themes in five analysed papers, three papers focused on the vessel propulsion system [46], [48], [49], whereas the remaining two papers targeted vessel SCADA network [56] and canal lock CPS [51], respectively. Therefore, apart from the propulsion system, other parts of the vessel CPS have received little attention so far in the context of cyber security monitoring. Similarly, research on security monitoring for land-based maritime CPSs is scarce, and these research gaps are likely to be addressed by future works. As for the types of security monitoring methods (see Table 3), no particular method types have been dominantly employed for security monitoring of maritime CPSs, and proposed methods have included supervised ML [46], [51], unsupervised ML [48], rule-based [56], and graph-based [49] methods. However, when analysing OT data from maritime CPSs, existing methods have generally not considered discriminating cyber attack related CPS malfunctions from CPS faults not caused by malicious cyber activity. Therefore, the root cause analysis for maritime CPS faults and anomalies is an unexplored research area which deserves closer attention.

Furthermore, process-aware attacks target CPSs to induce disruptions in physical processes [63]. Temporal characteristics of the processes observed on the sensors, actuators or control algorithms are utilised for the detection of malicious actions beyond the failures [63]. The reviewed papers do not address this monitoring approach comprehensively. Just focusing on the control functions in the physical space via process-aware approaches may not be enough to discriminate the usual system failures from malicious actions. Process-centric indicators should be correlated with other cyber-space indicators that reveal the prior actions of the attackers before compromising the control functions. To facilitate this research, it is necessary to generate datasets that include indicators about physical and cyber spaces.

Finally, in order to properly study the effects of cyber attacks on maritime CPS, a highly realistic lab environment is needed which would mimic a real-life CPS as closely as possible. Apart from a few recent works [38], [44] that will be discussed in Section V-F, the creation of realistic maritime CPS testbeds has been understudied, and can be regarded as a promising future research direction.

E. SECURITY MONITORING SYSTEM ARCHITECTURES

In [13], a maritime SOC architecture was proposed. The authors first provided an overview of the specific constraints of the maritime domain which complicate building a maritime SOC (for example, the limited network connectivity of the vessels with shore). The SOC architecture described by the authors took these constraints into account, consisting of vessel-based and shore-based parts. The proposed vessel-based functional blocks of the SOC were the following:

- *Network Connection Safety* allowed to safely connect monitoring sensors to monitored systems (e.g., port mirroring for network monitoring sensors);
- *Network Probe Isolation* was responsible for monitoring the network (e.g., a signature-based IDS), while being isolated from other sensors;
- *Local Preprocessor* normalised and correlated events, to lessen the amount of data that needed to be sent to shore via network link with a limited bandwidth;
- *Local Engine* stored events on a ship for local alerting;
- *Ship Shore Manager* acted both as a data cache and sender of data from a ship to shore, keeping the data in cache if there were issues with the network link, and being responsible for the link bandwidth management;
- *Cyber Situational Awareness Console* provided a local simplified overview of the ship's cyber state to the crew. The presence of the local onboard monitoring capability allowed for addressing scenarios where connectivity with the shore-based SOC was missing and the ship's situation could not be assessed in a central land-based monitoring centre.

The proposed shore-based functional blocks of the SOC were the following. First, *Ship Shore Manager* and *Bandwidth Manager* were responsible for receiving the security data from ships and managing network connectivity with remote parties; *Central Processor* was responsible for filtering and normalising the received security data, and *Data Store* was a big data solution that stored the normalised security data. In addition to the aforementioned blocks, the shore-based SOC had other functional blocks that can also be found in traditional SOCs. For example, human operators could use specialised tools for big data analytics, searching the collected security data, creating visualisations, etc., to achieve maritime cyber situational awareness. In addition, SOC could be linked to external threat intelligence sources and incident response platforms. Finally, collected security data could be used for creating a so-called maritime-recognised cyber picture of the status of individual ships and the entire fleet. In their study [13], the authors mentioned that the previously described architecture has been thoroughly tested. Although no detailed information was provided about the nature of these tests and the performance of the architecture, the architecture was validated in a later independent study [14] by building a maritime exercise environment according to this architecture (see Section V-F).

Schauer et al. [52] proposed a security monitoring system architecture for ports which would integrate security data from two distinct domains – traditional IT systems (i.e., cyber assets) and physical assets of the port. The authors proposed to collect a wide variety of security events from IT systems, including firewall events, antivirus events from end user devices, and event logs of applications and servers. To monitor the physical assets of the port, the authors suggested data collection from physical access control systems, dedicated monitoring sensors which can create security events, etc. According to the authors, security events from cyber and physical assets should be collected into the hybrid situational awareness framework which can analyse events from both domains. For real-time analysis of these events, two major components were proposed for the situational awareness framework – Event Correlation Engine (ECE) and Threat Propagation Engine (TPE). According to a widely used definition [64], *event correlation* is a real-time process that involves assigning a new meaning to event groups which occur within predefined time windows. For implementing ECE, the DROOLS engine was used. As the authors stated, the use of ECE allows the detection of complex security incidents which manifest themselves through several events from different domains. The purpose of the TPE was to establish the impact of high-priority security alarms via graph-based analysis, where the nodes of the graph represented cyber and physical assets and the edges of the graph reflected the dependencies between assets. The approach by Schauer et al. [52] was sound and novel considering the time of its publication, integrating cyber and physical situational awareness methods for port infrastructures (including communication with ships). On the other hand, the study did not provide a deeper analysis of the possible cyber attacks and how they could be detected in the maritime infrastructure domain, exemplifying the proposed approach through two attack scenarios.

The paper [55] discussed a big data architecture to collect OT data from Uncrewed Surface Vehicles (USVs) for various purposes like business management, disaster prevention, anomaly detection, etc. The authors proposed the collection of the following data from USVs – ship's performance and navigational data (e.g., speed, position, level of fuel, etc.), data about the environment (e.g., wind, temperature, etc.), data from sensing devices that provided information about the objects around the ship (e.g., data from the radar), and data that was collected from other sources than the USV itself (e.g., industrial data about the USV collected from the manufacturer). For storing the collected data, a cloud-based solution was proposed that was using PostgreSQL database. According to the authors, visualisation capabilities were an important aspect of the big data architecture, and the authors suggested the use of the LinDA toolkit for processing the data in the PostgreSQL database. As an example use case for the big data architecture, the paper described an anomaly detection scenario for identifying abnormal combinations of the sailing angle and the USV speed. For anomaly detection purposes, an Isolation Forest-based method was proposed, but the study did not include its performance evaluation.

Möller et al. [53] discussed an agent-based intelligent maritime traffic management system to support a coastal Vessel Traffic Service (VTS) with a clear situational picture, traffic and environmental information. For that purpose, the authors proposed to introduce a Multi-Agent System (MAS) that extended to vessels to exchange relevant data (e.g., navigational and safety information) with the central VTS. Following the concept of connected cars, the authors also introduced the concept of connected ships which were continuously in contact with each other. That facilitated the exchange of important navigational information not only through VTS but directly between ships. The authors also described how to augment the proposed distributed MAS with a security monitoring functionality. First, the authors detailed the weaknesses of the wireless communication networks used by MAS, and mentioned a mitigation opportunity in the form of anomaly detection for data flows in the network. The study also suggested the use of neural networks for the detection of cyber attacks, but did not report any experiments with the proposed method together with attack detection performance results.

Discussion: From the four analysed papers, two papers have proposed generic security monitoring architectures, with [13] discussing a maritime SOC and [52] a situational awareness system for a port infrastructure which is similar to SOC. The remaining two papers have proposed security monitoring architectures for specific purposes (a big data architecture for monitoring USVs [55] and a VTS-centric security monitoring architecture [53]). Although the creation of SOCs is a widely studied cyber security topic (see [16] for a recent domain overview), most works in this area lack detailed recommendations and guidelines for implementing a SOC in a scalable and resource-efficient way (for example, recommendations on software solutions to use and guidelines for configuring them) [65]. Furthermore, only a few works have evaluated the SOC architectures and provided relevant performance data (e.g., for resource consumption and event processing rate of system components). Since maritime environments are often resource-constrained, these topics are also relevant in the maritime context and constitute valuable future research directions.

According to recent studies [16], [66], SOC analysts are often overwhelmed by security alerts of low importance which leads to analyst burnout and alert fatigue. For supporting the human analysts, alert prioritisation has been identified as an important topic for SOC environments [16], and several ML approaches have been recently proposed for that purpose [67], [68]. Since alert prioritisation algorithms for reducing human alert fatigue have not been studied in the context of maritime SOC, it can be regarded as one of the open issues for future work.

F. SECURITY MONITORING TESTBEDS

The short paper [57] aimed to present a platform to generate data and scenario traces for the evaluation of algorithms for intrusion detection. The introduced solution was based on a ship's two critical subsystems: 1) the propulsion and engine control in which a computer fan simulated the ship's propeller and the fan's actual RPM represented propulsion, 2) the navigation subsystem with the rudder control to simulate the ship's direction changes. Each subsystem had an independent controller which used common industrial communication protocols, like Modbus, DNP3, and S7. The heart of the setup was the central controller built on a Raspberry Pi. The simulated sensor – that provided the measurement of the engine parts' temperature – was made of an open-source electronics platform called Arduino. The authors provided an overview of the project, describing its overarching objectives and outcomes, but the overview lacked the required depth for allowing to recreate a similar platform.

Raimondi et al. [14] described a testbed for conducting cyber exercises to train maritime SOC teams. The testbed followed the maritime SOC architecture proposed in [13] (see the previous section for a detailed discussion) and was implemented with Linux containerisation techniques. The testbed employed a ship simulator for simulating the ship at sea and a custom Python script for transmitting data received from the simulator as NMEA messages to other ship-related testbed components. For monitoring the ship network, the authors proposed Suricata IDS which employed Lua scripting for parsing NMEA messages. For the cyber situational awareness console on the ship, the authors used Splunk which also forwarded data to a shore-based central SIEM server (another instance of Splunk). To illustrate the training process of maritime SOC operators, the authors described an example cyber exercise which involved the injection of false NMEA messages into the ship network that interfered with the gyrocompass. The task of the trainees was to detect this attack with the help of Splunk query language.

In [44], a testbed was presented for experimenting with the Industrial Control System (ICS) of a warship. To achieve a high degree of realism, the authors utilised the physical devices of real ships as much as possible. The testbed implemented the following four areas of the warship – propulsion system (engine and propellers), direction (rudders), energy (fuel for the engine and fuel pump), and artillery (76mm main gun and motors for moving the gun turret). For these four areas, a physical implementation contained a bow and rear of the ship with a physical gun turret, rudders, propellers, physical devices of the bridge, etc. According to the authors, the use of virtualised solutions would have decreased the realism of the testbed, since they would have not allowed for the full imitation of the ship's real-life environment. For low-level monitoring of Modbus RTU fieldbus traffic in the ICS of the ship, the authors proposed the use of Zeek IDS with specialised traffic capturing hardware and Zeek protocol parser for the Fieldbus protocol (in [69], the authors provided a more detailed description of this solution). For regular network monitoring, commercial IDS sensors were suggested by the authors.

Basels et al. [36] introduced a testbed to identify navigation radar vulnerabilities and to experiment with relevant security monitoring solutions. The offensive module of the testbed was based on the Radar Attack Tool (RAT) [59], which is able to launch a variety of image manipulation attacks against maritime radars (e.g., freezing or scaling the image, removing an object from the image, etc.). The defensive module of the testbed involved Snort3 and IPAL IDS solutions which were configured to detect the attacks against maritime radars by analysing application layer data in network traffic. For Snort3, the authors developed the rules for detecting message injection attacks, whereas IPAL was employed for detecting message modification scenarios. The detection by IPAL relied on two methods outlined in [70].

Longo et al. [38] described the MaCySTe testbed designed for maritime cyber security experiments with the vessel IT/OT systems. The authors released detailed installation instructions of the testbed together with the source code in order to facilitate maritime cyber security research in other organisations. The testbed was built on top of Linux containers, making it a highly resource-efficient solution with modest computational requirements. The testbed provided a detailed emulation of the vessel network, navigational devices, propulsion system, and other components together with relevant protocols (e.g., Navico BR24 and Modbus). For evaluating security monitoring functionality, the testbed supported the use of network probes and SIEM. The network probes captured and parsed traffic in the vessel network, forwarding relevant data to SIEM for visualisation and analysis. The authors also provided some illustrative examples on how the MaCySTe testbed can be utilised for cyber attack and attack detection experiments.

Discussion: From the five analysed papers, two papers have proposed testbeds for experimenting with vessel ICS and SCADA networks [44], [57], one paper has proposed a testbed for maritime radars [36], one paper has described a more general maritime testbed for a wide range of cyber security experiments [38], whereas [14] focuses on a SOC testbed for training maritime SOC analysts. Since [57] is a short paper, the discussion of the proposed testbed remains fairly brief, but in the remaining four papers [14], [36], [38], [44] detailed testbed descriptions are provided, with all testbeds being highly realistic environments for conducting maritime cyber security monitoring experiments and trainings.

However, it should be considered that some of the aforementioned studies represent specific environments (e.g., warship's ICS). Therefore, the creation of highly realistic maritime cyber security testbeds remains an open research area. Also, realistic testbeds allow for generating high-quality datasets for maritime cyber security monitoring experiments. As discussed in Section V-A, although recent studies have

publicly released several maritime-specific datasets, their number remains limited (see Table 4), and the creation of such datasets is another important future research direction.

VI. DISCUSSION

In order to answer RQ3 (see Section III-A), this section presents the discussion of our main findings about the identified research gaps. The main findings are based on the analysis from the previous section and are presented below.

Finding 1: Lack of evaluations on maritime-specific datasets which are publicly available. Numerous publications have evaluated the proposed security monitoring methods on datasets that are not publicly accessible (see Table 4), so the experiments in question are characterised by an inherent lack of reproducibility, thereby precluding the possibility of result verification. Although a number of studies have employed publicly available datasets, these publicly available datasets are often not maritime specific but rather generic intrusion detection datasets like NSL-KDD, CICDDoS2019, TON-IoT, etc. (see Table 4). Therefore, the validity of these research results remains questionable, because the datasets do not represent the actual maritime systems closely enough. Some notable exceptions include [30], [31], [33], [41] which have employed the publicly available maritime-specific datasets (see Table 4).

Finding 2: Lack of data generation about system failures. According to recent domain overview papers [71], [72], [73], research datasets used for developing and testing security monitoring solutions in IT networks [71], ICSs [72], and CPSs [73] include attack and normal system activities. Thus, the developed security monitoring approaches discriminate attacks from normal activities or identify anomalies originating from malicious actions. We have observed a similar approach in the datasets related to the maritime domain. However, in practice, system failures arising from unintentional causes (e.g., software or hardware errors, environmental condition changes) can be mistakenly detected as anomalies resulting from cyber attacks. Thus, the root causes of the incidents are not usually identified accurately and timely, causing delays and discrepancies in incident handling and recovery operations. As pointed out in [73], it is important to include activities representing all failure modes of the target system in the datasets. For example, recent studies in the energy domain aim to discriminate cyber attack related anomalies from non-malicious ones [74], [75], [76]. Therefore, we contemplate that the generation of datasets that include system failures in addition to normal and attack cases would facilitate the research in developing solutions for more granular and informative security monitoring functions.

Finding 3: Lack of publicly available experiment code and prototype implementations. Most studies have not released the implementations of proposed methods and the experiment code (see Table 4). This shortcoming is another serious obstacle to achieving reproducibility, and it also complicates the evaluation of the proposed methods on different datasets and in live environments.

Finding 4: Lack of proper performance evaluations with appropriate metrics. Several studies have failed to properly evaluate the performance of the proposed security monitoring methods with proper metrics (see Table 4). However, in the field of security monitoring and ML, widely acknowledged performance metrics exist such as precision, recall, and F1-score [17]. The failure to use such widely used metrics makes it difficult to assess what is the attack detection rate and false positive rate of the proposed methods, and how the proposed methods compare to other approaches.

Finding 5: Lack of proper computational cost evaluations. Only some studies (e.g., [15], [31], [34], [37], [40]) have assessed the computational cost (e.g., CPU time and memory consumption) of the proposed security monitoring methods. However, the computational cost is an important consideration, since vessel networks can usually not accommodate specialised computing platforms for expensive calculations. For example, some recently proposed security monitoring methods are based on DL (see Table 3), which is known to be computationally expensive [17], and without the computational cost assessment the applicability of these methods in maritime environments remains questionable.

Finding 6: Lack of detailed assessments of cyber attack impacts on maritime CPSs. Some papers (e.g., [46], [51]) which have proposed methods for detecting cyber attacks against maritime CPS have not conducted cyber attacks in a relevant lab environment. However, the lack of such cyber attack experiments prevents to assess what is the real impact of these attacks on CPS, and what are the best avenues for detecting these attacks. Furthermore, the assessment of cyber attack impacts and best attack detection approaches requires a lab environment which mimics CPS as closely as possible. However, apart from a few recent studies [38], [44], the methods for building highly realistic maritime CPS labs and testbeds have not received enough attention in the relevant literature.

Finding 7: Lack of detailed evaluation of the proposed security monitoring system architectures. Security incident handling processes usually require collecting, aggregating and correlating security events from various sources to do more relevant prioritisation, accurate incident categorisation and impact assessment. Although the idea of using maritime SOC and aggregating diverse security data from many sources has been proposed in several past studies [13], [52], [53], [55], existing works have not published detailed evaluation data for the proposed architectures. However, some similar studies that are not maritime specific have included such evaluations (e.g., see [65]), and works from maritime domain should follow the same approach.

Finding 8: Security monitoring methods for some maritime systems have been understudied. As discussed in Section V, security monitoring methods for distributed maritime networks have been largely focusing on IoT networks, while other network types have received less attention. Also, most network monitoring research has utilised supervised ML methods, and studying the feasibility of other methods is

a valuable future research direction. For example, semi-supervised ML is known to greatly reduce the model development cost of supervised ML [61], but we found only one relevant work in the analysed literature [33]. Also, process-aware maritime CPS monitoring which correlates indicators from the physical and cyber space remains an open research topic. As for security monitoring methods for navigational systems, the use of supervised and semi-supervised ML, rule mining, and inductive logic programming for rule learning are other possible future research directions.

Finding 9: Advanced ML issues have been understudied in the maritime context. The shortage of domain-specific datasets in the maritime field is a major obstacle to understanding the performance of ML methods in solving maritime security monitoring problems. However, once datasets are created, various advanced problems related to the application of ML methods can be addressed. Handling the concept drifts that may occur in the feature space, learning from small labelled datasets and efficient utilisation of experts for labelling are some research directions that can be tackled in this domain. The application of large language models for a better understanding of the detection rules and monitoring results [77], and receiving suggestions from these models about the course of actions can be studied in the maritime context. Some of the security monitoring tasks can be deployed into the resource-constraint devices in maritime systems for making real-time decisions. Thus, another potential research dimension would address running and optimising learning models on such devices (e.g., TinyML applications as recommended in a recent study [78]).

Finding 10: Human aspects of security monitoring systems have been understudied in the maritime context. Although the ultimate goal of cyber security monitoring would be the full automatisation of attack detection and response mechanisms, it is highly expected that human experts will take a critical part in incident handling processes in any case. Thus, interdisciplinary and holistic approaches involving human and technical aspects of the problem domain are highly needed. Training and awareness programs for security analysts and maritime operators addressing design issues for the minimisation of human errors (e.g., optimising user interfaces of monitoring tools), enhancing communication between incident handling teams or selecting the right course of action under stressed conditions are some sample topics that require further research in this domain. Another potential research topic is the use of ML tools for alert prioritisation that helps to prevent alert fatigue among SOC analysts (a recent study among maritime cyber security experts has confirmed the importance of this topic [29]). Apart from a few works which have discussed the expected competence of maritime SOC analysts and their training process [14], and the design of training events for building maritime cyber security skills [79], existing studies have generally not touched on human aspects of maritime security monitoring.

VII. CONCLUSION AND FUTURE WORK

In our research, we conducted a systematic literature review in which we surveyed four digital libraries. After a careful selection process described in Section III, we identified 32 papers in the field of cyber security monitoring in maritime. In Section V, we provided a comprehensive overview of these publications, highlighting their strengths and shortcomings. We shared the bibliometric analysis of the papers in Section IV, and we discussed the identified research gaps in Section VI. Our developed taxonomy (outlined in Section V-A) provides a structured framework for analysing cyber security monitoring-related literature, allowing insights into the strengths and limitations of existing publications.

As we discussed in Section VI, we identified several shortcomings and limitations of the currently available literature. The present study yields the following findings. First, we found several dataset related issues (Findings 1-2). Maritime-specific publicly available datasets should be used for experiments to ensure the reproducibility and the validity of research results for maritime environments. Also, the datasets should include system failure data not associated with cyber attacks, since that would allow us to evaluate how well the security monitoring methods can distinguish the effects of cyber attacks from other system failures.

Second, we identified several evaluation related issues (Findings 3-7). To improve the quality of evaluations, appropriate metrics should be used for assessing the performance of algorithms. Also, it is important to assess the computational cost of the proposed methods. Evaluations should be realistic, involving real cyber attacks that are conducted in a lab environment with a high degree of realism. For the sake of reproducibility, it is essential to share the experiment code and prototype implementations. Similarly to security monitoring methods, detailed evaluations are needed for security monitoring system architectures.

Third, we identified several previously unexplored research areas of maritime security monitoring (Findings 8-10). For example, the monitoring methods for maritime IoT networks and vessel propulsion systems have been studied more in the current literature, whereas other types of maritime distributed networks and maritime CPSs are potential targets of future research. Similarly, process-aware model-based methodologies, emphasising the correlation between physical and cyberspace indicators for enhanced system malfunction and cyber attack distinction, could be leveraged in the maritime domain. Furthermore, several advanced ML issues like concept drift and learning models for resource-constrained environments deserve more attention in the field of maritime security monitoring. While the training of personnel constitutes a fundamental aspect of cyber security monitoring, it is noteworthy that only few works specifically addressing this subject matter could be identified in the relevant literature.

As for future work, we plan to study the methods of creating a realistic maritime cyber security monitoring lab,

using our experience in the field [27]. Also, we plan to use this lab environment for the creation and release of maritime-specific datasets to facilitate security monitoring research in the maritime domain. Finally, our plans include studying advanced ML-based security monitoring methods on these datasets.

REFERENCES

[1] C. Bueger and T. Liebetrau, "Critical maritime infrastructure protection: What's the trouble?" *Mar. Policy*, vol. 155, Sep. 2023, Art. no. 105772. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308597X23003056

[2] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *Int. J. Crit. Infrastruct. Protection*, vol. 37, Jul. 2022, Art. no. 100526. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166

[3] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *Int. J. Crit. Infrastruct. Protection*, vol. 39, Dec. 2022, Art. no. 100571. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555

[4] M. A. B. Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, p. 22, Jan. 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22

[5] C. Bronk and P. DeWitte, in *Proc. Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor*. Cham, Switzerland: Springer, 2022, pp. 241–254.

[6] A. Belokas. (May 2018). *Maersk Line: Surviving from a Cyber Attack*. [Online]. Available: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

[7] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean Coastal Manage.*, vol. 236, Apr. 2023, Art. no. 106493. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0964569123000182

[8] J. King. (2016). *The Story You aren't Being Told About Iran Capturing Two American Vessels*. Accessed: May 2, 2025. [Online]. Available: https://www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two-american-vessels/212937/

[9] T. Blake. (2017). *Hackers Took 'full Control' of a Container Ship's Navigation Systems for 10 Hours*. Accessed: May 2, 2025. [Online]. Available: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems

[10] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, "Assessing cyber challenges of maritime navigation," *J. Mar. Sci. Eng.*, vol. 8, no. 10, p. 776, Oct. 2020. [Online]. Available: https://www.mdpi.com/2077-1312/8/10/776

[11] *International Safety Management Code*, IMO Publishing, London, U.K., 2018.

[12] (2024). *The Guidelines on Cyber Security Onboard Ships*. [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[13] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin, "Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre," in *Proc. 2nd Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2018, pp. 1–8.

[14] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo, "Training the maritime security operations centre teams," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2022, pp. 388–393.

[15] C. Boudehenn, O. Jacq, M. Lannuzel, J.-C. Cexus, and A. Boudraa, "Navigation anomaly detection: An added value for maritime cyber situational awareness," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2021, pp. 1–4.

[16] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020.

[17] G. Apruzzese, P. Laskov, E. M. de Oca, W. Mallouli, L. B. Rapa, A. V. Grammatopoulos, and F. D. Franco, "The role of machine learning in cybersecurity," *Digit. Threats, Res. Pract.*, vol. 4, no. 1, pp. 1–38, Mar. 2023, doi: 10.1145/3545574.

[18] (2024). *Guidelines on Maritime Cyber Risk Management*. [Online]. Available: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[19] M. V. C. Mesa, C. E. Patino-Rodriguez, and F. J. G. Carazas, "Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains," *Information*, vol. 15, no. 11, p. 710, Nov. 2024. [Online]. Available: https://www.mdpi.com/2078-2489/15/11/710

[20] M. Erbas, S. M. Khalil, and L. Tsiopoulos, "Systematic literature review of threat modeling and risk assessment in ship cybersecurity," *Ocean Eng.*, vol. 306, Aug. 2024, Art. no. 118059. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0029801824013970

[21] S. Symes, E. Blanco-Davis, T. Graham, J. Wang, and E. Shaw, "Cyberattacks on the maritime sector: A literature review," *J. Mar. Sci. Appl.*, vol. 23, no. 4, pp. 689–706, Dec. 2024, doi: 10.1007/S11804-024-00443-0.

[22] H. Yu, Q. Meng, Z. Fang, and J. Liu, "Literature review on maritime cybersecurity: State-of-the-art," *J. Navigat.*, vol. 76, nos. 4–5, pp. 453–466, Jul. 2023.

[23] M. Chaal, X. Ren, A. BahooToroody, S. Basnet, V. Bolbot, O. A. V. Banda, and P. V. Gelder, "Research on risk, safety, and reliability of autonomous ships: A bibliometric review," *Saf. Sci.*, vol. 167, Nov. 2023, Art. no. 106256. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753523001984

[24] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584908001390

[25] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *BMJ*, vol. 339, no. 1, p. b2535, Jul. 2009, doi: 10.1136/bmj.b2535.

[26] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *Int. J. Surg.*, vol. 88, 2021, Art. no. 105906. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1743919121000406

[27] G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam, "Multi-purpose cyber environment for maritime sector," in *Proc. 17th Int. Conf. Cyber Warfare Secur.*, vol. 17, Mar. 2022, pp. 349–357, doi: 10.34190/iccws.17.1.26.

[28] G. Visky, A. Šiganov, M. U. Rehman, R. Vaarandi, H. Bahşi, and L. Tsiopoulos, "Hybrid cybersecurity research and education environment for maritime sector," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Sep. 2024, pp. 644–651. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10679392

[29] A. Nganga, G. Nganya, M. Lützhöft, S. Mallam, and J. Scanlan, "Bridging the gap: Enhancing maritime vessel cyber resilience through security operation centers," *Sensors*, vol. 24, no. 1, p. 146, Dec. 2023. [Online]. Available: https://www.mdpi.com/1424-8220/24/1/146

[30] M. A. Hossain, M. D. Hossain, R. Choupani, and E. Doğdu, "MRS-PFIDS: Federated learning driven detection of network intrusions in maritime radar systems," *Int. J. Inf. Secur.*, vol. 24, no. 2, p. 92, Apr. 2025.

[31] M. S. Popli, R. P. Singh, N. K. Popli, and M. Mamun, "A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones," *IEEE Access*, vol. 13, pp. 12634–12646, 2025.

[32] K. Abbad, L. Khoukhi, L. Mesnil, A. Alliot, and I. Alliot, "Advanced anomaly detection for maritime IoT systems: Integrating semi-Markov processes for robust cybersecurity," in *Proc. Global Inf. Infrastructure Netw. Symp. (GIIS)*, Feb. 2025, pp. 1–6.

[33] M. A. Hossain, M. S. Hossain, M. D. Hossain, M. S. Islam, H. A. Mustafa, and M. M. Rahman, "Enhancing marine radar security through semi-supervised learning: A self-training approach," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICICT)*, Oct. 2024, pp. 279–283.

[34] D. Agnew, A. Rice-Bladykas, and J. Mcnair, "Detection of zero-day attacks in a software-defined LEO constellation network using enhanced network metric predictions," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 6611–6634, 2024.

[35] A. Algarni, T. Acarer, and Z. Ahmad, "An edge computing-based preventive framework with machine Learning- integration for anomaly detection and risk management in maritime wireless communications," *IEEE Access*, vol. 12, pp. 53646–53663, 2024.

[36] F. Basels, K. Wolsing, E. Padilla, and J. Bauer, "Demo: Maritime radar systems under attack. Help is on the way!" in *Proc. IEEE 49th Conf. Local Comput. Netw. (LCN)*, Oct. 2024, pp. 1–4.

[37] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and defending) the maritime radar system," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3575–3589, 2022.

[38] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, Jul. 2023, Art. no. 101426. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235271102300122X

[39] W. Liu, X. Xu, L. Wu, L. Qi, A. Jolfaei, W. Ding, and M. R. Khosravi, "Intrusion detection for maritime transportation systems with batch federated aggregation," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2503–2514, Feb. 2023.

[40] E. Gyamfi, J. A. Ansere, M. Kamal, M. Tariq, and A. Jurcut, "An adaptive network security system for IoT-enabled maritime transportation," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2538–2547, Feb. 2023.

[41] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, and J. Bauer, "Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring," *J. Mar. Sci. Eng.*, vol. 11, no. 5, p. 928, Apr. 2023. [Online]. Available: https://www.mdpi.com/2077-1312/11/5/928

[42] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2472–2481, Feb. 2023.

[43] A. Zainudin, R. N. Alief, M. A. P. Putra, R. Akter, D.-S. Kim, and J.-M. Lee, "Blockchain-based decentralized trust aggregation for federated cyber-attacks classification in SDN-enabled maritime transportation systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2023, pp. 182–187, doi: 10.1109/ICCWORKSHOPS57953.2023.10283507.

[44] F. Sicard, E. Hotellier, and J. Francq, "An industrial control system physical testbed for naval defense cybersecurity research," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Jun. 2022, pp. 413–422.

[45] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/3/104

[46] B. Qiu, M. Wei, W. Xi, Y. Li, and Q. Li, "CPS attack detection of ships using particle filter," in *Proc. China Autom. Congr. (CAC)*, Oct. 2021, pp. 4993–4998.

[47] D. Tiwari, B. S. Bhati, B. Nagpal, S. Sankhwar, and F. Al-Turjman, "An enhanced intelligent model: To protect marine IoT sensor environment using ensemble machine learning approach," *Ocean Eng.*, vol. 242, Dec. 2021, Art. no. 110180.

[48] C. Boudehenn, J.-C. Cexus, and A. A. Boudraa, "A data extraction method for anomaly detection in naval systems," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2020, pp. 1–4.

[49] N. Pelissero, P. M. Laso, and J. Puentes, "Naval cyber-physical anomaly propagation analysis based on a quality assessed graph," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2020, pp. 1–8.

[50] C. Iphar, A. Napoli, and C. Ray, "An expert-based method for the risk assessment of anomalous maritime transportation data," *Appl. Ocean Res.*, vol. 104, Nov. 2020, Art. no. 102337. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0141118720304314

[51] S. Yoginath, V. Tansakul, S. Chinthavali, C. Taylor, J. Hambrick, P. Irminger, and K. Perumalla, "On the effectiveness of recurrent neural networks for live modeling of cyber-physical systems," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 309–317.

[52] S. Schauer, E.-M. Kalogeraki, S. Papastergiou, and C. Douligeris, "Detecting sophisticated attacks in maritime environments using hybrid situational awareness," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manage. (ICT-DM)*, Dec. 2019, pp. 1–7.

[53] D. P. F. Möller, I. A. Jehle, J. Froese, A. Deutschmann, and T. Koch, "Securing maritime traffic management," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 453–458.

[54] I. Kontopoulos, G. Spiliopoulos, D. Zissis, K. Chatzikokolakis, and A. Artikis, "Countering real-time stream poisoning: An architecture for detecting vessel spoofing in streams of AIS data," in *Proc. IEEE 16th Intl. Conf. Dependable, Autonomic Secure Comput., 16th Intl. Conf. Pervasive Intell. Comput., 4th Intl. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 981–986.

[55] S. Jia, L. Ma, and S. Zhang, "Big data prototype practice for unmanned surface vehicle," in *Proc. 4th Int. Conf. Commun. Inf. Process.* New York, NY, USA: ACM, Nov. 2018, pp. 43–47, doi: 10.1145/3290420.3290466.

[56] B. Xing, Y. Jiang, Y. Liu, and S. Cao, "Risk data analysis based anomaly detection of ship information system," *Energies*, vol. 11, no. 12, p. 3403, Dec. 2018. [Online]. Available: https://www.mdpi.com/1996-1073/11/12/3403

[57] T. Becmeur, X. Boudvin, D. Brosset, G. Héno, B. Costé, Y. Kermarrec, and P. M. Laso, "Generating data sets as inputs of reference for cyber security issues and industrial control systems," in *Proc. 11th Int. Conf. Res. Challenges Inf. Sci. (RCIS)*, May 2017, pp. 453–454.

[58] J. N. Ptasinski, D. Wasserman, and R. Casey, "Protecting QoS in the ciphertext domain," in *Proc. MILCOM - IEEE Mil. Commun. Conf.*, Nov. 2013, pp. 1328–1333.

[59] 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. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Sep. 2022, pp. 114–122.

[60] A. Amro and V. Gkioulos, "Communication and cybersecurity testbed for autonomous passenger ship," in *Proc. Comput. Security. (ESORICS) Int. Workshops*, S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. M. Vidal, and M. A. S. Monge, Eds., Cham, Switzerland: Springer, Jan. 2022, pp. 5–22.

[61] G. Apruzzese, P. Laskov, and A. Tastemirova, "SoK: The impact of unlabelled data in cyberthreat detection," in *Proc. IEEE 7th Eur. Symp. Secur. Privacy (EuroS P)*, Los Alamitos, CA, USA, Jun. 2022, pp. 20–42, doi: 10.1109/EuroSP53844.2022.00010.

[62] A. Cropper, S. Dumančič, R. Evans, and S. H. Muggleton, "Inductive logic programming at 30," *Mach. Learn.*, vol. 111, no. 1, pp. 147–172, Jan. 2022, doi: 10.1007/s10994-021-06089-1.

[63] F. Khorrami, P. Krishnamurthy, and R. Karri, "Cybersecurity for control systems: A process-aware perspective," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 33, no. 5, pp. 75–83, Oct. 2016.

[64] G. Jakobson and M. Weissman, "Real-time telecommunication network management: Extending event correlation with temporal constraints," in *Proc. 4th Int. Symp. Integr. Netw. Manage. IV*, Jan. 1995, pp. 290–301.

[65] R. Vaarandi and S. Mäses, "How to build a SOC on a budget," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2022, pp. 171–177.

[66] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: A qualitative study of SOC analysts'perspectives on security alarms," in *Proc. 31st USENIX Secur. Symp. (USENIX Secur.)*, Boston, MA, USA, Aug. 2022, pp. 2783–2800. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

[67] T. V. Ede, H. Aghakhani, N. Spahn, R. Bortolameotti, M. Cova, A. Continella, M. V. Steen, A. Peter, C. Kruegel, and G. Vigna, "DEEPCASE: Semi-supervised contextual analysis of security events," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2022, pp. 522–539.

[68] R. Vaarandi and A. Guerra-Manzanares, "Network IDS alert classification with active learning techniques," *J. Inf. Secur. Appl.*, vol. 81, Mar. 2024, Art. no. 103687. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212623002715

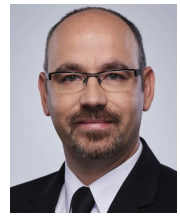
[69] E. Hotellier, N. Boukhobza, F. Sicard, J. Francq, and S. Mocanu, "Behavior-based intrusion detection approach deployed on a naval testbed," in *Proc. IEEE 29th Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 29, Sep. 2024, pp. 1–8.

[70] A. Saillard, K. Wolsing, K. Wehrle, and J. Bauer, "Exploring anomaly detection for marine radar systems," in *Proc. Comput. Security (ESORICS) Int. Workshops*, J. Garcia-Alfaro, K. Barker, G. Navarro-Arribas, C. Pérez-Solà, S. Delgado-Segura, S. Katsikas, F. Cuppens, C. Lambrinoudakis, N. Cuppens-Boulahia, M. Pawlicki, and M. Choraś, Eds., Cham, Switzerland: Springer, 2025, pp. 361–381.

[71] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Comput. & Secur.*, vol. 86, pp. 147–167, Jun. 2019.
[72] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2248–2294, 4th Quart., 2021.
[73] A. Tantawy, "On the elements of datasets for cyber physical systems security," 2022, *arXiv:2208.08255*.
[74] K. Gupta, S. Sahoo, R. Mohanty, B. Ketan Panigrahi, and F. Blaabjerg, "Distinguishing between cyber attacks and faults in power electronic systems—A noninvasive approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 2, pp. 1578–1588, Apr. 2023.
[75] G. Tertytchny, N. Nicolaou, and M. K. Michael, "Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103121. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014193312030288X
[76] Q. Wang, X. Cai, Y. Tang, and M. Ni, "Methods of cyber-attack identification for power systems based on bilateral cyber-physical information," *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106515. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061520318299
[77] V. Jüttner, M. Grimmer, and E. Buchmann, "ChatIDS: Explainable cybersecurity using generative AI," 2023, *arXiv:2306.14504*.
[78] A.-R. Morariu, T. Ahmad, B. Iancu, J. Poikonen, and J. Björkqvist, "Analysing MLOps and its applicability in the maritime domain through a systematic mapping study," in *Proc. IEEE 7th Int. Conf. Ind. Cyber-Physical Syst. (ICPS)*, May 2024, pp. 1–8.
[79] A. Vineetha Harish, K. Tam, and K. Jones, "Generating training events for building cyber-physical security skills," *Comput. J.*, vol. 12, p. 123, Dec. 2024, Art. no. bxae123, doi: 10.1093/comjnl/bxae123.

RISTO VAARANDI received the Ph.D. degree in computer engineering from Tallinn University of Technology, Estonia, in 2005. He is currently an Associate Professor with the Centre for Digital Forensics and Cyber Security, Tallinn University of Technology. From 1998 to 2018, he was affiliated with the SEB Financial Group and NATO CCDCOE. His research interests include machine learning for cyber security, event correlation, data mining for event logs, and network security.

LEONIDAS TSIOPOULOS received the Ph.D. degree in computer science from Åbo Akademi University, Finland, in 2010. He is currently a Senior Research Fellow with Tallinn University of Technology, Estonia. His research interests include the application of formal methods-based techniques to the development of critical systems and the application of such techniques for the development of enhanced cybersecurity solutions for the maritime domain.



GÁBOR VISKY received the M.Sc. degree in information engineering from the University of Miskolc, Hungary, in 2004. He is currently pursuing the Ph.D. degree with the Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Estonia, specializing in the cyber security of maritime operational technologies. With more than 15 years of experience in designing hardware and software for embedded control systems, he has also conducted extensive research into their vulnerabilities during his tenure at NATO CCDCOE.

MUAAN UR REHMAN (Graduate Student Member, IEEE) received the M.Sc. degree in software engineering from Wuhan University, China, in 2017. He is currently pursuing the Ph.D. degree with the Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Estonia. His research interests include cyber security for industrial control systems and machine learning for cyber security.

HAYRETDIN BAHŞI received the Ph.D. degree from Sabancı University, Türkiye, in 2010. He is currently a tenure-track Assistant Professor with the School of Informatics, Computing, and Cyber Systems, Northern Arizona University, USA; and a Research Professor with the Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Estonia. His research interests include applying machine learning to cybersecurity problems and cyber-physical system security.

Appendix 2

Publication II

G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam. Multi-purpose cyber environment for maritime sector. *Proceedings of the International Conference on Information Warfare and Security*, pages 349–357, Mar. 2022

Multi-Purpose Cyber Environment for Maritime Sector

Gabor Visky[1], Arturs Lavrenovs[1], Erwin Orye[1], Dan Heering[2], Kimberly Tam[3], Olaf M. Maennel[4]
[1]NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
[2]Estonian Maritime Academy, Tallinn University of Technology, Tallinn, Estonia
[3]University of Plymouth, Plymouth, UK
[4]Department of Computer Science, Tallinn University of Technology, Tallinn, Estonia

gabor.visky@ccdcoe.org
arturs.lavrenovs@ccdcoe.org
erwin.orye@ccdcoe.org
dan.heering@taltech.ee
kimberly.tam@plymouth.ac.uk

Abstract: The cyber attack surface in a maritime environment is constantly growing. More current information and computer technologies are being used on cargo and passenger ships to save on operational costs and increase navigational safety.

Along with the growing reliance on automation, the risk of a disruption to a vessel's critical systems by drawing on the wrong inputs from sensors to change the behaviour of the actuators has significantly increased.

Traditional operational technological systems are much more complicated to update than the automatic software updates we see in information technology systems. To better understand existing cyber threats in the maritime sector and increase cybersecurity resilience, this paper aims to replicate the digital components of a ship's bridge to examine scenarios when the bridge system loses connectivity, receives the wrong inputs from sensors, or the internal system becomes compromised.

The simulator differentiates fundamentally from traditional simulators or digital twins in the maritime sector that focus on training seafarers. This environment generates data streams that are similar to those on board a ship. Those data streams can be analysed, modified and spoofed to observe the effects. The effects can be technical but it is equally necessary to analyse how human beings would react in specific circumstances.

Our work provides the opportunity to isolate the ship network traffic, conduct penetration testing, find cybersecurity vulnerabilities on devices, and execute cyber attacks without the dangers associated with running such scenarios on a vessel in the open sea.

Keywords: maritime, cybersecurity, testbed

1. Introduction

Cyber threats and actual incidents in the maritime sector are constantly growing. Recent cyber incidents and accidents have highlighted how fragile the naval industry is, despite its importance in world trade. The industry depends increasingly on digitalisation, integration of systems, operations, and automation. The growing role of autonomous vehicles makes the problem more severe. The consequences of possible cyber attacks can include financial losses, safety issues, bad publicity, and compliance risks. The cases usually originate in technology, staffing, or cybersecurity operating procedures that lead to technology testing and education.

This paper proposes a multi-functional environment for cyber-related education and maritime-related cyber research that is flexible enough to adapt to specific needs. Although the proposed environment has enormous potential in education, this paper highlights the technical perspective and introduces the testbed functionality. The simulator aims not to provide sailing-related experience but focuses on the consequences of cyber attacks and how to react to those attacks. Furthermore, the environment offers a maritime-related climate for cyber experts to conduct experiments.

The environment has a network similar those found on vessels. The generated data streams traffic is used as a source for analysis and penetration testing. Using the simulator, we achieve similar results to those on actual vessels without violating the integrity of the expensive equipment on board a ship. Even though the proposed

environment has considerable potential for education, this paper highlights the technical perspective and introduces the testbed functionality.

The first section focuses on the current situation in the maritime sector and its challenges. In Section 2, we provide relevant background on cybersecurity in the maritime sector. Section 3 reviews related research addressing the available solutions that can be used as a training or research environment. In Section 4, we describe the setup of the multi-purpose cyber environment that was built on the premises of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, and discuss its similarities and differences compared to a real ship. Section 5 presents the conclusions and highlights the future directions.

2. Background

In recent times, the importance of cyber defence has been continuously increasing in the maritime sector, as in other industries. The following section provides an overview of the sector's specific characteristics.

2.1 Cybersecurity in the maritime sector

Nowadays, the importance of the shipping industry for modern society is constantly growing. The volumes of goods carried by ships in 2019 reached 11.08 billion tons (*Explaining shipping*, 2021). It is estimated that over 80% of world trade is carried by the shipping industry (United Nations, 2021). The need to reduce operational costs has led the shipping industry to seek new and advanced technological solutions. In 2017, the International Maritime Organization (IMO) initiated a scoping exercise to determine how the safety, security and environmental soundness of Maritime Autonomous Surface Ships (MASS) operations might be addressed using IMO instruments (International Maritime Organization, 2021). The development of technologies and policies that make autonomy a feasible solution has enabled several organisations to make progress on such projects and will soon sail their first autonomous ships (Tam and Jones, 2018).

Along with the growing reliance on automation, the risk of external interference and the disruption of critical systems is greatly increased; malicious actors can interfere with the different control systems of the ship. They can cut off all external communications or obtain confidential data. Cybersecurity on board ships is gaining in importance due to recent incidents on ships at sea (Caprolu *et al.*, 2020).

In June 2017, the world's largest container shipping company, A.P. Møller-Maersk was one of the companies hit by the malware NotPetya (WIRED, 2018). In July 2018, one of the biggest shipping companies, China Ocean Shipping Company (COSCO), was victim of a cyber attack (Goud, 2018). Norsk Hydro was hit by an extensive cyber attack in March 2019 (SAFETY4SEA, 2019). Although these incidents were ransomware related and the role of the operators was high, it has been successfully demonstrated by researchers that both information technology (IT) and operational technology (OT) systems used on board have vulnerabilities that can be exploited or exposed unintentionally by crew members (Bhatti and Humphreys, 2017), (Pen Test Partners, 2020).

Those unique circumstances demanded creating an environment for research and education in this field so that the maritime sector will become more resilient to cyber attacks.

2.2 Aspects of cybersecurity

Cybersecurity refers to the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. In Information Technology (IT) it focuses on the practice of ensuring the confidentiality, integrity and availability of information (CIA triad). It comprises an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorised access (Gourlay, 2000).

Cybersecurity has several aspects: application security, information or data security, network security, disaster recovery/business continuity planning, operational security, cloud security, critical infrastructure security, physical security, and end-user education. Technology, people, and regulatory frameworks are always essential to solving problems in cybersecurity, and this is no different in the maritime field. These three elements are fundamentally interconnected. At the same time, research can improve how these function from a cybersecurity perspective for the maritime sector.

According to (Fortress Information Security, 2020), the maritime-specific cybersecurity challenges span technology, staffing, and cybersecurity operating procedures. The main purpose of this work is to provide an environment that can be used to educate the crew, research technologies and test operating procedures.

2.3 Technology-related challenges

Maritime organisations have a vast array of legacy operational technology (OT) and information technology (IT) systems deployed. The majority of those systems were not designed with cybersecurity in mind. In addition, the different OT system configurations and architectures on the various ships make it challenging to secure the network infrastructure and their topologies aboard a vessel.

The situation is becoming more severe since autonomous or remotely operated off-shore vehicles will contain even more OT components, interconnected with navigational and other subsystems. Since the control system of the whole industry cannot change overnight, new ships have to maintain compatibility with obsolete systems, and since they have the heritage of old solutions requested by legacy standards, the applicability of the newest cybersecurity solutions will be limited.

Despite growing automation on ships, communication links use satellite-based solutions that provide only limited bandwidth. These circumstances limit remote assistance and maintenance in the case of a cybersecurity problem.

Appropriate technologies (e.g. antivirus, firewalls, intrusion detection/prevention systems, endpoint security and others) should be selected and implemented to provide comprehensive cybersecurity protection for these OT systems. Still, ship-system producers keep sailing safety in the primary position, often at the cost of cybersecurity. In most cases, it is hard to select the proper defence solution for several reasons.

The applied technology is barely standardised, the communication standards are vendor-specific, and furthermore, with an approximated 40-year life cycle, operators on ships cannot update CPS on the same frequency we are doing with generic IT systems where software vendors are constantly pushing their updates. Therefore, it is difficult to neutralise potential vulnerabilities in this field and this leads to weak system resilience. Currently, there is a lack of environments in which we can research and educate the maritime sector to test the different components individually or the whole system.

2.4 Education-related challenges

Ships, ports, terminals and offshore facilities are increasingly dependent on networked information and communication technology (ICT) (Heering *et al.*, 2020). Seafarers must be ready to cope with a growing number of cyber threats on board ships, with cybersecurity awareness playing an essential role in emergency and crisis management. Maritime education and training institutions (MET) offer high-level facilities for training seafarers, such as maritime simulators. These tools aim at learning and practising different operations like sailing, docking, and the use of onboard devices like RADAR, Electronic Chart Display and Information System (ECDIS), and others. Cybersecurity education is usually outside the scope of the curriculum, and the facilities do not support this task.

The authors argue that a certified ship bridge simulator can be used for teaching and practising responses to cyber-related incidents. Besides this fact, the lack of a proper testing environment is a severe barrier to improving cybersecurity awareness. The key to more cyber-safe operations at sea lies in the proper implementation of cybersecurity awareness training for active and future seafarers by taking into account their responsibilities onboard the ship and their background knowledge of IT. Training and awareness are key elements to effective cyber risk management on ships.

3. Related work

3.1 Testbeds

Determining the vulnerabilities of industrial control systems using embedded devices is a complicated process because of the complex hardware and software interactions. Lund et al. (Lund *et al.*, 2018) shed light on the great importance of the central components like Integrated Navigation Systems (INS) and ECDIS for the safety and security of maritime operations, but claims that the topic has barely been studied.

One approach is to build a comparatively simple system that captures the relevant complexity (i.e., a testbed) (Davis *et al.*, 2006). A testbed is an essential tool, avoiding the need to experiment exclusively on live systems. The topic is highly researched in the field software testing, primarily in the context of vulnerability identification. Salunkhe et al. have published (Salunkhe *et al.*, 2018) systematic literature review results regarding the cyber-physical testbeds focused on simulation. According to their findings, the literature focuses on electrical grids, network and communication, but not on maritime related topics.

Frank et al. introduce the design considerations for cybersecurity testbeds (Frank *et al.*, 2017) for education. The main requirements were automated deployability, reusability, low cost, high availability and scalability. The paper introduces the main challenges of the testbed setup and installation, but the cases focus on the vulnerabilities of web application, which is not relevant on a ship.

3.2 Maritime-related solutions

Brinkmann and Hahn offer a testbed architecture for maritime systems (Brinkmann and Hahn, 2017). Their work introduces the physical testbed 'LABSKAUS' (Laboratory for Safety Critical Analysis On Sea) as part of the eMaritime Reference Platform (eMIR), which is a CPS, and provides various maritime specific components, such as a reference waterway, research boat, sensor infrastructure and a mobile bridge. According to the paper the development of safety-critical systems such as a highly automated and autonomous vessel brings the need to establish a test environment (or 'testbed') close to the real world in addition to simulative test environments. This solution can support the development, validation and certification process. The highly sophisticated testbed uses a sensorbox that contains sensors and actuators which correlate with the environment; for example, a waterway network or a hydrodynamic environment. The complex system supports the solution of technical questions, but does not have educational features.

Modelling and simulation technologies are also extensively used in the maritime industry. A digital twin is a digital representation of a physical object, asset or system: a ship, a car, a wind turbine, a power grid, a pipeline, or a piece of equipment, such as a thruster or an engine (Smogeli, 2017). Although they enable early and continuous simulation-based testing, cutting the expenses of the system integration (Smogeli, 2017), this solution cannot be used to identify vulnerabilities, since the digital twin setup differs from the actual devices installed on ships. At the same time, a system based on a digital twin can be used for cybersecurity education.

Tam et al. presents a Cyber-SHIP Lab (Hardware, Software, Information and Protections) as a next-generation research capability for maritime cybersecurity (Tam *et al.*, 2019). This facility offers a complex research capability considering the physical aspects as well as the digital, with a lab that is accurate at the hardware level and not based on simulation or emulation. According to the plans, Cyber-SHIP would accommodate ship controller devices, so ship-identical systems could be installed at a considerably higher budget. Multiple configurations of the equipment can be created to imitate different ships. Although the setup proposed in our paper has the same objectives (supporting research and education), but our solution uses simulation-based data source that offers a more simple setup but still close to the real world.

Although the relevant literature is rich, only a few papers are available about a maritime-related environment for education, research and penetration testing. Their research offers help for industry, government, and academia to understand and mitigate cyber threats in the maritime sector.

4. Multi-purpose cyber environment

As was introduced in the previous chapter, the maritime industry faces challenges in cybersecurity. These issues are also growing instead of getting easier to solve. The following section presents the multi-purpose cyber environment, a tool that can be used to ease the pain related to those problems.

The solution can be used for several different purposes. Besides the demonstration and educational functions, it offers data source functionality and environment vulnerability testing.

4.1 System setup

The environment is based on a Transas NTPRO 5000 Navigational Simulator that was designed exclusively for educating crew. A simulator environment contains the visualisation part that is responsible for the audio and visual experience, with several TVs, as it can be seen on Figure 1.

All the environmental parameters that can influence the simulated ship, such as visibility, wind and weather conditions, current and tide, can be set on the instructor machine, just like marine traffic and the position of other ships, that defines the RADAR picture and NMEA-Messages from real world data (e.g. Automatic Identification System (AIS)).

Figure 1. Multi Purpose Cyber Environment

The seafarer, who operates the simulated ship can control it via its fundamental components – the wheel, buttons and telegraph – and can see the actual status of the vessel on the screen of the coning machine. All the parameters are calculated by the simulator server. The crew can use the MFD as on a real ship. Since the laboratory is used for demonstration purposes as well, an extra monitor is added on which the screen of the MFD can be seen. As Figure 2. shows, the original setup was extended using a Gateway Machine, Researcher's Computer, Data Collection Unit and additional MFD for research purposes.

In a simulator environment, the central components (i.e. MFD and ECDIS) are identical to the devices installed on ships, but the computers contain simulator-related software components as well. These software components (RADAR and MFD Server) generate a ship-like network traffic according to the simulated values; therefore, the network traffic of the sensors and RADARs exists only in these computers and are not available from outside of the device.

In contrast to a real ship, the sensors measure the different physical values that are converted into a digital format and transferred via NMEA-0183 protocol to the sensor integration unit – though given different names such as Data Distribution Unit, Data Acquisition Unit, Data Collection Unit (DCU), Sensor Concentration Unit and so on – that converts these values into an IP based data communication format, usually TCP. (In some cases, the sensors have direct serial connections to the workstations) Since the RADAR data (picture) is different from the sensor data, the RADAR is treated differently: it is connected directly to the INS. RADAR can have an independent network or it can use the same network but a different protocol, for example UDP.

The main purpose of this research was to create an environment, where the ship network traffic appears, and the control devices are exactly the same (without simulator-related software pieces) like on a vessel. This solution provides the opportunity to isolate the ship-network traffic, conduct penetration testing on devices, or simulate cyber attacks. To achieve this goal, a Gateway Machine is used to host the RADAR and MFD servers, emulate the ship's RADAR and the DCU from which the ship-related data is available. The simulator sends the simulated data to the Gateway Machine, and the MFD and RADAR application also connects to it and reads the sensor values and RADAR pictures.

Since the simulator offers a wide range of ship types, the solution provides configurable network traffic that is very close to the actual ship's network traffic.

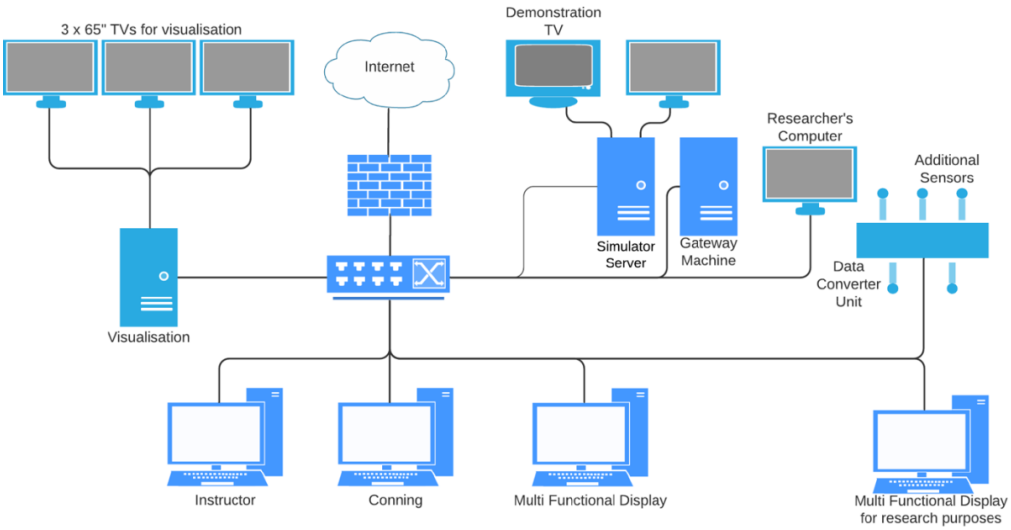


Figure 2. System setup.

4.2 Use cases

The multi-purpose cyber environment can be used mainly in the field of technology and education. This paper focuses on technology-related use cases that will be introduced in detail in this chapter.

4.2.1 Vulnerability testing environment

Nowadays, a ship can have several isolated networks for different purposes. The navigational network, the ship control network, the WiFi network used during loading and unloading the cargo, and the propulsion controlling network are all isolated networks (sometimes physically). The networks are logically interconnected by different crew members, who operate different devices based on data from different sources. As the level of integration between ships is increasing, these networks could no longer be separated. With less system isolation to protect systems, environments for simulating complex networks become more useful to the maritime sector.

The obsolete, twisted-pair and serial data transmission based on IEC 61162-1/NMEA-0183, and more recently the NMEA-2000 protocols are widely used on vessels. Since the devices that use these protocols must be integrated on modern ships, the legacy protocol was encapsulated into TCP/IP packets. Although this solution was simple, it brought a considerable amount of cyber-related problems into the picture. The modern ships using TCP/IP networks use legacy NMEA-0183 protocol packets encapsulated into TCP packets to transport their sensor data. The multi-functional environment can be used for generating this kind of network traffic, which can be analysed and reused in different ways.

The highly sophisticated switch offers Encapsulated Remote SPAN (ERSPAN) capability. As the name says, it delivers generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains. This feature together with the installed VNC clients enables full remote and network traffic analysis via a Virtual Private Network (VPN).

The Transas NTPRO-5000 – on which the environment is based – offers several different ships with its sensor and actuator sets for selection and the available sensor data generated according to the selected ship's sensor set. In the ship's network segment a research computer is installed for network traffic analysis, creation, and modification purposes. This solution offers an environment, where the ship-identical network data is available for the tested device, together with a modified or artificially generated one.

The environment also helps develop and test cyber defence solutions, such as antivirus, intrusion detection systems, and so on, since all the necessary devices are available for measurement and behaviour analysis in the setup.

4.2.2 Offensive cyber testing environment

There exist dozens of different types of cyber attacks, and defending against them is a tedious task with no single overall solution available. Since ships can be considered a system of systems, their defence, especially via the IT infrastructure and port management systems, is demanding. A ship's controlling device is an industrial control system (ICS). These are specialist information systems that differ significantly from traditional information systems used in the IT world (Drias *et al.*, 2015). Some attacks are not applicable against a ship; for example, phishing attacks, URL interpretation attacks, or web attacks.

In a ship, one primary defence against cyber attacks is air-gapping ship controls, navigation, and sensors from the rest of the IT systems, networks and the internet. Correctly implemented air-gapping creates a challenge for the attacker. If there is no possibility of a network connection, the remaining way to compromise the system is to deliver malware via a physical medium such as a thumbdrive, which is connected to and physically transferred between the air-gapped system and other ship or off-ship systems that are compromised and ready to deliver the malicious payload.

A scenario with an inside attacker significantly expands the attack surface on the air-gapped system. An insider might purposefully craft and deliver malware via physical media, or even do it off-ship or instruct somebody else to deliver it. An insider might break the air-gapping by physically connecting to another ship network that can have deployed malware on other connected computers making it less noticeable. Air-gapping could be broken permanently, temporarily (e.g., to deliver malware), or intermittently – installing a communication device that could receive commands from and send data to an off-ship location. In the simplest case, it could be a mobile router or modem with a mobile data roaming plan that works across the globe and can communicate in ports or near the shore, or any of the vast variety of point-to-point communication devices enabling communication in more fixed locations or between moving ones (e.g., from another ship).

In the simplest case, these communication devices can be connected directly to one of the computers in the air-gapped network and be used by already functioning malware. In this case, the communication device only provides a communication channel for the malware, the computer provides power and the network stack. The malware injects network packets or manipulates the system's inputs or outputs. This type of deployment is the most visible at the system level – it might be visually displayed, visible in the systems network configuration and the malware might also be detected by defences on the infected system.

Other cases can combine a communication device with a networking device that can inject (e.g., VPN router providing OSI Layer 2 access to an attacker) or modify (e.g., transparent firewall or similar device on the line) packets in the air-gapped network. These deployments can function without deployed malware, and therefore can be harder to detect but also can have less functionality. The most obvious scenario is establishing a foothold and communication channel inside the network of the systems, usually a switched Ethernet network.

Individual systems have their own set of controls and sensors that are directly connected to the system via a shared communication bus or point-to-point connections, which is commonly aggregated by a controller. Most of the controls or sensors can be replaced by compromised ones or a network intermediary device on the line that injects or modifies the data stream. The best point for the injection of a physical malicious control channel (or pre-programmed device or software) is the control board which allows the data stream of multiple inputs or outputs to be modified at the same time.

Without purposeful inspection, malware injected physical devices or breaches of air-gapping are hard to find as usually nobody is looking for those as long as everything functions properly. Therefore, the attacker can be dormant for months or years waiting for a specific moment or an opportunity to achieve an objective – disable the ship to get it stranded or take over control to crash it into another ship, the shore or a port.

The controller component (processor unit), such as ECDIS or MFD or a sensor, uses the multi-purpose cyber environment to test against cyber attacks. All the described potential attacks can be classified as either network (packet injection, modification, replay) or system (malware). This allows us to simulate and research all the possible outsider and even more diverse insider attacks.

4.2.3 Maritime-related experiences

The widely used legacy NMEA-0183 industrial protocol does not have sophisticated error correction, nor encryption; therefore, TCP packets containing NMEA-0183 messages can be faked or injected easily. A possible attack scenario could be a malware attack, where the malware is installed and sends TCP packets with valid

sensor data. This kind of infection can be carried out in the supply chain or during software or chart updates on the ship.

Despite the fact that the periodicity of the sensor data is predictable, it is not checked in the ship's controller devices, so the displayed value can be overwritten if new -incorrect- data arrives right after the correct value. There are no resources describing how to detect abnormal behaviour in the messages with the valid payload. A possible solution could be an extension of an intrusion detection system that analyses and checks the data itself. This solution could also compare different sensor's data like speed data from speed sensor and location data from the GPS.

5. Summary and future works

The multi-purpose cyber environment introduced here aims to provide both education and research in cybersecurity issues for a specific vessel. Although this paper introduced only the technical and research perspective of the environment, education-related usage is the subject of a follow-up paper.

The solution increases cybersecurity research capabilities to include maritime cybersecurity, particularly for analysing systems, hardware and software components, protection development, and testing existing procedures.

Further development is needed to separate the ship-related and the simulator-related network traffic in order to create a more realistic environment.

6. References

Bhatti, J. and Humphreys, T. E. (2017) Hostile Control of Ships via False GPS Signals: Demonstration and Detection, *NAVIGATION*, 64(1), pp. 51–66.

Brinkmann, M. and Hahn, A. (2017) Testbed architecture for maritime cyber physical systems, in *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*, Emden: IEEE, pp. 923–928.

Caprolu, M. *et al.* (2020) Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, *IEEE Communications Magazine*, 58(6), pp. 90–96.

Davis, C. M. *et al.* (2006) SCADA Cyber Security Testbed Development, in *2006 38th North American Power Symposium*. *2006 38th North American Power Symposium*, Carbondale, IL, USA: IEEE, pp. 483–488.

Drias, Z., Serhrouchni, A. and Vogel, O. (2015) Analysis of cyber security for industrial control systems, in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. *2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC)*, Shanghai, China: IEEE, pp. 1–8.

Explaining shipping (2021). URL https://www.ics-shipping.org/explaining/ (accessed 6.25.2021).

Fortress Information Security (2020) *White Paper: Building A Sustainable Maritime OT Cyber Security Program*. URL https://fortressinfosec.com/building-a-sustainable-maritime-ot-cyber-security-program/ (accessed 5.22.2021).

Frank, M., Leitner, M. and Pahi, T. (2017) Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education, in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Orlando, FL: IEEE, pp. 38–46.

Goud, N. (2018) *Cyber Attack on COSCO*, *Cybersecurity Insiders*. URL https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/ (accessed 5.17.2021).

Gourlay, L. (2000) *Chambers guide to English for I.T. and the internet*. Edinburgh: Chambers.

Heering, D., Maennel, O. and Vanables, A. (2020) Shortcomings in cybersecurity education for seafarers. Preprint.

International Maritime Organization (2021) *Autonomous ships: regulatory scoping exercise completed*. URL https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx (accessed 6.25.2021).

Lund, M. S. *et al.* (2018) Integrity of Integrated Navigation Systems, in *2018 IEEE Conference on Communications and Network Security (CNS)*. *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China: IEEE, pp. 1–5.

Pen Test Partners (2020) *Speed 2 – The Poseidon Adventure – Part One*. URL https://www.pentestpartners.com/security-blog/speed-2-the-poseidon-adventure-when-cruise-ships-attack-part-1/ (accessed 7.19.2021).

SAFETY4SEA (2019) Norsk Hydro lost about $35-40 million after cyber attack, *SAFETY4SEA*, 1 April. URL https://safety4sea.com/norsk-hydro-lost-about-35-40-million-after-cyber-attack/ (accessed 5.17.2021).

Salunkhe, O. *et al.* (2018) Cyber-Physical Production Testbed: Literature Review and Concept Development, *Procedia Manufacturing*, 25, pp. 2–9.

Smogeli, Ø. (2017) Digital Twins at Work in Maritime and Energy.

Smogeli, Ø. (2017) FEATURE FEBRUARY 2017, p. 7.

Tam, K., Forshaw, K. and Jones, K. (2019) Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities, in *Conference Proceedings of ICMET Oman*. *International Conference on Marine Engineering and Technology Oman*, Muscat, Oman: IMarEST.

Tam, K. and Jones, K. (2018) Cyber-Risk Assessment for Autonomous Ships, in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow: IEEE, pp. 1–8.

United Nations (2021) *Review of Maritime Transport 2020.* S.l.: United Nations.

WIRED (2018) *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. URL https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 6.25.2021).

Appendix 3

Publication III
G. Visky, S. Katsikas, and O. Maennel. Lightweight Testbed for IEC61162-450-Related Cyber Security Research. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 638–643, 2024

2024 IEEE International Conference on Cyber Security and Resilience (CSR)

Lightweight Testbed for IEC61162-450-Related Cyber Security Research

Gabor Visky
Department of Computer Science
Tallinn University of Technology
Tallinn, Estonia

Sokratis Katsikas
Department of Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

Olaf Maennel
School of Computer & Mathematical Sciences, University of Adelaide, Adelaide, Australia

2024 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-7536-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSR61664.2024.10679439

***Abstract*—The world is shifting towards increased digitalisation, severely impacting critical infrastructure like maritime transportation. Electronic navigation equipment—such as echo sounders, sonars, anemometers, gyrocompasses, autopilot systems, GPS receivers, and many other instruments—used on modern ships have undoubtedly decreased naval accidents over the years. Still, these devices may suffer from cyber security vulnerabilities because system developers and vendors often do not consider cyber security aspects. This paper presents a lightweight research environment, focusing on the IEC61162-450 protocol and able to simulate cyber attacks against an Electronic Chart Display and Information System (ECDIS) included in a Multi-Functional Display (MFD). This environment is a vital tool for marine cyber security experts wishing to engage with research addressing existing and potential cyber security vulnerabilities in electronic navigation equipment.**

***Index Terms*—cyber security, IEC61162-450, maritime, testbed**

I. Introduction

Cyber security threats in the maritime industry are rising fast; the sector witnessed a 400% increase in attempted attacks between February and June 2020 [1]. Gartner forecasts that cybercriminals will progressively weaponise industrial control systems (ICSs) this decade to potentially cause harm to life and the environment [2]. Adding to this challenge, ICS vulnerabilities saw an increase of 27% in 2022, while 77% of vulnerabilities lack any mitigation [3]. Electronic navigation equipment on modern ships has undoubtedly increased maritime safety over the years [4], but they may be susceptible to cyber vulnerabilities. [5], [6] Meland et al. introduces 46 maritime-related cyber incidents [7]. This forecast worsens since the required data and navigational networks are getting more complex to support the growing maritime automation capability, becoming a critical maritime component [8].

According to Katsikas, cyber security is a critical issue for ships because of their increased dependence on information and communication technologies (ICT) for ship control, their advanced integration of control systems, their increased connectivity with shore control centres, and their accessibility to and from the Internet [9].

To minimise the attack surface of the control systems, the security of network services and devices is essential because a flaw in the implementation can make a controlling system vulnerable. To help developers with this task and ensure interoperability, a rigorous standardisation process is in place, which should also include security.

Despite all the efforts, a standardised protocol might remain vulnerable to cyber attacks, and implementation flaws might weaken the software. To tackle these challenges, experts need safe and secure research environments and testbeds, to develop and test their solutions.

The IEC61162-450 is a standardised protocol, which is widely accepted by manufacturers and maritime agencies worldwide and used in navigation systems composed of Electronic Chart Display and Information System (ECDIS), Integrated Navigational Systems (INS) and Data Collector Units (DCU) [10], [11].

The IEC61162-460 standard extends the IEC61162-450 by providing requirements and test methods for equipment to be used in environments where higher safety and security standards are needed since there is a risk of exposure to external threats. It does not introduce new application-level protocol requirements since those are defined in IEC61162-450; it focuses on the safety and security of the Ethernet interconnection [12].

This paper's main contribution is to introduce a testbed to support cyber security research, focusing on the above-mentioned protocol. Additionally, we overview the IEC61162-450 protocol and we introduce attacks to demonstrate the workings and usefulness of our testbed. In this environment, we exploited the protocol's—which has undergone a rigorous standardisation process—severe vulnerabilities, which extend the attack surface of ECDIS.

The remaining of the paper is structured as follows. Section II presents the background necessary to make the paper self-sustainable, as well as the related work. Section III introduces the testbed, while Section IV confirms that it satisfies the requirements set out for such testbeds in the literature. Section V describes the attacks executed on the testbed and Section VI presents and discusses the results we obtained. Finally, Section VII summarizes our conclusions and offers suggestions for future research.

II. Background and Related Work

This section provides a comprehensive overview of the onboard communication protocols under study and a discussion of the related work.

A. Onboard Communication Protocols

ICSs control and monitor industrial processes such as logistics, manufacturing, and transportation. Real-time response, high availability and reliability are the key features of these systems. Different industries often have unique, sector-specific protocols to fulfil these requirements.

In the maritime domain, NMEA (National Marine Electronics Association) is a worldwide organization that, among other activities, issues marine electronics interface standards, to enhance the technology and safety of such equipment. One of these standards that supports digital onboard communication is the NMEA-0183 standard, that later evloved into the IEC61162 standard. These are described in the next subsections.

1) NMEA-0183: In the early 80s, the NMEA issued the NMEA-0183 standard, which defines the interfacing between various marine electronic equipment and navigational computers, allowing them to share vital information [13]. NMEA-0183 evolved from earlier NMEA standards (-0180 and -0182) and is based on the serial communication protocol standard "RS422" (Standard EIA-422-A). This underlying protocol supports data exchange between one talker and up to 10 listeners. The data exchange used 7-bit ASCII-encoded *sentences*, up to 82 characters long [14].

2) IEC61162-1 Protocol: In 1997, NMEA-0183 v.1.5 was translated into the international industrial standard IEC61162-1 [15].

The most commonly used communication protocols in navigation follow the IEC61162 standard, a collection of International Electrotechnical Commission (IEC) standards for "digital interfaces for navigational equipment within a ship". Several standard versions were published during the IEC61162's long evolution. While the IEC61162-1 protocol is designed to work over serial lines, its gradual development led to the IEC61162-450 protocol that works over Ethernet. This paper focuses on this protocol, whose detailed description is given below.

3) IEC61162-450 Protocol: Over the years, the number of onboard sensors increased, along with the complexity of the ship control systems. Along with it, Ethernet networks with Internet Protocols (IPs) became predominant. As Rødseth and Christensen wrote in [8] in 2007, Swedish experts proposed an Ethernet-based interface standard for maritime navigation and radio communication equipment and systems. This proposal was accepted in March 2008 by Working Group 6 (Digital interfaces) of Technical Committee 80 of the IEC. The standard has been published as IEC61162-450 [10]. Although the new protocol offers more flexible services, the data format still follows the first version, in which the sensor data is transferred in IEC61162-1 sentence format. This new protocol, referred to as "Light-Weight Ethernet" (LWE), has been developed to be used in instrument or process layer networks since it has moderated complexity to be implementable on devices with limited resources such as embedded computers, radios, and AIS receivers.

The LWE protocol is based on the standard User Datagram Protocol (UDP), in which the talker sends multi-cast packets that propagate over the ship's network. The IEC61162-450 supports four general communication patterns for data transmission: Multi-Sentence Message (MSM), Binary Image Transfer (BIT), Command-Response Pair (CRP) and Sensor Broadcast Message (SBM). Current research focuses on the latter. According to [16], the SBM is a standard UDP packet that allows transmitting the IEC61162-1 sentences in a network environment from multiple talkers to multiple listeners. The payload of the UDP packet contains a six- byte-long static header (UdPbC'0') and one or more TAG (Transport, Annotate, and Group) blocks, followed by the original data (IEC61162-1 sentence). The general structure of the TAG block is explained below and depicted in Table I.

Table I
IEC61162-450 PACKET STRUCTURE.

Byte Offset	Function	Example value
00	IEC61162-450 Header	UdPbC'0'
06	Delimiter	\
07	Parameter code	s
08	Parameter code delimiter	:
09	System function indicator	SI0011
15	Parameter field delimiter	,
16	Parameter code	n
17	Parameter code delimiter	:
18	the Parameter value	683
21	Checksum delimiter	*
22	Checksum value	16
23	Delimiter	\
24	IEC61162-1 data	$TIROT,123.45*hh

For example, consider an SMB message with the following payload: UdPbC'0'\s:SI0011,n:683*16\$SIHBT,01,A,44*28

In this example, "UdPbC" followed by a null character is the datagram header that indicates the transmitted data type, and in this case it is an IEC61162-1 formatted sentence.

The first TAG block transfers the system function ID (SFI). In this case the "s" parameter code is for talkers and the parameter value contains the SFI—in this example "SI0011"—which is the default SFI value.

The next TAG block with the "n" parameter code is assigned a sequence number to each sentence transmitted from each SFI, the parameter value in this example is 683.

After the checksum delimiter and checksum the transferred data comes; in this example an IEC 61162-1 formatted sentence: "$SIHBT, 01,A,44*28".

Before the DCU starts converting and sending the data from the sensors in IEC61162-1 format, the MFD software starts, and an initialisation procedure occurs. However, in our paper we cannot disclose the initialisation part of the communication to respect the manufacturer's copyright restrictions. First, the MFD software sends a ping request towards the DCU. If the

DCU answers the request, the MFD establishes a Transmission Control Protocol (TCP) communication socket with the DCU using Transport Layer Security (TLSv1). In the encrypted data exchange, 160 bytes are sent from the MFD to the DCU, then the connection is closed, and the UDP broadcast stream starts flowing from the DCU.

B. Related Work

We conducted a comprehensive literature survey in several digital libraries to get an overview of publications related to cyber security, testbed, and maritime together. The rich literature introduces several testbeds that can support cyber security-related research in the field.

Conti et al. published a comprehensive review on testbeds and cyber ranges [17]. Their work introduces the ICSs' architecture, their components, the most common protocols, and attacks against them. Although the publication includes an enormous number of testbeds, none of them deals with marine-related systems.

Sicard et al. in [18] presented a cyber security testbed for the naval defence sector involving ICS components focusing on four main systems: direction, energy, artillery and propulsion. The introduced testbed involves different Programmable Logic Devices (PLCs), Human Machine Interfaces (HMIs), physical simulated actuators and sensors, and attack generator computers. Unlike our work, this one does not deal with navigational devices.

The publication of Puys et al. suffers from the same shortages. Their Hardware-In-The-Loop Labs can serve cybersecurity awareness training and research on SCADA (Supervisory control and data acquisition) systems [19].

Tam et al. share the proposal for a complex research environment for maritime cyber research called Cyber-SHIP platform involving real maritime equipment not only for testing but also for data generation. The excellent environment can support the penetration testing of such devices, but this solution needs serious financial resources to implement [20].

Kavallieratos et al. review the cyber-physical testbeds which potentially can support cyber security research [21]. Their work compartmentalises the testbeds as physical, virtual and hybrid ones and shares the different functionalities like vulnerability analysis, training, defensive mechanism, assessment of cyber attacks impact and threat analysis. It highlights the requirements for a cyber-physical range, that we adopt in this paper. Our testbed follows the Cyber-Enabled Ships' Testbed in a simplified way: our work includes only the sensor simulator, the network and the visualisation device, together with the research computer.

Our literature survey shows a need for a lightweight research environment that can be used for cyber security research or testing of ECDIS or other navigational devices.

III. Our testbed

Our testbed, which aims at facilitating research on the cyber security of the IEC61162-450 protocol, contains sensor simulator software, data converters to convert the simulated values into IEC61162-1 and IEC61162-450 format, an MFD to visualise the data, and a researcher's computer to process the network traffic and to investigate different attacks.

The logical schema of the research environment can be seen in Figure 1.

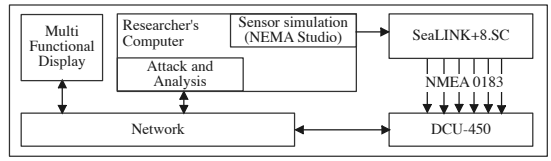


Figure 1. Research environment.

A. Sensor data simulation

The data is generated by the NEMA Studio [22] software which can simultaneously simulate several different physical sensors, such as wind speed and direction, velocity, etc. and data sources, like AIS and GPS receiver, and encapsulate them into IEC61162-1 sentences. Instead of the commercial solution, the open-source NMEASimulator [23] also can be used. The data generator software runs on the researcher's computer.

B. USB to serial interface

The sentences are sent over USB to an eight-port USB/serial converter [24]. Individual serial ports were used for each simulated sensor to make the research environment realistic. This device supports the RS422 standard as the underlying protocol, according to IEC61162-1.

C. Serial to Ethernet Interface

The serial ports are connected to a DCU450, which has 16 bidirectional ports (supporting IEC61162-1 format) and acts like a bridge between the legacy and the new communication protocol: it generates the IEC61162-450 data stream from the data arriving on the different serial ports of the DCU. This data stream is sent further to the MFD computer.

D. MFD computer

The MFD is an integrated electronic display system that consolidates various navigational and operational information into a single or multiple screens. It provides comprehensive, real-time data about navigation, engine, weather, and other operational values. In our setup the MFD computer runs a Navi-Sailor 4000 MFD software, that contains the ECDIS and RADAR subcomponents. Our research environment embed this software, however it can accomodate other solution that uses the IEC61162-450 communication protocol [25].

E. Network device

In this research environment only a TP-Link TL-SG108E 8-Port Gigabit Easy Smart Switch is installed, providing the network connectivity between the devices. The switch mirrors all the network traffic to the researcher's computer, to provide the data for network traffic analysis.

F. Researcher's computer

This computer is used to accomodate the different software packages for sensor value generation. Since the network traffic between the DCU450 and the MFD is mirrored to this computer, it can be used for network flow analysis. Additionally, the computer can accomodate software for vulnerability analysis over different attacks.

G. Software components

The researcher's computer can accommodate different software; we used the following ones in our testbed:

1) Wireshark: is a commonly used network traffic and protocol analyser software [26].

2) TCPReplay: is a suite of free Open Source utilities for editing and replaying previously captured network traffic [27].

3) Self-developed software: We developed software in Python to replay previously recorded UDP streams and generate fake sensor values to be injected into the network traffic. One can develop and run any software that the infrastructure can accommodate.

IV. Satisfying relevant requirements

Kavallieratos et al. in [21] define the requirements for a cyber-physical range that we have adopted. Although our testbed is simple, it is *flexible*, since the researcher's computer can accommodate a wide range of simulators and penetration testing software. The same feature applies to the MFD computer. The only seeming bottleneck is the chain of protocol converters since the testbed converts the NMEA sentences into NMEA-450 format. This shortage can be handled easily, as the researcher's and MFD computers are in the same network, therefore any ethernet-based protocol can be used, according to the needs.

Regarding the *Scalability* and *adoptability* requirements, our testbed can easily accommodate devices and services, according to the specific objectives. However, the computers used limit the processing power and other available resources for the individual components. Because of the simple setup, it is limited in number of users, leading to low *shareability*; it offers a workspace for only one person at each time. On the other hand, the simple setup allows experienced users to *easily access* and use the system with reasonable training.

The testbed can work without any external connections, providing a *fully isolated* environment. At the same time, it does not provide external interconnection capabilities, limiting its *interoperability*.

Because of the simple structure, our solution is extremely *cost effective*. In particular cases, it can be built using only open-source software.

Therefore, our analysis shows that the testbed meets most of the requirements introduced in [21].

V. Executed Attacks

The CIA-triad (confidentiality, integrity and availability) has been a conceptual model of computer security for several decades [28].

To test our research environment, we conducted attacks against the Navi-Sailor 4000 ECDIS by exploiting the communication protocol's weaknesses. These attacks are not new, since this research focuses on the testbed, not on the attacks.

The introduction of the foothold establishment on a real ship is out of the focus of this paper; however, malicious software or a secretly installed attacker device can generate malicious traffic.

As detailed below, the MFD cannot resist malicious activities. To prove this, we conducted the following attacks against the navigation system: replay, injection, modification, and eavesdropping; these undermine the CIA-triad of the system.

A. Replay Attack

This attack is based on retransmitting previously recorded packet or sensor data. For this attack, the relevant packets were filtered out from the network traffic and replayed with our own-developed scripts. Since the IEC61162-450 relies on UDP, our attack was successful, and the ECDIS displayed the replayed information.

B. Injection Attack

In the case of false data injection, the malicious actor injects crafted packet to falsify operational values. During our experiments, the following *sensor values*: wind speed and direction, water depth, heading and turning were injected. Artificially generated packets were sent to the MFD, which could not detect the attack. There is no warning or other indication of improper behaviour or false value representation.

C. Modification

In the case of a modification attack, the transferred data is caught by the malicious actor, and after it has been modified, it is sent to the receiver. To analyse this attack, an Address Resolution Protocol (ARP)-based Man-In-The-Middle (MITM) attack was executed to pipe the communication over the researcher's computer. During our experiment, the packets with the relevant sensor data were captured from the original message, they weremodified and then resent. We modified ships' positions in the simulated AIS packets. The UDP headers needed to be changed to accommodate any manipulation of the payload length. The sensor data modification attack was successful.

D. Eavesdropping

The IEC61162-450 protocol transfers the sentences in cleartext format, without encryption. Since it broadcasts UDP packets, all sentences are delivered to every host in the subnet, making eavesdropping trivial. We were able to collect sensor data with our setup.

VI. Results

In our testbed, a particular ECDIS device was used, meaning that other vendors' products might not be vulnerable to the attacks we executed. Despite this fact, the challenged IEC61162-450 protocol enabled the abovementioned attacks against the communication between the DCU and the MFD.

According to Kim et al. the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) methodology is suitable for distributed control systems' threat modeling [29], [30]. Here we introduce the attacks' results with respect to the relevant aspects of the STRIDE methodology.

A. Spoofing

During the injection attack, the MFD showed the artificially generated data from the packets regardless of the sensor value. The fake data is displayed even if it came from a different input channel or different IP. The replay attack——in which the pre-recorded sensor values or network traffic were used——was also successful.

To calculate the optimal attack rate a Monte Carlo-like simulation was executed [31]. The simulated sensor transmitted messages at a rate of 10 times per second, while the display refresh time was set to 1 second. We executed attacks at varying rates, starting from 1 attack per second and incrementally increasing to rates such as 1.1, 1.2, 1.5, then 2, 2.1, 2.2, 2,5 attacks per second, and continuing up to 20 attacks per second. This progression is illustrated in Figure 2. During the simulation, we measured the probability of fake values being displayed.

According to the results, the pre-recorded or artificially generated packets' transmission frequency influenced the success rate of suppressing the attacked sensor values. the probability of a successful attack increased significantly when the malicious packets were sent slightly more often than the original sensor value (blue, red, and orange lines) or its harmonics (10.x, 20.x, 30.x). In our case, the original sensor sent ten samples a second, and it was suppressed with $p>0.8$ probability if the fake values were sent 10.1, 10.5 times in a second. We also experienced high probabilities with higher attack ratios, but they didn't reach the same result.

When the attack was executed at multiple rates of the original sensor data, such as once, twice, or three times a second, the success rate was higher when the attack frequency was higher than the double of the original data's frequency.

It is important to mention that the probability heavily depends on the timing because of the interference of the attack and sample rate.

B. Tampering

Since the analysed protocol supports only limited cyber security measures, the involved navigation and control systems are exposed to cyber attacks in which the attacker modifies the actual data or fabricates fake messages. A successful attack can lead to the navigation or control system's denial of service, which can have severe consequences on a ship. The IEC61162-450 protocol is defenceless against replay or spoofing attacks. Since the integrity of the systems cannot be guaranteed, an attack can cause fake sensor values to be visualised; this might be considered as a type of denial of service, because the crew cannot see the actual operational values. This can have serious consequences, for example a ship can run aground because of falsified depth data.

The modified sensor values——regardless of the attack type——can harm the automated navigation systems, like track and course control systems, that can lead to severe consequences like grounding, collision, etc. The modified control values can cause financial losses, for example, increased delivery time, increased fuel consumption; environmental damage e.g., oil spill in the case of accidents; or safety issues like loss of stability because of incorrect ballast management.

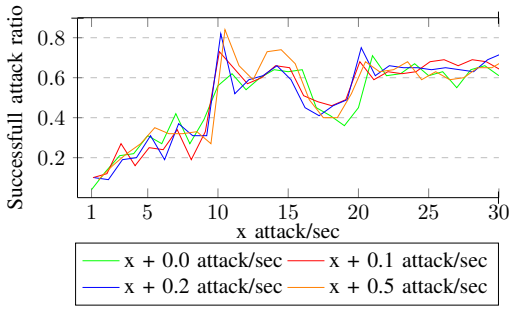


Figure 2. Probability of successfull injection attack.

C. Repudiation

The analysed protocol does not support nonrepudiation.

D. Information Disclosure

The eavesdropping was successful against the protocol, meaning that it does not support privacy-related security goals.

E. Denial of Service (DOS)

Although this paper focuses on an application layer protocol, it is worth mentioning that the IEC61162-450 protocol relies on the UDP protocol, which is a connectionless protocol i.e, it does not require an acknowledgement during communication. This protocol characteristic makes it vulnerable to attacks that overwhelm the connections with large volumes of malicious traffic (UDP flood attack) that can lead to denial of service [32]. Since the protocol is connectionless, it does not guarantee the source nor the reliable delivery of datagrams [33].

These preconditions make onboard communication unreliable. The sensors or data aggregators cannot check if their data arrived at the control device, and there is no way to check the validity and reliability of data. This means that data are interpreted for use by the ship operator or navigational system without any content control. In our research, the MFD is flooded by packets containing modified sensor values that cause DoS because of the above reasons.

F. Elevation of Privilege

The privilege elevation pertains to the processes on the end systems; this was out of the scope of the current research.

VII. Conclusion and Further Work

In this paper we highlighted the importance of cyber security research in the maritime sector and identified the need for a testbed that can be used for this purpose.

The lightweight solution we propose provides a safe and secure environment for cybersecurity research and device testing focusing on IEC61162-450-related works; however, other protocols can also be tested. We demonstrated its value by successfully executing cyber attacks that exploited the weaknesses of the protocol and of the ECDIS. This process revealed the vulnerabilities of the protocol.

The main contribution os our work is the easily replicable environment that can support researchers, opening up a world of possibilities for further research. The executed attacks and revealed vulnerabilities shed light on the fragility of the maritime sector from a cyber security perspective.

Our results provide a good environment and background for further research. Protocol, device, and application-related vulnerabilities can be researched to enhance the sector's cyber security preparedness.

Acknowledgement

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

References

[1] W. Loomis, *Raising the colors: signaling for cooperation on maritime cybersecurity*. Washington, DC: Atlantic Council, 2021.

[2] M. Susan, "Cyber-Physical Systems Must be Part of Your Security Strategy," 2021. [Online]. Available: https://www.gartner.com/smarterwithgartner/develop-a-security-strategy-for-cyber-physical-systems

[3] Dragos, "Ics/iot cybersecurity, year in review 2022," in *Annual review 2022*. Dragos Inc., 2023.

[4] S.-B. Hong, "A study on the effects of e-navigation on reducing vessel accidents," 2015.

[5] B. Svilicic, 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, 2019. [Online]. Available: https://www.mdpi.com/2077-1312/7/10/364

[6] M. S. Lund, J. E. Gulland, O. S. Hareide, ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. Beijing, China: IEEE, 2018, pp. 1–5.

[7] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, no. 3, pp. 519–530, 2021. [Online]. Available: https://doi.org/10.12716/1001.15.03.04

[8] M. J. C. Ørnulf Jan RØDSETH, "Design challenges and decisions for a new ship data network," 2011.

[9] S. K. Katsikas, "Cyber security of the autonomous ship," *CPSS 2017 - Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, co-located with ASIA CCS 2017*, pp. 55–56, 2017.

[10] I. E. Commission, "Maritime navigation and radiocommunication equipment and systems – digital interfaces – part 450: Multiple talkers and multiple listeners – ethernet interconnection," in *International Standard - IEC61162-450*. Geneva, Switzerland: International Electrotechnical Commission, 2018.

[11] K. Tran, S. Keene, E. Fretheim, and M. Tsikerdekis, "Marine network protocols and security risks," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 239–251, 2021. [Online]. Available: https://www.mdpi.com/2624-800X/1/2/13

[12] I. E. Commission, "Maritime navigation and radiocommunication equipmentand systems – digital interfaces – part 460: Multiple talkers and multiple listeners – ethernet interconnection – safety and security," in *International Standard - IEC61162-460*. Geneva, Switzerland: International Electrotechnical Commission, 2020.

[13] R. Langley, "Nmea 0183: A gps receiver," *GPS world*, vol. 6, no. 7, pp. 54–57, 1995.

[14] N. M. E. Association, "Nmea 0183," National Marine Electronics Association, Standard, 1987.

[15] I. E. Commission, "Iec 61162-1 maritime navigation and radiocommunication equipment and systems - digital interfaces - part 1: Single talker and multiple listeners," in *International Standard*. Geneva, Switzerland: International Electrotechnical Commission, 2002.

[16] E. W. G. for Mutual Exchange and D. of AIS & Data, "Ais data format - iec standard 61162-450 for ethernet interconnections," 2019.

[17] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2248–2294, 2021.

[18] F. Sicard, E. Hotellier, and J. Francq, "An industrial control system physical testbed for naval defense cybersecurity research," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022, pp. 413–422.

[19] M. Puys, P.-H. Thevenon, and S. Mocanu, "Hardware-in-the-loop labs for scada cybersecurity awareness and training," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES 2021. ACM, Aug. 2021. [Online]. Available: http://dx.doi.org/10.1145/3465481.3469185

[20] K. Tam, K. Forshaw, and K. Jones, "Cyber-ship: Developing next generation maritime cyber research capabilities," in *Conference Proceedings of ICMET Oman*, ser. ICMET Oman. IMarEST, Nov. 2019. [Online]. Available: http://dx.doi.org/10.24868/icmet.oman.2019.005

[21] G. Kavallieratos, S. K. Katsikas, and V. Gkioulos, "Towards a cyber-physical range," in *Proceedings of the 5th on Cyber-Physical System Security Workshop*, ser. Asia CCS '19. ACM, Jul. 2019. [Online]. Available: http://dx.doi.org/10.1145/3327961.3329532

[22] sailsoft, "Nemastudio from sailsoft," Sailsoft Inc., 2022. [Online]. Available: https://www.sailsoft.nl/ais_simulator.html

[23] "panaaj/nmeasimulator: Nmea sentence generator," https://github.com/panaaj/nmeasimulator, (Accessed on 05/01/2024).

[24] Sealevel, "Usb to 8-port rs-232, rs-422, rs-485 (software configurable) db9 serial interface adapter," 2022. [Online]. Available: https://www.sealevel.com/product/2823-usb-to-8-port-rs-232-rs-422-rs-485-software-configurable-db9-serial-interface-adapter/

[25] W. Inc., "Navisailor 4000," Wartsila Inc., 2022. [Online]. Available: https://www.wartsila.com/voyage/integrated-vessel-control-systems/navi-sailor-ecdis

[26] "Wireshark · go deep," https://www.wireshark.org/, (Accessed on 02/25/2024).

[27] F. Klassen, "Tcpreplay - pcap editing and replaying utilities," Appneta, Dec 2022. [Online]. Available: https://tcpreplay.appneta.com/

[28] M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2021. [Online]. Available: https://books.google.ee/books?id=Hwk1EAAAQBAJ

[29] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, Nov. 2022. [Online]. Available: https://doi.org/10.4218/etrij.2021-0181

[30] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamillaand, and A. M. Satyam, *Improving Web Application Security*. Microsoft Corporation, 2003. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330

[31] R. L. Harrison, C. Granja, and C. Leroy, "Introduction to monte carlo simulation," in *AIP Conference Proceedings*. AIP, 2010. [Online]. Available: http://dx.doi.org/10.1063/1.3295638

[32] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of udp ddos flood cyber attack and defense mechanisms on web server with linux ubuntu 13," in *2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15)*. Piscataway, NJ, USA: IEEE, 2015, pp. 1–5.

[33] K. Brown and S. Singh, "M-udp: Udp for mobile cellular networks," *SIGCOMM Comput. Commun. Rev.*, vol. 26, no. 5, p. 60–78, oct 1996. [Online]. Available: https://doi.org/10.1145/242896.242901

Appendix 4

Publication IV

G. Visky, A. Šiganov, M. u. Rehman, R. Vaarandi, H. Bahşi, H. Bahsi, and L. Tsiopoulos. Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 644–651, 2024

Hybrid Cybersecurity Research and Education Environment for Maritime Sector

Gabor Visky[1], Aleksei Šiganov[1], Muaan ur Rehman[1], Risto Vaarandi[1], Hayretdin Bahşi[1,2], and Leonidas Tsiopoulos[1]

[1]Department of Software Science, Tallinn University of Technology, Tallinn, Estonia
[2]School of Informatics, Computing and Cyber Systems, Northern Arizona University, United States
Email:{gabor.visky, aleksei.siganov, muaan.ur,
risto.vaarandi, hayretdin.bahsi, leonidas.tsiopoulos}@taltech.ee

2024 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-7536-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSR61664.2024.10679392

***Abstract*—Digitalization is a global trend affecting many critical infrastructures, including maritime transportation. Incorporating information and operational technologies into transportation processes significantly enhances efficiency but also introduces substantial risks originating from cyberspace. It is a significant endeavour to develop lab environments to research offensive and defensive aspects of cybersecurity and facilitate hands-on experience in educational settings.**

This paper introduces a hybrid cybersecurity research and education lab environment for the maritime domain. It enables real-world data to be fed into a controlled setting equipped with various emulation system components. The lab, which combines open-source and low-cost commercial software, also benefits from virtualization technologies and real hardware devices. Its scalability and affordability make it a viable solution for educational purposes. Although the environment is defended against external access, it can be provided for third parties on demand.

We conducted a series of cyberattacks on the network and an open-source navigation application to demonstrate the effectiveness of our lab setting. The recorded and shared network traffic from these attacks not only serves as a fertile ground for our own research but also invites other researchers to develop and test their solutions, fostering a collaborative environment for the advancement of cybersecurity in the sector.

***Index Terms*—Cybersecurity, Maritime, Research Environment, Education Environment**

I. Introduction

The maritime industry is actively adopting advanced technologies, including sensors, sophisticated networks, and heterogeneous devices, to boost efficiency and tackle contemporary challenges. These technologies have become increasingly integrated, so the maritime industry faces heightened cybersecurity concerns [1]–[4]. Consequently, the necessity for a diverse research lab environment becomes critical to fortifying cybersecurity infrastructure, learning and protecting against evolving threats, and ensuring the sector's resilience and safety. Moreover, empowering cybersecurity researchers to comprehend such offensive and defensive strategies necessitates the public availability of various attack datasets.

Various research studies have addressed a similar goal of establishing a lab environment in the maritime domain [5]–[7]. Despite the rich content of emulated system components, some of them do not provide publicly available datasets [5], [7] or the attacks realized in the datasets address limited attack types (e.g., only Man-in-the-Middle (MiTM) attacks to RADAR communication are addressed in [6]). The development and design of defensive mechanisms, such as intrusion detection systems (IDSs), highly require public datasets with diversified attack types to conduct effective benchmarking among the available solutions. More importantly, the current datasets include only attacks and normal system behavior [8]. However, in real-world settings, it is also important for IDSs to discriminate between malicious actions and system failures, as they initiate distinct incident-handling processes encompassing different teams. Thus, the datasets should include different system failure cases in addition to malicious actions to meet real-world requirements.

We have established a lab infrastructure that is designed to emulate a small-scale maritime network environment to facilitate research regarding various offensive and defensive aspects of cybersecurity. Although our aim is to extend the infrastructure with other operational technology components of a ship (e.g., engine automation, cargo handling), the current version mainly replicates navigational components, which constitute a significant attack surface for cyberthreats. In this paper, we detail the architecture of this laboratory setup. We also present a series of application and network layer cyberattacks executed within this lab environment. In addition to cyberattacks, we also emulate normal system behavior and system malfunctions induced by non-malicious factors. We capture the network packets of whole system activities, and derive the MarCyb dataset which is publicly available in raw format at https://data.taltech.ee/records/00fa9-5xv20.

Our lab infrastructure leverages virtualization technologies to deploy and test diverse system configurations easily. As malicious activities are generated in cybersecurity research, these technologies enable us to restore the system upon completion of the experiments. Although our current efforts focus on research activities, we also aim to use our experience to develop training environments for students and professionals in the future. Thus, virtualization perfectly aligns with this goal as it offers the required flexibility and scalability to create controlled settings for educational purposes. We also integrate real hardware devices into our lab to emulate more realistic cases when the research necessitates it. More specifically,

we have deployed an Automatic Identification System (AIS) receiver device that collects real-world AIS messages from the environment and relays them to the navigation system.

The rest of the paper is organized as follows: Section II gives some background information about maritime system components, standards and proprietary protocols. Section III presents the system architecture of the developed lab and details the system components and tools used for lab development.

The attacks, carried out in the environment are introduced in Section IV, which also includes the openly available MarCyb dataset. Section V elaborates on our results. Section VI introduces the related work and highlights the difference between ours and other's solution. Section VII concludes the paper and provides some insights about future research directions.

II. Background

A. Maritime system assets

Modern vessels typically adopt overarching digital onboard architecture to aid safe navigation. One critical component that is utilized is the Global Navigation Satellite System (GNSS), enabling worldwide localization. Additionally, one of the key factors that affect several aspects of navigation decision-making is the availability of information broadcasted between vessels and between vessels and shore base stations in proximity through the AIS [9]. AIS is a tracking system used in vessels and vessel traffic control services to identify and locate vessels. It is regarded as the main tool for complementing navigators' direct visual/audible information augmented with RADAR data to prevent collisions at sea. Information such as the unique identification number of the vessel (MMSI), its current position (longitude-latitude), heading, rate of turn, navigational status (e.g., underway or at anchor), course over ground (COG), and speed over ground (SOG) is broadcasted to other vessels and/or to base stations. This undoubtedly aids in navigation, as well as in tracking and monitoring the movement of other vessels. The rate of broadcasts ranges between 2 and 12 seconds depending on the size, speed and maneuver of the vessel while underway, and every 3 minutes while at anchor. The European Union has since 2010 required that passenger vessels, irrespective of size, and all vessels, other than passenger vessels, of 300 gross tonnage and upwards engaged on international as well as non-international voyage use an AIS system. Also, all fishing vessels of the EU countries whose lengths exceeded 15m were required to install the system by 2014 [10].

The RADAR system on a vessel also contributes to visualizing the static landmasses or buoys while also enabling automatic tracking of moving objects through the automatic radar plotting aid (ARPA), thereby revealing the course of vessels. Also, the dispersed sensors throughout the entire vessel are consolidated into a central Integrated Bridge System (IBS) and depicted on nautical displays called Electronic Chart Display and Information Systems (ECDIS) to support the crews.

B. Maritime networks and protocols

Nowadays, the transmission of sensed data on vessels is typically carried out through an ethernet-based network, specifically IEEE 802.3. A fundamental approach for transmitting nautical data is to utilize NMEA 0183, a standard specified by the National Marine Electronics Association (NMEA). NMEA formats the maritime data in human-readable sentences and encapsulates it within UDP datagrams or TCP streams. This facilitates the distribution of the nautical information through unicast, multicast, or broadcast transmissions over Internet Protocol (IP) [11].

The AIS infrastructure identifies nearby vessels and communicates with marine traffic control base stations. Typically, an AIS transceiver is connected to the network of the vessel via a serial link interface standardized by NMEA 0183. AIS messages are encoded within NMEA 0183 sentences inside link layer frames captured by the receiving station. These messages resemble IP packets featuring message lengths and structures determined by bit values in the header, and payloads encapsulated within higher-level frames. The receiving station can add blocks of tags to such sentences or add new sentences as needed [12].

III. System Architecture

The high-level network architecture of the lab setup is demonstrated in Figure 1. The main system components included in this architecture are described below.

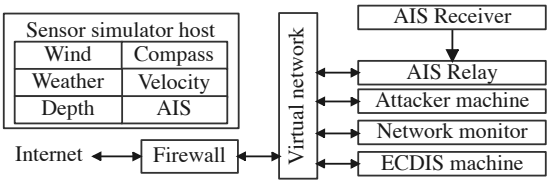


Figure 1. Network Architecture of Lab Setup

OpenCPN Server (OCPN): This component represents a simpler version of the ECDIS system [13]. It is the target host for the information collected from the navigation interfaces and other system components (i.e., AIS messages and sensory information).

AIS Receiver (AISRec): This device collects AIS messages transmitted by the ship in the coverage of the receiver and sends them to AIS Relay over TIA/EIA-422 protocol [14].

AIS Relay (AISRel): This host relays the AIS messages received by AISRec to OCPN. This host has a network interfaces connected to the internal network. An AIS Dispatcher software running on this host encapsulates AIS messages into UDP packets before relaying them [15].

Attacker Host (AttackH): This host is the source for the attacks conducted in the lab setup. Kali Linux 2023.2a is deployed to realize various attacks (e.g., network scan, MiTM, Denial of Service (DoS)).

Firewall (FW): This gateway applies network-level filtering rules by running Pfsense. It creates a controlled environment by enforcing strict inbound and outbound rules to isolate the lab environment from the Internet.

Network Monitor (NetMon): This component runs Zeek and Suricata to store and analyze the network packets regarding the normal behavior of the system components (benign traffic) and the attack-related behavior (attack traffic). Although our research environment can be used for system malfunction simulation and detection, this has not been implemented yet, and no system malfunction detector has been installed.

Sensor Simulator (SenSim): This component runs NemaStudio, a software to generate network traffic with the NMEA protocol [16]. It can simulate various source devices (e.g., AIS, RADAR, sensors) within different vessel contexts. As we utilize a real AIS device that collects real-world data from the environment, in our setting, this simulator is used to generate data related to various sensors such as wind, heading, and weather sensors.

In our network setting, AttackH, OCPN, AISRel, and SenSim are located in the same VLAN, which is referred to as shipLAN. NetMon is connected to the switch port, which listens to all traffic in promiscuous mode.

Table I
SYSTEMS COMPONENTS AND TOOLS

System Component	Operating System	Tools and Versions
OpenCPN Server	Security Onion 2.3	OpenCPN 5.8.4-1
AIS Relayer	Kali linux 2023.2a	NemaStudio 1.36
Sensor Simulator		Pfsense CE 2.6
Firewall		Zeek & Suricata
Network Monitor		
Attacker Host		

Table I provides detailed information about the system components (i.e., installed OSs and tools). Except for the AISRec, all system components run on the virtualization system using 14.48 GB RAM, 100GB disk and 7 virtual cores. We assigned 1 virtual core and 2 GB RAM to FW, 2 virtual core and 4GB RAM to each OCPN, SenSim and AttackH. AISRec is a hardware McMurdo SmartFind M15S device.

IV. SYSTEM BEHAVIOR AND EXECUTED ATTACKS

A. System Behavior

We defined two system behaviors, the normal one and the system failure and cyberattack-related one.

1) Normal System Behavior: Normal behavior refers to the period of the baseline generation, when a simulated cyberattack does not take place, and the network traffic consist of UDP packets conveying sensor data generated by SenSim, and relayed by AISRel. It also contains the IT infrastructure related packets, like ARP, ICMP, TUP packets.

2) System Failures and Cyberattacks: In this period the network traffic contains additional packets generated by AttackH. These packets are related to the malicious activity that is introduced in Section IV and can lead to system failures. Our current setup contains the NetMon component, that can indicate abnormal network traffic, but the system failure detector is the matter of further research. To support researchers, we also provide a file containing data on sensor malfunctions.

B. Network Attacks and MarCyb Dataset

To demonstrate the capabilities of our laboratory the most common attacks were conducted, and these attacks are introduced below [17]–[19].

1) Man-in-the-Middle attack: A "Man-in-the-Middle" (MiTM) attack is a form of cyberattack in which an attacker secretly intercepts and may modify communication between two parties. An address resolution protocol (ARP) spoofing was conducted to intercept the communication between the data source and the ECDIS. During this process the ARP tables of the endpoints were overwritten and the packets were transferred through the malicious actor's computer, where the content of the packets was optionally modified.

2) Replay attack: Replay attack involves recording network traffic between two peers, and replaying recorded network traffic at a later time, possibly changing the content of original network packets. Replay attacks are regarded as lower-tier MiTM attacks, since the adversary is not intercepting and modifying the network traffic in real time. In the lab environment, the replay attack was successfully executed for AIS messages, changing the name and the location of the vessel. For traffic recording, the *tcpdump* tool was used. Recorded network packets were modified with the *tcprewrite* tool, and replayed with the *tcpreplay* tool.

3) Fuzzing attack: Fuzzing is a method for testing the software which involves providing unexpected input to the software. In the field of network security, protocol fuzzing involves manipulating the protocol fields in network packets, so that the fields would have unexpected or abnormal values. Protocol fuzzing is useful for verifying if network applications are able to cope with abnormal packets and for identifying vulnerabilities in these applications (for example, buffer overflow vulnerabilities, conditions where the application crashes on specific abnormal protocol field values, etc.). In the lab environment, protocol fuzzing was applied to the NMEA protocol for testing the OpenCPN navigational application.

4) DoS attack: Denial of Service (DoS) attack involves saturating the network bandwidth or the computational resources of a network application with an excessively large number of network packets or application requests. In the lab environment, DoS attacks were staged with *T50*, *hping3*, and *Metasploit* tools, creating a flood of UDP packets not in NMEA format. The OpenCPN navigational application was targeted by these DoS attacks, testing its ability to cope with large number of packets in invalid format.

5) Scanning attacks: The lab environment was also used for various scanning activities with the *nmap* and *masscan* tools:

A) TCP and UDP port scanning – this type of scanning allowed for identifying open ports (network services) which

can be accessed by the attacker. Since TCP protocol involves a connection setup with a three-way handshake, a valid response from the network service during the handshake indicates that the service is available. In contrast, for UDP ports the service availability cannot always be reliably determined, since UDP does not involve a connection setup procedure, and many UDP services are not guaranteed to respond to packets from scanning tools.

B) Scanning with NSE (Nmap Scripting Engine) scripts – this type of scanning allowed to use custom *nmap* scripts for automated vulnerability checks and collection of additional information about network services.

C. Application attacks

Khandker et al. in [20] published a comprehensive study about the cyberattacks against AIS system. We followed that work and adopted and executed the application-layer attacks on network level against the ECDIS in our environment. Furthermore, we extended the targets and attacked the navigational system from other direction as well by modifying sensor values, such as wind, velocity, depth sensors.

1) Man overboard (MOB): The result of this attack is marking of a position where someone has fallen off the ship into the water triggering a rescue operation. The MOB is a distress AIS message containing coordinates and triggers immediate alerts on neighboring vessels. This attack can trigger false alerts, causing significant waste for rescue forces and other ships.

2) Spoofing: refers to the manipulation of AIS data transmission to deceive other vessels or monitoring systems about the position, identity, or other relevant information of a ship.

3) Visual navigation disruption (VND): refers to the appearance of different fake targets. Such a scenario could significantly confuse the ship operator's situational awareness, even in the absence of triggered alerts. We executed a large number of spoofing and MOB attacks by injecting UDP packets to the network containing NMEA sentences with malicious content to cause VND.

4) Collision alert: deployed by adding fake ship positions to an AIS signal near by the targeted ship. This prompts the targeted ship to alter its course or take evasive action unnecessarily.

5) Logically invalid data encoding: describes a situation when a ship sends inconsistent interdependent data. For example the change of the position is not valid according to its speed.

D. MarCyb dataset

Cybersecurity researchers always need efficient validation for their proposed approaches; However, the maritime sector is lacking in richly available attack datasets in comparison to other domains [21]. To fill this gap, we have documented MarCyb, a thorough dataset encompassing cyberattacks on/in the vessels. This dataset comprises network captures stored as PCAP files, along with necessary labelling. Also, the MarCyb dataset comprises samples from both network attacks (Section IV-B) and application layer attacks (Section IV-C), including their variations. Table II presents the dataset details including attack type, references to detailed descriptions in our paper, the targeted assets, and short attack descriptions.

V. Discussion

A. Performance Analysis

Kavallieratos et al. in [22] outline the requirements for the cyber-physical range that we have adopted to evaluate our research environment.

1) Flexibility: The proposed solution mainly consists of virtualized software components, providing high flexibility. To extend this feature we introduce infrastructure as code (IaC) technology by using the Ansible software tool [23]. At the same time, it can be extended with external hardware components that can bring challenges into the picture.

2) Scalability: One of the key strengths of our system is its scalability. By deploying multiple instances, we can easily accommodate a growing user base. This feature is also supported by Ansible. Furthermore, the system can be expanded with additional components, software, and scenarios, ensuring its ability to meet future needs.

3) Isolation: Our research laboratory environment offers a unique feature: the ability to operate without external connections. This isolation provides a safe and secure environment for cybersecurity research. However, it is important to note that this feature does limit remote access. To overcome this limitation we allowed remote access to the environment over Virtual Private Network (VPN). Simultaneously a Firewall limits the external access and ensures the defensive measures.

4) Interoperability: The introduced environment has broad interconnection capabilities since it uses standardized components and communication protocols. The interoperability is heavily supported by VPNs among the instances.

5) Cost-Effectiveness: Since the environment mainly relies on open-source components, it is cost-effective. To achieve this goal one common AIS receiver provides data over UDP protocol to every instance. The environment supports deploying additional hardware while keeping the operational and maintenance costs as low as possible.

6) Built-In Monitoring: The environment natively provides real-time and post-mortem access to detailed monitoring data, if they are recorded, including flow data and captured packets from the network links, as well as metrics and logs related to the simulated processes. This feature makes the research results and teaching processes reproducible.

7) Easy Access: Experienced users can use the environment with reasonable training. The IaC technology support this feature and helps to create a clear environment in the case of need. Furthermore it supports education and training as well, since the instructor can deploy an environment according to the needs of the given training or lecture by running a code.

8) Adaptability: Because of its design, the environment is highly flexible, providing high adaptability. It is possible to install and uninstall different components with reasonable reconfiguration effort.

Table II
MARCYB DATASET

Attacks	Section	Targeted assets/protocols	Variations/types	PCAP
Network attacks				
MiTM	IV-B1	ARP tables, OpenCPN, AIS	AIS target modification (Vessel name, location change)	mitm.pcap
Replay	IV-B2	OpenCPN, AIS	AIS target injection	replay_attack.pcap
Fuzzing	IV-B3	OpenCPN, AIS	Protocol fuzzing	fuzzing.pcap
DoS	IV-B4	OpenCPN, Network	Network Flooding	network_flood.pcap
Scanning	IV-B5	UDP, TCP, OS	Aggressive scan, fast scan	nmap_fast_scan_udp.pcap nmap_fast_scan_tcp.pcap masscan_fastscan.pcap nmap_agressive_scan.pcap
		Hidden port scan	Low rate scan	masscan_lowrate.pcap nmap_hidden_scan_tcp.pcap
Application attacks				
Visual navigation disruption	IV-C3	OpenCPN, AIS	Too many AIS and MOB targets on the screen	Introduced as man overboard flooding and spoofing attacks.
Spoofing	IV-C2	OpenCPN	Fake Sensor values	sensor_modification_wind.pcap sensor_modification_depth.pcap sensor_modification_gps.pcap
AIS Target flooding	IV-C3	OpenCPN, AIS	Fake AIS target	randomized_other_ship_position.pcap randomized_ship_position.pcap
Man overboard flooding	IV-C1	OpenCPN, AIS	Fake MOB target	man_overboard.pcap
Collision alert	IV-C4	OpenCPN, AIS	Fake collision alert on the screen	collision_alert_attack.pcap
Logically invalid data encoding	IV-C5	OpenCPN, AIS	Logically invalid sensor values	LID_attack.pcap
Files without attacks				
48 hours long capture.				normal_traffic_48h.pcap
11.5 hours long capture, containing only UDP encapsulated sensor data.				normal_UDP_traffic_48h.pcap
48 hours long capture without external communication.				normal_traffic_without_internet.pcap
File with sensor failure				
File with sensor malfunction.				sensor_malfunction.pcap

9) Shareability: Our environment is highly shareable since the multiple instances can accommodate several students simultaneously. On higher scale it can be deployed in other environments as well, because of the IaC technology.

B. Discussion on the attacks

1) Successful attacks: We meticulously executed a variety of attack types, each specifically targeting different layers of the network protocol. Our focus extended to the ECDIS application as well, ensuring a comprehensive evaluation.

At the lower layers, we conducted a scanning and MiTM attack. Our scanning revealed the network topology, a crucial step that paved the way for the successful execution of the MiTM attack. This attack allowed us to poison the ARP tables and initiate communication sniffing between the sensor simulator and the ECDIS. This comprehensive method enabled us to eavesdrop, spoof, and even launch a form of DoS attack. The eavesdropping feature was particularly useful as we recorded the relevant communication, which we later replayed during the replay attack. This aided in the analysis of the communication structure. This feature can prove invaluable in the case of more complex communication scenarios.

We targeted the ECDIS application with fuzzing. With this method, we found that the ECDIS does not check the CRC of the received packets, and its receiver buffer can be overflown with randomly generated data.

We also executed spoofing attacks against the ECDIS, in which we faked or generated different sensor data implicating different real-life scenarios, like MOB or faulty sensors.

The same method was used for jamming attacks, that was also discussed in [20]. During this attack, we overloaded the ECDIS and its operator with false alerts that can endanger the safety at sea.

2) Unsuccessful attacks: Khandker et al. [20] discuss overwhelming alerts as an attack that describe the situation where many simultaneous alerts are triggered, potentially leading to the crash of ECDIS software or overloading its operator. Similarly, a true positive alert may go unnoticed in such a chaotic situation. The consequences of ECDIS failure due to overwhelming alerts can be severe, posing immediate risks to maritime safety and navigation. The installed OpenCPN ECDIS software did not trigger alerts so this attack was not executed successfully. However, we share the relevant network traffic file supporting researchers dealing with such scenarios.

3) Other attacks: The above-mentioned paper [20] introduced jamming as a form of attack, its two forms — the radio frequency (RF) jamming when the AIS frequencies are overpowered with noise to suppress valid AIS transmissions, and the display flooding when valid AIS signals are transmitted so that the valid ships cannot be displayed or they are suppressed— were not executed, since the above-mentioned technologies are related to electronic warfare, so they are out of the scope of our paper. However, the display flooding was

executed on the network level, and we discussed it as part of spoofing.

Similarly, the coordinated attack —referring to the situation when attackers send multiple signals that contain the same reference (MMSI number) but differing values in some of the AIS data fields— was not executed, since on the network level the transmitters can not be distinguished.

VI. Related Work

Longo et al. [5] developed MaCySTe, which is an open-source testbed which reproduces the core components of the onboard cyber-physical systems (CPSs) and network infrastructure of a ship. MaCySTe is capable of simulating key onboard sensors, including the RADAR antenna, Electronic Position Fixing System (EPFS), AIS, Speed and Distance Measurement Equipment (SDME), gyroscope and compass. MaCySTe interfaces with ship and hydraulic system simulators, enabling realistic testing and training scenarios for cybersecurity and maritime operators. The different architecture components are connected through an integration layer that utilizes a dedicated Message Queue (MQ) for exchanging data, facilitating easy replacement of components. The IBS can also be simulated by integrating the ECDIS and a RADAR Plan Position Indicator (PPI), thereby centralizing access to sensor data through their interconnected setup. Network zones and the connections of components follow the standard configuration of a ship area network, utilizing the NMEA 0183 protocol and Multicast UDP for communications between onboard equipment and sensors. Moreover, for RADAR video information transmission from the antenna, Navico Broadband Radar BR24 [28] or the Eurocontrol standard ASTERIX Cat-240 [29] protocols are utilized. Lastly, communications between Programmable Logic Controllers (PLC) and their interactions with the Integrated Platform Management System (IPMS) operate by using the standard MODBUS [30] protocol.

The MaCySTe testbed can be executed with different scenarios, the core one that implements the abovementioned components, and an extended version that incorporates Security Information and Event Management (SIEM) and a malware which executes targeted attacks. To simulate attacks a Simulated Internet network is added, probing for capturing NMEA and MODBUS traffic and mimicing the ship connection to the public Internet via a dedicated Router component. A malicious software installed on the Integrated Navigation System (INS) can overhear or monitor traffic on the Bridge network, inject packets, and communicate with a remote Command & Control (C&C) server on the Internet. Specifically, the malware software can either inject high-frequency NMEA packets to fake the heading value or inject ASTERIX packets to disrupt the RADAR image. Although MaCySTe involves an advanced overall architecture, currently only MiTM and DoS attacks can be simulated.

Amro and Gkioulos described a cybersecurity testbed for autonomous passenger ships [24], which has been shown to effectively analyze and evaluate maritime use cases with a focus on cybersecurity and communication dimensions [31]. Similarly to the set-up of our lab environment, Amro and Gkioulos utilized both simulation/emulation components with actual equipment to strike a balance between cost, realism, scalability, and reproducibility. For example, AIS could be replicated using physical equipment or an AIS simulator software and OpenCPN is used as the chart plotter software. Overall, the testbed is structured into both a physical and a virtual testbed, and an integration of both. The range of attacks deployed is rather broad including network sniffing, service scanning, ARP cache poisoning, as well as attacks against maritime sensor data (NMEA) including variations of Manipulation and/or denial of view attack techniques. Although the set-up of this testbed is advanced, it is not currently available for public access and generation and availability of maritime-related datasets has not been discussed by the authors.

Wolsing et al. [6] implemented a holistic simulation environment and identified MiTM network-level attacks against marine radar. In their model, the authors simulated modern vessels with sensors such as radar, ARPA, GNSS, and AIS, connected via Ethernet to an IBS. The simulation environment utilizes Bridge Command (BC) software for radar and environmental simulation, enhancing its realism and adding support for broadcasting AIS reports. Realistic scenarios are designed, accounting for varying terrain and environmental conditions, with vessels modeled using historical AIS data. The IBS is modeled using OpenCPN software, serving as the radar display and control unit, with autopilot functionality for navigating predefined routes. To execute MiTM attacks, the authors leveraged the Radar attack tool, which serves as a MiTM malicious device between the sensor network and the IBS. Overall, the simulation environment primarily focuses on MiTM manipulation of the Radar images using packets based on the Navico BR24 RADAR protocol. However, to establish a comprehensive research environment, it is necessary to also simulate different attacks on AIS and other sensor-based attacks.

The simulation environment described by Becmeur et al. [25] introduces a platform for generating data and scenario traces to evaluate IDS algorithms. The platform can simulate the critical subsystems of a ship, including propulsion and engine control systems, as well as navigation systems, using independent controllers and common industrial communication protocols. While the environment is outlined based on objectives and outcomes, its description lacks sufficient detail on procedural intricacies essential for comprehensive understanding and reproducibility.

Raimondi et al. [26] described a testbed for conducting cyber exercises to train maritime Security Operations Center (SOC) teams. The training scenario described integrates a practical, hands-on approach to cybersecurity training, specifically tailored for maritime SOC operators. This simulation environment, based on the digital twin framework LiDiTE, involves a dual-site setup; a remote ship and a shore-side SOC. The remote ship simulation employs the Bridge Command simulator to mimic ship operations and onboard sensors like GPS and AIS transponders, with data collection managed via

Table III
COMPARISON TO RELATED WORKS

Reference	Components simulated	Main attack scenarios	Protocols	Dataset	Cost
Longo et al. [5]	RADAR, EPFS, AIS, SDME gyroscope, compass, ship and hydraulic system, ECDIS	MiTM, DoS, malware attacks	NMEA 0183, Navico BR24, ASTERIX Cat-240, MODBUS	no	low
Amro et al. [24]	AIS, GPS, Network simulation, OpenCPN	Network sniffing, service scanning, ARP poisoning, NMEA manipulation.	NMEA	no	medium
Wolsing et al. [6]	Radar, IBS, GNSS, BC, AIS, OpenCPN	MiTM attack on radar network	Navico BR24, AIS, ARPA	yes	medium
Becmeur et al. [25]	Propulsion, engine control, navigation systems	DoS, attack against navigation, propulsion and SCADA systems	ModBus, DNP3, S7	no	medium
Raimondi et al. [26]	Ship operations & shore-side centre components, gyrocompass	NMEA packet injection, data tempering	NMEA 0183	no	high
Visky et al. [7]	ECDIS, RADAR, weather, Operational situation, AIS, 10+ OT sensors	Network sniffing, ARP poisoning, network data manipulation.	NMEA 450, Transas proprietary protocol	no	high
Sicard et al. [27]	Propulsion, artillery control, Trajectory Generator, Energy	Network attacks and process attacks	Modbus, Profibus	no	medium
Our environment	AIS, GNSS, weather, compass, velocity, depth sensors	Application and network layer attacks	TCP, UDP, AIS, NMEA 0183	yes	low

a Python script and further processing by an INS network. This network supports an IDS and a shipboard SIEM system, parsing and analyzing NMEA traffic to detect anomalies and maintain cybersecurity. Connectivity between the ship and the shore-side SOC is facilitated through a simulated VPN, with the shore-side SOC using tools such as Splunk for SIEM functionalities and OPNsense for firewall protection. The setup is designed to train SOC operators in real-world cybersecurity threat detection, response, and management through interactive and immersive simulations. The authors set up a scenario where trainees face simulated attacks, including the injection of false NMEA messages that interfere with the ship's gyrocompass, with the task of detecting this interference. However, a broader range of attack types, the availability of attack data and the complexity of accurately reproducing sophisticated attacks remain areas that need further development.

Visky et al. [7] introduced a multi-purpose simulation environment for the maritime sector. The solution supports, besides the seaferes' cyber education, cyber-related research, particularly for system analysis, hardware/software and cybersecurity protection development, and testing. The authors leveraged Transas NTPRO 5000 Navigational Simulator for seafarer training. This simulator realistically replicates ship operations with dynamic control over environmental conditions and uses authentic maritime equipment to provide visual and functional simulation. It generates network traffic mimicking actual ships through protocols like NMEA 0183, facilitating cybersecurity research by enabling the testing and simulation of cyber-attacks in a controlled setting. Furthermore, the environment supports the existing procedures' testing. The drawbacks of the solution are its complexity, its relatively high price and its low scalability.

Sicard et al. [27] described a testbed for experimenting with the Industrial Control System (ICS) of a warship. The paper introduces a sophisticated maritime testbed tailored for cybersecurity research within the naval defence sector. This simulated environment mirrors the complex system operations of a warship, focusing on key operational segments such as ship direction, propulsion systems, artillery control, and energy management. Each segment is equipped with specific control systems and hardware that simulate real maritime conditions. The testbed employs a variety of maritime-specific technologies, such as shipboard PLCs for rudder control and propulsion management, and uses communication protocols integral to naval operations. This facility enables the testing of cyber-attacks, including those that target navigation systems and artillery components, in a secure yet realistic maritime setting. The configuration allows researchers to rigorously evaluate potential cybersecurity measures, and develop intrusion detection systems, significantly contributing to enhanced maritime cyber resilience. However, no dataset was published in [27] and generating realistic data was identified as future work.

Table III provides an overview and comparison of the related work. We have listed the main modules simulated in the related work, major attack scenarios executed, protocols used, access to the generated dataset and corresponding cost of developing and maintaining the environments. Table III shows that we have created the lab environment cost-effectively and provided public access to the generated dataset.

VII. LIMITATIONS, CONCLUSION AND FUTURE WORK

In this paper, we describe the architecture of a maritime lab infrastructure that allows maritime cybersecurity experiments and training in a realistic environment. We also describe network and application layer cyberattacks executed in the lab environment. In addition, we emulate the expected system behaviour and system malfunctions caused by cyberattacks. The network traffic from all aforementioned activities was captured to create the openly available MarCyb dataset containing data from two classes: benign and attack network traffic. Although

the research environment is available only on our institution's premises, the dataset is publicly accessible.

Our research was limited by the open-source ECDIS, since it is rarely used in shipping industry, and the limited number of sensors, but we consider our environment realistic enough for research and education purposes and it proofs our concept.

For future work, we plan to extend the dataset to include novel attack types not covered in the current paper. Additionally, our research environment provides a unique opportunity to study system malfunctions, which are often difficult to distinguish from cyberattacks. We intend to generate such traffic to facilitate the evaluation of advanced detection methods, which are essential for accurately identifying whether an anomaly is due to a cyberattack or a system malfunction.

ACKNOWLEDGEMENT

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

REFERENCES

[1] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166

[2] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100571, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555

[3] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22

[4] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean &; Coastal Management*, vol. 236, p. 106493, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1016/j.ocecoaman.2023.106493

[5] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "Macyste: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, p. 101426, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235271102300122X

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

[7] G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam, "Multi-purpose cyber environment for maritime sector," *17th International Conference on Cyber Warfare and Security*, pp. 349–357, 2022. [Online]. Available: https://doi.org/10.34190/iccws.17.1.26

[8] R. Kalakoti, H. Bahsi, and S. Nõmm, "Improving iot security with explainable ai: Quantitative evaluation of explainability for iot botnet detection," *IEEE Internet of Things Journal*, 2024.

[9] *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*, ITU-R Radiocommunication Sector of ITU, 2014, recommendation ITU-R M.1371-5.

[10] I. M. Organization, *Solas: Consolidated Text of the International Convention for the Safety of Life at Sea, 1974, and Its Protocol of 1988, Articles, Annexes and Certificates, Incorporating All Amendments in Effect from 1 January 2020*, ser. IMO publication. International Maritime Organization, 2020. [Online]. Available: https://books.google.hu/books?id=JKULzgEACAAJ

[11] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, and J. Bauer, "Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring," *Journal of Marine Science and Engineering*, vol. 11, no. 5, p. 928, 2023.

[12] D. Blauwkamp, T. D. Nguyen, and G. G. Xie, "Toward a deep learning approach to behavior-based ais traffic anomaly detection," in *Dynamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop, San Juan, PR*, 2018.

[13] "Opencpn official site," https://opencpn.org/, (Accessed on 05/29/2024).

[14] "Rs-422 - wikipedia," https://en.wikipedia.org/wiki/RS-422, (Accessed on 05/31/2024).

[15] "Ais dispatcher - free ais data sharing tool — aishub," https://www.aishub.net/ais-dispatcher, (Accessed on 05/31/2024).

[16] sailsoft, "Nemastudio from sailsoft," Sailsoft Inc., 2022. [Online]. Available: https://www.sailsoft.nl/ais_simulator.html

[17] R. Daş, A. Karabade, and G. Tuna, "Common network attack types and defense mechanisms," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, 2015, pp. 2658–2661.

[18] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol. 40, pp. 307–324, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804513001756

[19] A. A. Ghorbani, W. Lu, and M. Tavallaee, *Network Attacks*. Boston, MA: Springer US, 2010, pp. 1–25. [Online]. Available: https://doi.org/10.1007/978-0-387-88771-5_1

[20] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity attacks on software logic and error handling within ais implementations: A systematic testing of resilience," *IEEE Access*, vol. 10, pp. 29 493–29 505, 2022.

[21] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2248–2294, 2021.

[22] G. Kavallieratos, S. K. Katsikas, and V. Gkioulos, "Towards a cyber-physical range," in *Proceedings of the 5th on Cyber-Physical System Security Workshop*, ser. Asia CCS '19. ACM, Jul. 2019. [Online]. Available: http://dx.doi.org/10.1145/3327961.3329532

[23] "Homepage — ansible collaborative," https://www.ansible.com/, (Accessed on 05/28/2024).

[24] A. Amro and V. Gkioulos, "Communication and cybersecurity testbed for autonomous passenger ship," in *Computer Security. ESORICS 2021 International Workshops*, S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge, Eds. Cham: Springer International Publishing, 2022, pp. 5–22.

[25] T. Becmeur, X. Boudvin, D. Brosset, G. Héno, B. Costé, Y. Kermarrec, and P. M. Laso, "Generating data sets as inputs of reference for cyber security issues and industrial control systems," in *2017 11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2017, pp. 453–454.

[26] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo, "Training the maritime security operations centre teams," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2022, pp. 388–393.

[27] F. Sicard, E. Hotellier, and J. Francq, "An industrial control system physical testbed for naval defense cybersecurity research," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2022, pp. 413–422.

[28] A. Dabrowski, S. Busch, and R. Stelzer, "A digital interface for imagery and control of a navico/lowrance broadband radar," in *Robotic Sailing*, A. Schlaefer and O. Blaurock, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 169–181.

[29] *Specification for Surveillance Data Exchange – ASTERIX Category 240: Radar Video Transmission, 1st Edition, EUROCONTROL-SPEC- 0149-240*, EUROCONTROL, 2015. [Online]. Available: https://www.eurocontrol.int/publication/cat240-eurocontrol-specification-surveillance-data-exchange-asterix

[30] A. Swales, *Open modbus/tcp specification*, Schneider Electric 29, 1999.

[31] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104

Appendix 5

Publication V
G. Visky, D. Khisteva, and O. Maennel. *Technical Considerations for Open-Source Intrusion Detection System Integration in Marine Vehicles*, pages 143–160. Springer Nature Switzerland, Cham, 2025

Technical Considerations for Open-Source Intrusion Detection System Integration in Marine Vehicles

Gabor Visky, Dariana Khisteva, and Olaf Maennel

Abstract Maritime transport is critical to the global economy; however, it is vulnerable to disruptions impacting global trade. Academia, industry, and national and international organisations make serious efforts to enhance the sector's resilience, focusing on the cyber aspects as well. With their unique characteristics, marine vehicles and their defence has only recently emerged as a significant area of cyber security study. Existing literature touches upon various aspects of intrusion detection systems (IDSs) as a potential defensive measure for Information Technology (IT) infrastructure against cyber attacks, along with the special characteristics of the marine vehicles that brings the need for solutions considering the uniqueness of the operational technologies (OT). Despite of the reach literature a comprehensive discussion presenting an overall, conceptional view is needed. Our paper, that addresses this need, introduces the different technical aspects to be considered during the design and integration of an IDS into a marine vehicle. To find the relevant details, we conducted a comprehensive literature survey and gathered details that could help the integration process.

Key words: maritime, cyber, intrusion detection system, concept

Gabor Visky
Department of Computer Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: gabor.visky@taltech.ee

Dariana Khisteva
Department of Computer Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: dakhis@taltech.ee

Olaf Maennel
School of Computer & Mathematical Sciences, University of Adelaide, Adelaide, Australia, Address of Institute e-mail: olaf.maennel@adelaide.edu.au

1 Introduction

1.1 Intrusion Detection Systems

Intrusions usually cause anomalous behaviour of their victims [1]. Anomalous behaviours can also be attributed to random system failure and unforeseen external factors. Intrusion detection systems are designed to identify anomalies attributed to cyber security incidents [2]. An IDS identifies and logs predefined activities in network parameters, system configurations, or user behaviours and, if programmed, can also notify staff members to investigate specific alerts and take further actions.

We can distinguish IDSs according to the source of the acquired input samples in the environment they monitor. A NIDS, serving as the first line of defence, monitors network activity, collects network-related data, and identifies malicious traffic. It scrutinizes all network traffic and flags any suspicious patterns.

Conversely, a HIDS provides a deeper, more localized level of security analysis by focusing on detecting potential attacks on individual computers where the IDS is installed. This system monitors system parameters such as memory content and usage, CPU load, network traffic, processes, and user actions.

These devices, using different anomaly detection methods, rule violation detection, or signatures recognition, identify possible hostile activities [3, 4].

1.2 Cyber-situation in the maritime sector

Modern society relies significantly on marine transportation, which handles approximately 80% of global trade [5]. To enhance efficiency, maritime systems have become increasingly digitalised and interconnected over recent decades, introducing significant cybersecurity concerns in the sector [6–9].

Many actors in the field, companies [10, 11], universities and research institutions [12, 13] make serious efforts to increase the cyber resilience of the sector. However, many ships rely on obsolete technologies produced without cyber security considerations, making them vulnerable to cyber-attacks. Because of their complexity, ships' navigational and control systems cannot be upgraded overnight, and they can only be extended with security solutions after a deep analysis of the impacts. So, vendors producing such systems are hesitant about this question regarding old products.

Cybersecurity companies provide commercial-of-the-self (COTS) solutions for various sectors focusing on IT. There is a large community of commercial and/or open-source vendors, so COTS defends against "up-to-date attackers" on the IT side on moderated costs.

Since IT is easily available, OT has also started to use it: OT components are integrated into the IT world, making OT targeted by malicious actors.

Most of these COTS products handle only IT networks, but they omit the unique needs of a ship: specialised offerings for waterborne vessels remain limited since the attack surface in the maritime environment contains not only IT but navigational, surveillance, OT and Industrial Control Systems (ICS) [14].

These particular characteristics are still an open issue and must be addressed: Fine-tuned, tailor-made solutions are needed. Numerous studies have explored the challenges of introducing defence measures on a ship, and suggested the deployment of open-source IDSs on board.

Jacq et al. discuss the concept of naval systems' situational awareness and introduce how to detect cyber attacks on board ships in real-time, and elaborate on cyber situational awareness. They found that the host-based IDS (HIDS) cannot be installed on a computer in the ship control system without causing a warranty disruption. They offered network-based IDS (NIDS) as a feasible extension [15].

Amro et al. in [16] proposed a systematic approach for navigational message analysis to detect sensor data anomalies caused by malicious activities. They demonstrated their detection capabilities by specification-based and frequency-based detection. They also propose that NIDS be added to the networks to monitor network traffic and detect anomalies.

Visky et al. highlighted the open-source IDS integration as a response to the challenge and identified the need for a concept as a research gap. Our current study addresses this gap and introduces a concept to fertilise the development and integration of such a system into marine vehicles [17].

These publications introduce the need and applicability of open-source IDSs on ships but do not evaluate all the technical details that come up during this process. Our research widens the focus and introduces more technical details that could be evaluated.

2 Related Work

Reach IDS-related literature is available. Gupta et al. surveyed and introduced it in [18]. The study introduces 113 research articles related to IDS, intrusion prevention systems (IPSs) and intrusion detection and response systems (IDRSs). The review focuses on the literature and introduces the topic but does not share detailed considerations for marine-related IDSs.

Alkasassbeh et al. introduced IDS' the state-of-the-art [2]. The paper overviews the field in detail, mainly from a technology point of view, without focusing on the needs of a particular industry segment, like shipping, where the OT-related details are significant.

Schell et al. in [19] discuss IDS concepts for intra-vehicle communication. Their publication focuses on wireless communications (Bluetooth, WiFi) and services, like Global System for Mobile Communication (GSM), and introduces the requirements for anomaly handling. These details are limited in the case of the current ships, but they gain importance as autonomous shipping comes into the picture.

Agrawal et al. in [20] introduce the concept of federated learning, which is a decentralised learning technique. It helps preserve the privacy of what gets jeopardised since IDSs often process, store, and communicate private data. The paper introduces, besides the current challenges, —such as communication overhead, vulnerabilities in intrusion detection setup and federated poisoning attacks— as well as future challenges like edge computing, implementation and optimisation issues.

Our research, motivated by the lack of a comprehensive study, collects the considerations needed for IDS development for water surface vehicles.

3 Main considerations and components

Integrating an into marine vehicles involves several critical considerations and components that are introduced in this section.

3.1 System Requirements and Objectives

3.1.1 Security Goals

To set up the optimal IDS for a marine vehicle, the security goals should be defined. The CIA triad, comprising confidentiality, integrity, and availability, has served as a foundational framework for computer security for several decades. [21]. The STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) methodology, as defined by Shostack [22] includes three additional elements: authentication, non-repudiation, and authorisation. [23].

Based on this attack modelling method, the main security goals can be defined. Spoofing involves the ability of an adversary to masquerade as someone or something else. Denial of service refers to compromises to the system's availability by consuming the necessary resources for its proper operation. Elevation of privilege is when an adversary can execute unauthorised actions. An IDS can identify such attacks.

Tampering refers to modifying or disrupting a system's disk, network, or memory. Repudiation relates to threats where someone denies having taken specific actions that impact the system's operation or disclaims responsibility for the resulting outcomes. Information disclosure is another threat that exposes confidential information to unauthorised individuals. An IDS cannot identify such kinds of attacks.

3.1.2 Performance Requirements

To reduce the damage caused by a cyber attack, it is crucial to identify it as soon as possible and take immediate actions. The potential risks of a cyber attack are significant, and early detection is key to mitigating these risks.

An IDS can indicate malicious activity in a network, that increases the cyber security significantly, but it cannot implement any security measure, while an IPS can. Installation of an IPS sounds like a legitimate solution, but according to our studies, the first objective of the shipping is to safely complete the mission so that a cyber incident cannot risk it. For example, an IPS cannot exclude a mission-critical host. This decision may be made by a cyber expert. Since there is limited or no cyber expert in the crew, the decision should be made in the shore control centre, based on anomaly-related information collected on the ship. The limited communication bandwidth makes this process difficult, setting a special requirement for the IDS on the board. It must indicate the anomaly in its early stage, and assist its mitigation on no or limited communication with the shore.

3.1.3 Regulation Compliance

An IDS must comply with the regulations and national and international law.

Cyber security in maritime has been gaining momentum because of recent incidents [24]. To handle this emerging problem, authorities are making significant efforts. To support effective cyber risk management and safeguard shipping from cyber threats and vulnerabilities in 2017. IMO issued a guideline containing high-level recommendations on maritime cyber risk management [25,26]. However, guidelines are just recommendatory.

To encourage administrations to appropriately address cyber risks in existing safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021 [27] in June 2017, the Maritime Safety Committee also adopted the resolution for Maritime Cyber Risk Management in Safety Management Systems.

International Ship and Port Facility Security (ISPS) Code established by the IMO is partly regulates the cyber security risk assessment [28]. These regularities do not specify particular characteristics of cyber security solutions on a ship, so there are no precise requirements that an IDS should meet.

According to the data protection laws organisations must ensure that their use of an IDS complies with relevant data protection laws, such as the General Data Protection Regulation (GDPR) [29] in the European Union, the California Consumer Privacy Act (CCPA) [30] in the United States, or other applicable regulations. These laws typically require transparency in data collection, the right of individuals to access their data, and strict controls on data processing.

In some jurisdictions, organisations may be required to inform employees or network users that their activities are being monitored. In certain cases, explicit

consent may be necessary before implementing an IDS, especially if it involves monitoring personal communications.

3.2 Selection of the IDS

After analysing the literature, experts' opinions, and the current situation, we found that installing a NIDS into ships' networks is optimal for increasing their resilience with anomaly early detection.

The market offers several commercial NIDS [31–34]. These products have high capacity and scalability, which is not needed on ships because of their limited network size, but they can not be extended with ship-specific features. The deployment of an open-source NIDS, known for its reliability, can effectively overcome these limitations. To find the optimal one, many details should be considered.

Adeeb Alhomoud et al. compared Suricata and Snort in high-speed networks. According to their results, the virtualisation significantly increases the number of packet drops. Additionally, Suricata performed better on Linux while Snort on FreeBSD, especially when handling high speeds [35].

Traditional IDSs can detect known attacks by predefined rules or anomaly detection using baselines. Modern technologies collect and analyse vast amounts of data. To increase the efficiency of these IDSs, the most relevant features should be selected to shrink the dataset.

Harbola et al. discuss four kinds of feature selection methods: filter-, wrapper-, embedded methods and classification algorithm [36]. Gül and Adali [37] analysed the features of the NSL-KDD (Network Security Lab - Knowledge Discovery in Databases) dataset [38]. According to their studies, the number of the selected features depends on the attack types we want to detect. They found the most important ones in the *dst_bytes* and the *count features*. In the second-degree service, logged_in, root_shell, srv_diff_host_rate and dst_host_count were the most important.

The long life conditions are also important when choosing an IDS. The support of the different communal products often ends within a few years, unlike in the case of open source solutions. In their case, the activity of the community defines the "quality of the support".

3.3 Architecture

3.3.1 System Architecture

There can be several networks on the ships, which have different impacts on the missions. For example the wireless network providing internet access to the passengers is not that mission critical like the navigation or propulsion network. While designing the architecture this fact should be evaluated.

There are different approaches to keep these networks isolated.

Every network can have a separate, low-profile IDS, and the alerts and logs can be aggregated. This solution has moderated deployment and high maintenance costs since every IDS must be updated separately. At the same time, the different IDSs can be highly trained according to the characteristics of the given network, which can improve their sensitivity and moderate the false positive rate. This solution can also handle special typologies, such as link topology.

Another solution is the deployment of separated sensors into the different networks, and all of them send the prepossessed and unified data to a central IDS. This solution can still handle the different characteristics of the networks but needs a higher-performance central IDS.

The third solution, a high-performance centralised IDS that processes all the network traffic from the different networks, is a considerable option. However, it's important to note that this solution cannot guarantee the isolation of the networks, and the unique features of the networks are crucial from an anomaly detection perspective.

3.3.2 Network Topology

A ship may have multiple distinct networks, each serving a specific function. Visky et al. in [39] identified the following networks on a passenger ferry.

- **The administrative network**, a tree topology structure on the ship that is connected to the company's virtual private network (VPN), serves multiple functions. It ensures continuous communication with the headquarters, supports administrative tasks such as status reporting and map update downloads, and offers a monitored internet connection for administrative use.
  The network is consistently connected via WiFi at ports, and during voyages, it connects over 4G or 5G mobile networks whenever the service is available. Satellite communication is not utilised for this purpose.
- **The navigational network** is a partially isolated system that connects navigation-related devices such as Electronic Chart Display and Information Systems (ECDIS), Integrated Navigation Systems (INSs), Multi-Functional Displays (MFDs), Data Collector Units (DCUs), and RADAR. This network operates with a redundant ring topology and receives propulsion-related data from the Propulsion Control Network through a one-way connection.
- **The propulsion control network** is a partially isolated, redundant system that facilitates communication between the bridge and the propulsion automation. The passenger ferry's propulsion can be operated in fully manual mode, allowing control of propulsion and direction via physical switches in the engine room during emergencies. This network transmits propulsion-related data to the Navigational Network through a one-way connection.
- **The Cargo Handling Network** is an isolated system of wired and wireless devices. It supports cargo handling and administration activities. Cargo-related

data sent from the shore in a specific format is imported into the offline cargo management system.
- **The public WiFi network** is an isolated system specifically designed to provide internet access to passengers through a dedicated WiFi infrastructure. This network ensures a seamless online experience for passengers while onboard. It incorporates advanced network devices that manage user connections, ensuring logical separation to maintain security and privacy.
- **The network for the independent support company** is an isolated system that comprises both wired and wireless connections. It supports the ferry's onboard restaurant operations, facilitating essential functions such as order management, payment processing, and other related services. Being isolated from other networks provides enhanced security and reliability, ensuring that the restaurant can operate independently without interference from other onboard systems.

It is highly recommended that these networks be physically isolated to maintain the highest security standards. If this is the case, each network will need to be monitored individually, making the installation of an IDS more complex.

To adopt the IDS to the above-mentioned requirements, network-related data should be collected in every isolated network and sent to the centralised IDS to ensure comprehensive coverage.

3.4 Sensor Placement

Sensor placement is essential during IDS planning. We conducted a literature survey to identify the most prominent approaches.

According to Noel and Jajodia the optimal sensor placement can be determined by an attack graph analysis [40]. During this procedure, the critical assets and paths through the network can be highlighted along with the prioritization of alerts and effective attack response.

Chen et al. in [41] evaluated the IDS sensor placement to find an optimal trade-off. According to their results, the optimal placement of sensors depends on our main objective. It may be influenced by the attack type, we wish to detect, the price, or the placement of firewalls and servers.

Based on the literature survey, there is no common method for determining the optimal sensor placement. It requires deep knowledge about the actual networks and their topology, as well as the needs and main objectives.

In order to avoid single points of failure and ensure reliable detection, it is crucial to deploy redundant sensors. It involves the use of multiple sensors to monitor the same parameter or condition in different network segments.

This approach increases reliability by making the IDS more failure-resistant: If one sensor fails, others can continue to provide the necessary data, ensuring continuous monitoring and detection. Besides that, it helps with error detection. Redundant sensors can support the cross-validation of the data and indicate a malfunction in one of the sensors.

3.5 Detection Mechanisms

3.5.1 Signature-Based Detection

One of the two primary methods an IDS uses to detect intrusion is the signature-based or misuse detection. This type of IDS is particularly effective because most attacks have unique signatures that can be identified. The simplicity and practicality of this method lie in its straightforward process-learning to specify a pattern and deciding which patterns should trigger the IDS.

Signature-based IDSs operate using rule sets, which are files containing a defined traffic pattern that triggers a specified reaction. These rules are crucial as they can contain a variety of patterns, from previous attack sequences to known system vulnerabilities, that can trigger the IDS's reaction.

Each intrusion triggers unique reactions, such as denied access to a file or directory, failed login attempts, failed attempts to run an application, etc. These unique patterns are then used to detect and alert when a similar attack is happening in the future. Data is collected from different places, such as network traffic, particular resource usage, number of requests from the same IP, etc. After this data is collected and analysed, it could be added to the knowledge base for future uses.

Some advantages of such an IDS include easier detection of attacks if the signatures are well known. In modern systems, pattern matching is optimised, making it effective and quick. Such systems are versatile, and rules might be easier to understand compared to anomaly baselines. On the other hand, the collection of signatures must be constantly updated. It is possible that a signature-based IDS fails to identify unique attacks. Rules may be redundant and use up computational resources to calculate an already evaluated result in a different way. [42, 43]

3.5.2 Anomaly-Based Detection

The other section of IDSs based on how they detect intrusions is the anomaly-based IDSs. Their techniques are fundamentally different from signature-based IDSs, so their usage differs greatly. Their perspective is opposite to the signature-based variants. They do not monitor the individual packets one by one, but instead, they compare their behaviour to a standard pattern, and if that differs, it gets classified as an anomaly.

Unlike signature-based versions, anomaly-based IDSs do not rely on rule sets. Instead, they adapt to the system's behaviour profile, which defines normal activities. This adaptability ensures that any significant deviation from the norm triggers the necessary countermeasures, reinforcing their effectiveness.

The IDS refers to a behaviour profile that defines the normal behaviour of the system. Any variation from the normal will trigger alarms. This version can detect zero-day exploits. Anomaly detection can be done during run time or later down the line. Like AIDSs, anomaly-based IDSs are great against protocol or port missuses, detecting DoS attacks with crafted IP packets and other network or resource failures

[44]. Attacks without known signatures are also detectable, like new worms or viruses.

The advantages of anomaly-based IDSs are significant. They can detect new versions of attacks that lack known fingerprints, instilling confidence in their ability to keep systems secure. As time passes, behaviour profiles can become more advanced, and custom profiles for different networks and applications can be created to detect unique system attacks. However, it might be hard to understand and make a profile. It is challenging to find the boundary between normal and abnormal behaviour. All protocols analysed must be well defined and tested for accuracy; otherwise, malicious behaviour might be associated with normal behaviour. [42–44]

3.6 Data Collection, Storage, and Analysis

The sheer volume of data generated by IDSs necessitates significant storage capacity and advanced data management solutions to handle the influx efficiently. Furthermore, the urgency and importance of the work in threat detection is underscored by the need for real-time analysis. This involves sophisticated algorithms and substantial computational resources, and the need for high-speed processing capabilities and low-latency data handling. The diverse nature of data types collected, ranging from network traffic logs to application-specific information, further highlights the need for versatile analytical tools and methodologies.

Implementing robust log management practices for storing and analyzing IDS logs involves several steps to ensure efficient storage, timely analysis, and comprehensive security monitoring.

To simplify data management and analysis, a central data server should be deployed to collect data from various IDS sensors across the network. The data should be collected in standardized formats (e.g., JSON, syslog) to ensure consistency and facilitate easier parsing and analysis.

Data storage should be scalable. Depending on the network's characteristics, the amount and generation speed of the data can vary. Modern, scalable storage solutions such as cloud storage or distributed file systems (e.g., Hadoop HDFS) can handle large volumes of log data, but on ships, the limited external communication capacity restricts the applicable technologies.

The volume of the data also involves data retention policies based on compliance requirements and business needs. To use the storage capacities optimally, it is worth moving older logs to less expensive storage options.

Different IDSs and other data sources may send the logs in different formats, which needs log parsing and normalization. During this process, the logs are transferred into a common format, making them easier to analyze. The collected data should be indexed to enable quick and efficient querying.

To improve the IDS's sensitivity, log data should be enriched with contextual information such as geolocation, threat intelligence feeds, and asset data. This method can enhance data analysis and incident response.

The collected logs should be integrated with a Security Information and Event Management (SIEM) system for real-time monitoring, correlation, and analysis.

3.7 Alerting and Response

Once a potential security threat or anomaly is detected, to reduce the impact and damages an IDS should trigger alerts for the responsive system and associated security personnel.

During the critical initial detection phase, the IDS diligently monitors network traffic or system activities to identify any suspicious behaviour, such as unusual login attempts, abnormal data transfers, or known attack signatures. This is where your expertise comes into play. When a potential threat is detected, the IDS generates an alert, providing details such as the type of anomaly detected, the source and destination IP addresses, timestamps, and other relevant metadata. The IDS should correlate multiple alerts to identify patterns that indicate a larger, coordinated attack. Your role in this phase is crucial, as it reduces the likelihood of false positives and helps in understanding the full scope of the threat.

Since the response process is crucial for mitigating the impact of an intrusion, minimising damage, and protecting the organisation's assets, alerts must be escalated based on their severity. Predefined incident response protocols should be defined to minimise the delay and maximise the efficiency of the action taken.

These actions must consist of initial triage, in which a responsible personnel or automated system reviews the alert to determine its validity and assess the potential impact. This may involve automated log or network traffic analysis. If a higher level of action is needed, such as a manual log or network traffic analysis or forensic tools to gather more information, a cyber security analyst must be involved.

Depending on the threat, immediate actions must be taken to contain the intrusion, such as isolating affected systems, blocking malicious IP addresses, or disabling compromised accounts. Longer-term mitigation strategies might include applying patches, re-configuring firewalls, or enhancing security policies to prevent similar incidents in the future.

After containment, efforts focus on restoring normal operations. This might involve cleaning up malware, restoring data from backups, or repairing damaged systems. These actions need deep IT knowledge and cannot be done as a remote operation. During the process —to prevent recurrence— additional controls or changes should be implemented, such as improving monitoring, updating IDS rules, or conducting staff training.

In summary, the alerting and response in an IDS is a multi-step process that involves detecting threats, generating alerts, investigating and containing incidents, and finally recovering from and learning from the event. A well-designed alerting and response system is essential for maintaining the security and integrity of an organization's network and systems.

3.8 Testing and Validation

The performance of the detection and alerting system should be validated through a series of comprehensive tests. These tests should encompass the entire environment and evaluate not only the accuracy of anomaly detection but also the effectiveness of the system's response.

3.8.1 Performance Analysis and Detection Testing

Several methods can be used to test and validate IDSs. Each method provides insights into different aspects of the IDS, ensuring its effectiveness across a range of scenarios.

The IDS's ability to differentiate between normal and abnormal traffic patterns is a key function in maintaining network security. This is tested through traffic analysis and anomaly detection, where normal and abnormal traffic patterns are introduced into the network to see how the IDS performs. This process can be conducted with publicly available datasets.

- **KDD Cup 99** [45]: One of the most well-known datasets for intrusion detection, which contains labelled data for different types of network attacks and normal traffic. According to Tavallaee et al., it suffers deficiencies: the dataset contains a huge number of redundant records, and they appear in the training and test set as well. It makes the classifiers biased, causing a high classification rate [46].
- **NSL-KDD** [47]: An improved version of KDD Cup 99, which focuses on attack and normal traffic. It does not suffer from any of the mentioned problems. Furthermore, the number of records in the train and test sets is reasonable, allowing the experiments to be run on the complete set without the need to randomly select a small portion [46].
- **CICIDS 2017** [48]: The dataset contains benign and common attacks, which resemble real-world data. It includes 86 network-related features that also contain IP addresses and attack types. It also includes the results of the network traffic analysis: flows labelled based on many features, along with their definition.
- **UNSW-NB15** [49]: This dataset includes normal traffic and nine types of attacks namely, Backdoors, Fuzzers, DoS, Analysis, Generic, Exploits, Worms, Reconnaissance and Shellcode [50].

The common characteristic of the above-mentioned datasets is that they aim to improve IDSs, focusing mainly on IT but not OT systems. Another shortcoming is the lack of maritime-related data.

Visky et al. published the MarCyb dataset that contains benign and attacks in ship OT networks [51]. Along with the common attacks, such as Address Resolution Protocol (ARP) spoofing and DoS, this dataset contains attacks against navigation systems, like Electronic Chart Display and Information System (ECDIS) and Global Positioning System (GPS). Furthermore there are attacks against the navigation process, like man overboard flooding, collision alerts, and logically invalid data encoding.

The performance analysis result shows the rate of false positives (benign events flagged as threats) and false negatives (actual threats missed by the IDS).

3.8.2 Penetration Testing

Penetration testing is a method used to evaluate the security of a computer system, network, or web application by simulating an attack from malicious outsiders or insiders. The goal is to identify vulnerabilities that could be exploited by attackers, assess the effectiveness of the defences in place, and recommend improvements [52]. This helps identify how well the IDS detects real-world attacks.

The process begins with a crucial phase, the reconnaissance. This step is instrumental in understanding the target system and defining the scope of the test. It provides vital information about the target, such as domain names, IP addresses, network topology, and any public-facing services or applications. This comprehensive understanding allows for the creation of a detailed plan that outlines the targets, methods, and schedule for the penetration test, ensuring you are fully prepared for the task at hand.

The next step in the process is the scanning phase, a proactive measure to identify potential entry points and vulnerabilities in the target system. Automated tools like Nmap [53] and Nessus [54] can scan the network for open ports, running services, and potential vulnerabilities, such as outdated software, misconfigurations, or unpatched vulnerabilities. This vigilance is key to staying ahead of potential threats.

Exploitation of the identified vulnerabilities gives unauthorized access to the system. This process uses tools like Metasploit [55] or other cybersecurity frameworks to simulate various attack scenarios, such as SQL injections, DDoS attacks, or malware infections.

The successful attack demonstrates the system's weakness and gives the attacker the opportunity to deploy a backdoor, create hidden user accounts, or install malware to ensure continued access even if the initial vulnerability is patched. Establishing this foothold helps the attacker maintain access, monitor the system, and attempt to move laterally within the network to access more sensitive areas or data.

The activity's result is a report that includes the penetration test's findings and provides actionable recommendations. The detailed report outlines the vulnerabilities discovered, the methods used to exploit them, and the potential impact of each vulnerability.

3.9 Maintenance and Updates

Maintenance and updates for an IDS are crucial to ensuring that the system functions effectively in detecting and responding to potential threats. The tasks involved can be broken down into several key areas.

Maintaining up-to-date signature databases is essential for signature-based IDS. New threats and vulnerabilities emerge regularly, so the IDS needs regular updates to recognize these new patterns. Creating and refining custom rules specific to the organisation's environment can improve the accuracy of the IDS and reduce false positives.

System software and firmware updates include the IDS software and its underlying operating system or firmware to ensure they have the latest security patches and enhancements. This helps to protect the IDS itself from vulnerabilities. This process covers the implementation of new features and improvements provided by the IDS vendor that can enhance detection capabilities, performance, or usability.

Response procedures also should be updated based on the latest threats and the IDS's capabilities to ensure the most efficient incident response processes.

During regular maintenance, the IDS can be fine-tuned to maximise its sensitivity and minimise false positives. Revision of the IDS logs helps this process, by trend, repeated false positives, or new types of suspicious activity identification. The fine-tuning can involve the modification of thresholds, rules, or response actions.

Logs, configuration files, and other critical IDS data should be archived regularly to support incident response, disaster recovery, or forensics activity in the future. Maintaining the incident response plan, including regular testing of backup procedures, is also essential to quickly restore IDS functionality in case of failure.

Continuously monitoring the IDS to ensure it is operating correctly. This includes checking that sensors are functional, the network connection is stable, and the IDS is correctly logging and alerting. Besides that, during the maintenance, the IDS testing ensures that it correctly detects known threats. This could involve running simulations or using test signatures.

4 Conclusion and Future Work

4.1 Summary

In our literature analysis we found results that highlights the usability of the open-source IDSs on ships, but we did not find any that introduces a concept with all the technical aspects to fertilise the development and integration such a system into marine vehicles.

In our research we reviewed the existing literature to answer this need, collected and introduced the relevant challenges. We highlighted many aspect to be considered.

4.2 Main findings

The ship usually needs IT or cyber security experts, so the alerts must be handled by non-expert personnel, or they could be managed from the shore, which makes the situation difficult because of the limited communication bandwidth.

Since the ship has limited or no IT experts on board, the crew should clearly know if they can start or carry on the mission in the given cyber situation or, if they can't, how they can mitigate the problem.

The effectiveness of the IDS depends on its accuracy —the ability to detect real threats accurately while minimising false positives— and speed of detection, which can be increased by an automated response process. While it can speed up the response process, certain alerts may require human analysis to understand and respond to the threat fully.

Effective response to cyber threats requires a well-coordinated system. This involves the IDS, other security tools (e.g., firewalls, SIEM systems), and the security team working together. Integration and communication are key to this well-organised and efficient system.

All these findings should be held in the forehead during the design of an IDS.

4.3 Limitation and Future Work

Our research was limited to the technical aspects. However, the administrative, human-related, financial and legal aspects also need to be examined, which we plan to do in future work.

Acknowledgements This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

References

1. S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the internet of things: A comprehensive investigation," *Computer Networks*, vol. 160, p. 165–191, Sep. 2019. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2019.05.014
2. M. Alkasassbeh and S. Al-Haj Baddar, "Intrusion detection systems: A state-of-the-art taxonomy and survey," *Arabian Journal for Science and Engineering*, vol. 48, no. 8, p. 10021–10064, Nov. 2022. [Online]. Available: http://dx.doi.org/10.1007/s13369-022-07412-1
3. A. S. Ashoor and S. Gore, "Importance of intrusion detection system (ids)," *International Journal of Scientific and Engineering Research*, vol. 2, no. 1, pp. 1–4, 2011.
4. M. Pihelgas, "A comparative analysis of open-source intrusion detection systems," *Tallinn: Tallinn University of Technology & University of Tartu*, 2012.
5. H. N. Psaraftis, *The Future of Maritime Transport*. Elsevier, 2021, p. 535–539. [Online]. Available: http://dx.doi.org/10.1016/b978-0-08-102671-7.10479-8

6. M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean &; Coastal Management*, vol. 236, p. 106493, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1016/j.ocecoaman.2023.106493
7. E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166
8. V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100571, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555
9. M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22
10. "Maritime cyber security," https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/, 06 2022, (undefined 7/4/2024 13:20).
11. "Introduction cooperation on maritime cybersecurity atlantic council," https://www.atlanticouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/, 10 2021, (undefined 7/4/2024 13:22).
12. "Maritime cyber resilience prosjektbanken," https://prosjektbanken.forskningsradet.no/project/FORISS/295077, (undefined 7/4/2024 13:29).
13. "Maricybera," https://maricybera.taltech.ee/, 04 2021, (undefined 7/4/2024 13:30).
14. G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime cyber threats detection framework: Building capabilities," in *Information Security Education - Adapting to the Fourth Industrial Revolution*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds. Cham: Springer International Publishing, 2022, pp. 107–129.
15. O. Jacq, D. Brosset, Y. Kermarrec, and J. Simonin, "Cyber attacks real time detection: towards a cyber situational awareness for naval systems," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, Jun. 2019. [Online]. Available: http://dx.doi.org/10.1109/CyberSA.2019.8899351
16. A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104
17. G. Visky, D. Khisteva, R. Vaarandi, and O. M. Maennel, "Towards an open-source intrusion detection system integration into marine vehicles," in *2024 66th International Symposium ELMAR (ELMAR)*, 2024.
18. N. Gupta, V. Jindal, and P. Bedi, "A survey on intrusion detection and prevention systems," *SN Comput. Sci.*, vol. 4, no. 5, Jun. 2023.
19. O. Schell, J. P. Reinhard, M. Kneib, and M. Ring, "Assessment of current intrusion detection system concepts for intra-vehicle communication," in *INFORMATIK 2020*. Gesellschaft für Informatik, Bonn, 2021, pp. 875–882.
20. S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, vol. 195, pp. 346–361, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366422003516
21. M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2021. [Online]. Available: https://books.google.ee/books?id=Hwk1EAAAQBAJ
22. A. Shostack, *Threat modeling*. Nashville, TN: John Wiley & Sons, Feb. 2014.
23. J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamillaand, and A. M. Satyam, *Improving Web Application Security*. Microsoft Corporation, 2003. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330
24. K. Tam and K. D. Jones, "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping," *Journal of Cyber Policy*, vol. 3, no. 2, p. 147–164, May 2018. [Online]. Available: http://dx.doi.org/10.1080/23738871.2018.1513053

25. I. M. O. (IMO), "Msc-fal.1-circ.3 - guidelines on maritime cyber risk management," 7 2017, [Accessed: 15-11-2020].
26. ——, "Msc-fal.1/circ.3/rev.2 - guidelines on maritime cyber risk management," 6 2022, [Accessed: 11/04/2024].
27. International Maritime Organization, "Resolution msc.428(98) - maritime cyber risk management in safety management systems," 7 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.
28. B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *Journal of Navigation*, vol. 72, no. 5, p. 1108–1120, Feb. 2019. [Online]. Available: http://dx.doi.org/10.1017/S0373463318001157
29. "General data protection regulation (gdpr) – legal text," https://gdpr-info.eu/, (Accessed on 08/16/2024).
30. "California consumer privacy act (ccpa) — state of california - department of justice - office of the attorney general," https://oag.ca.gov/privacy/ccpa, (Accessed on 08/16/2024).
31. "Next-generation firewalls - palo alto networks," https://www.paloaltonetworks.com/network-security/next-generation-firewall, (Accessed on 04/21/2024).
32. "Mdr solutions & services from alert logic," https://www.alertlogic.com/managed-detection-and-response/, (Accessed on 04/21/2024).
33. "Cisco secure firewall - cisco," https://www.cisco.com/site/ca/en/products/security/firewalls/index.html, (Accessed on 04/21/2024).
34. "Apiiro — secure your development and delivery to the cloud," https://apiiro.com/, (Accessed on 04/21/2024).
35. A. Alhomoud, R. Munir, J. P. Disso, I. Awan, and A. Al-Dhelaan, "Performance evaluation study of intrusion detection systems," *Procedia Computer Science*, vol. 5, pp. 173–180, 2011, the 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011) / The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050911003498
36. A. Harbola, J. Harbola, and K. S. Vaisla, "Improved intrusion detection in ddos applying feature selection using rank; score of attributes in kdd-99 data set," in *2014 International Conference on Computational Intelligence and Communication Networks*. IEEE, Nov. 2014. [Online]. Available: http://dx.doi.org/10.1109/CICN.2014.179
37. A. Gul and E. Adali, "A feature selection algorithm for ids," in *2017 International Conference on Computer Science and Engineering (UBMK)*. IEEE, Oct. 2017. [Online]. Available: http://dx.doi.org/10.1109/UBMK.2017.8093538
38. "Nsl-kdd — datasets — research — canadian institute for cybersecurity — unb," https://www.unb.ca/cic/datasets/nsl.html, (Accessed on 07/24/2024).
39. A. Balint, R. Vaarandi, M. Pihelgas, and O. Maennel, "Open source intrusion detection systems' performance analysis under resource constraints," in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, 2024.
40. S. Noel and S. Jajodia, "Attack graphs for sensor placement, alert prioritization, and attack response," 01 2007.
41. H. Chen, J. A. Clark, S. A. Shaikh, H. Chivers, and P. Nobles, "Optimising ids sensor placement," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 315–320.
42. S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, "A survey on anomaly based host intrusion detection system," in *Journal of Physics: Conference Series*, vol. 1000, no. 1. IOP Publishing, 2018, p. 012049.
43. R. Kumar and D. Sharma, "Hyint: Signature-anomaly intrusion detection system," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018, pp. 1–7.
44. K. KR and A. Indra, "Intrusion detection tools and techniques–a survey'," *International Journal of Computer Theory and Engineering*, vol. 2, no. 6, p. 901, 2010.

45. “Kdd cup 1999 data,” https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, (Accessed on 08/10/2024).
46. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the kdd cup 99 data set,” in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6.
47. “Github - hoanp/nsl-kdd-dataset,” https://github.com/HoaNP/NSL-KDD-DataSet, (Accessed on 08/10/2024).
48. “Cicids2017 dataset — papers with code,” https://paperswithcode.com/dataset/cicids2017, (Accessed on 08/10/2024).
49. “The unsw-nb15 dataset — unsw research,” https://research.unsw.edu.au/projects/unsw-nb15-dataset, (Accessed on 08/10/2024).
50. N. Moustafa, “Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic,” Ph.D. dissertation, The University of New South Wales, 2017. [Online]. Available: http://hdl.handle.net/1959.4/58748
51. G. Visky, A. Šiganov, U. R. Muaan, R. Varandi, H. Bahsi, and L. Tsiopoulos, “Marcyb dataset,” 2024. [Online]. Available: https://data.taltech.ee/doi/10.48726/00fa9-5xv20
52. M. Bishop, “About penetration testing,” *IEEE Security & Privacy*, vol. 5, no. 6, pp. 84–87, 2007.
53. “Nmap: the network mapper - free security scanner,” https://nmap.org/, (Accessed on 08/10/2024).
54. “Download tenable nessus — tenable®,” https://www.tenable.com/downloads/nessus?loginAttempted=true, (Accessed on 08/10/2024).
55. “Metasploit — penetration testing software, pen testing security — metasploit,” https://www.metasploit.com/, (Accessed on 08/10/2024).

Appendix 6

Publication VI
G. Visky, A. Rohl, R. Vaarandi, S. Katsikas, and O. M. Maennel. Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639746

Hacking on the High Seas: How Automated Reverse-Engineering Can Assist Vulnerability Discovery of a Proprietary Communication Protocol

Gabor Visky[1], Alexander Rohl[2], Risto Vaarandi[1], Sokratis Katsikas[3], and Olaf M. Maennel[2]

[1]Tallinn University of Technology, Tallinn, Estonia
[2]The University of Adelaide, Adelaide, Australia
[3]Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
Email:gabor.visky@taltech.ee, alexander.rohl@adelaide.edu.au, risto.vaarandi@taltech.ee
sokratis.katsikas@ntnu.no, olaf.maennel@adelaide.edu.au

***Abstract*—The digitalisation of the world is a global trend affecting many industries, including the maritime transport sector. Electronic navigational equipment aboard modern ships has undoubtedly decreased naval accidents, but these devices may suffer from cybersecurity vulnerabilities. One such vector, is its reliance on a great number of protocols for communication. Currently there is limited awareness of the security strengths and weaknesses of maritime protocols, because of the manual-reverse-engineering cost due to their proprietary nature. However, we substantiate that advances in automated protocol reverse-engineering are effectively lowering this cost. Our paper analyses a proprietary protocol, widely used in naval equipment. This protocol was reverse engineered through manual and automated techniques, revealing the advantages and drawbacks of both. Our results show that statistical automated protocol reverse-engineering techniques were sufficient to discover the relevant protocol fields. We introduce the disclosed communication structure and its vulnerabilities, which are both verified by the success of rudimentary attacks. The disclosed protocol, by manual and automated techniques, could also aid intrusion detection (and prevention) system development for maritime operational technology systems, to help vendors avoid the identified vulnerabilities during system design and implementation.**

***Index Terms*—cyber security, proprietary protocols, maritime, automated protocol reverse-engineering, navigation**

I. Introduction

Cyber security threats in the maritime industry are rising rapidly; between February and June 2020, the sector suffered a 400% increase in attempted malicious activities [1]. Gartner forecasts that cybercriminals will progressively weaponise industrial control systems (ICSs) this decade to potentially cause harm to life and the environment [2]. Adding to this challenge, ICS vulnerabilities saw an increase of 27% in 2022, while 77% of vulnerabilities lack any attempt of mitigation [3]. Electronic navigation equipment aboard modern ships have undoubtedly increased maritime safety over the years [4], but they share many commonalities with ICSs and are susceptible to cyber vulnerabilities [5], [6]. Meland et al. [7] introduce 46 maritime-related cyber incidents. In particular, such attacks pose a significant threat to the growing automation capability of modern ships, as the required complexity of onboard networks and their communication protocols, are now a *mission-critical* component [8]. One third of the incidents related to OT systems.

Vendors rely on proprietary communication protocols to develop networked devices. During this process, they aim to find a trade-off between meeting the industry's needs and minimising the protocol's complexity, often without cyber security considerations [8]. The main reason for protocol development is to optimise the product's communication performance. To defend the market share, the communication specifications are not publicly available; the protocol is kept closed. To decrease the attack surface of onboard control systems, the security of network services and protocols is essential because a flaw in communications could lead to system-wide vulnerabilities. To help developers with this task and ensure interoperability, a rigorous standardisation process is in place, which *should* also consider security. However, this is not always the case, and communication protocols used aboard ships have cyber-security flaws. This paper puts the focus on a proprietary protocol used in navigation systems composed of Electronic Chart Display and Information Systems (ECDISs), Integrated Navigation Systems (INSs), Multi-Functional Displays (MFDs) and Data Collector Units (DCUs) [9].

Because of the limited crew aboard a ship, there is often no room for cyber or IT experts, so sailors must fix control systems by replacing the corrupted unit from spares kept onboard. This method, particularly when spares are limited, requires devices with minimal configuration so they are easy to install, which makes it challenging to introduce various security measures. For example, the unique identifier of the actual network devices (media access control address) cannot be registered into a network end-point protection solution (to avoid using unregistered devices) because the spare part's unique identifier is often unknown before troubleshooting.

This limitation can be overcome with intrusion detection systems (IDSs) or intrusion prevention systems (IPSs), which are installed during ship manufacture or scheduled mainte-

nance, to indicate anomalies and alert the crew. Our discovered detailed knowledge of the communication protocol is needed for the development of an IDS/IPS [10].

This paper demonstrates how statistical automated protocol reverse-engineering (APRE) techniques can assist security researchers in the reverse-engineering process when analysing a proprietary communication protocol. As a result of our reverse engineering effort, we disclose details of the protocol structure, as verified by demonstrating various attacks.

This paper's contributions are the publication of the reverse-engineered closed-protocol structure to help vendors with defence development, and the demonstration of APRE on this maritime protocol. Further more, it discusses the efficiency comparison of automated and manual reverse-engineering, and brings examples of the protocol's vulnerabilities and methods of exploitation.

II. Background

A. Onboard Communication Protocols

ICSs are required to monitor industrial processes such as logistics, manufacturing, or transportation. Real-time response, high availability and reliability are the key requirements of these systems. Different industries often have unique, sector-specific protocols to fulfil these requirements.

The National Marine Electronics Association (NMEA) is a worldwide organization that focuses on marine electronics interface standards to enhance their technology and safety. To explain the evolution of a maritime protocol's standardisation, this section will introduce the NMEA-0183 protocol and a proprietary protocol that relies on NMEA-0183.

1) NMEA-0183: In the early 80s, the NMEA issued their NMEA-0183 standard, which defines the interfacing between various marine electronic equipment and navigational computers, allowing them to share vital information [11]. NMEA-0183 evolved from earlier NMEA standards (-0180 and -0182) and is based on the serial communication protocol standard RS422 (Standard EIA-422-A). This underlying protocol supports data exchange between one talker and up to 10 listeners. The data exchange used 7-bit ASCII-encoded *sentences*, up to 82 characters long [12].

2) IEC61162-1 Protocol: In 1997, NMEA-0183 v.1.5 was translated into the international industrial standard IEC61162-1. The most commonly used communication protocols in navigation follow the IEC61162 standard, a collection of International Electrotechnical Commission (IEC) standards for "digital interfaces for navigational equipment within a ship" [13]. Several standard versions were published during the IEC61162's long evolution. While the IEC61162-1 protocol is designed to work over serial lines, its gradual development led to protocols that operate over Ethernet, such as OneNet, which provides a standard method for sharing NMEA-2000 data over a Local Area Network (LAN).

3) A Proprietary Protocol: Vendors often develop devices with a proprietary, closed communication protocol to keep their specifications secret in an attempt to provide security. However, it is common knowledge in the security community that "security by obscurity" is poor practice [14]. In our work, we manually reverse-engineered a proprietary protocol developed by a leading maritime market vendor, who requested anonymity, and we show that automated reverse-engineering methods can remove this technical barrier entirely.

III. Related Work

In our literature survey, in different digital libraries we searched for publications from the last 25 years that contain "cyber" AND "navigation" AND "maritime" keywords together. Despite the large volume of publications, this condition did not provide sufficient results assessing the low-level security of the protocols used by the navigational equipment onboard ships. To find a suitable field of related work, and provide a stronger overview of the state of the art, we shifted our criteria to include ICS security for any industrial sector.

A. Protocol Security

The research community shared results focusing on vulnerabilities and weaknesses in existing navigational equipment, tracking and monitoring systems [15]–[18]. These publications discuss external communication weaknesses rather than those linked to onboard communications. To address this gap, Frøystad et al. in [19] offer a Public Key Infrastructure (PKI) design to improve the cyber security of digital communication in the maritime sector. This solution brings trustworthy communication to the industry but does not aim to defend onboard communication. Baltic Marine Environment Protection Commission [20] focuses on a modern onboard communication protocol (IEC61162-450) and offers an extension that could improve the resilience of the ships' navigational systems. Although the paper focuses on the automatic identification system (AIS) data interface, the recommended measures may improve the overall security of the protocol. However, the paper does not evaluate the general shortcomings of the protocol.

In the ICS context, Drias et al. in [21] introduce an attack taxonomy model focusing on the Modbus and Distributed Network Protocol 3 (DNP3) protocols, to evaluate several attack types that can harm ICSs. Although DNP3 is most commonly used in the power industry, Modbus is also widely used onboard ships. Xu et al. in [22] introduce several protocols and their cyber vulnerabilities in the power industry. These works shed light on the weaknesses of ICS protocols (also used on ships) in the context of power-generation systems, rather than for navigation. That is why we focus on navigational networks and protocols, since similar vulnerabilities may have different consequences for maritime safety.

Although cyber security in the maritime domain is in focus, the cyber weaknesses of the onboard communication protocols have received little attention. The reason may originate from ships being considered isolated systems with minimal attack surface. This assumption creates a false sense of security. However, when the ship is in harbour during maintenance, the onboard control systems may be connected to other networks and devices, or interacted by unauthorised personnel,

accidentally or *on purpose*. Furthermore, the crew is likely to change throughout the lifetime of a vessel; so any previous crew member could leave behind a malicious payload.

Although new vessels are equipped with advanced automation systems to improve safety and efficiency, these systems often introduce cyber weaknesses [5], [6]. This modernisation of ships highlights the importance of maritime protocol research. Our paper addresses this problem by introducing a navigational onboard communication protocol and its susceptibility to different cyber attacks.

B. Automated Protocol Reverse-Engineering

Protocol reverse engineering is a tedious process when performed manually, so automated methods are required; especially if a protocol is indefinitely updated. There exists no evaluation of the application of APRE techniques to maritime protocols, however numerous studies evaluate their application to *land*-vehicle Control Area Network (CAN) bus protocols [23]–[25]. Yu et al. use genetic programming to find rules that correlate integer bytes with values found in the output of a vehicle diagnostics application [23]. A limitation of their approach is that it relies on fields having a byte-divisible length, and the endianness is known. Verma et al. propose a modular four-stage pipeline, *CAN-D*, that infers the field boundaries, endianness, signedness and physical interpretation for each CAN message type using linear regression [24]. Both approaches rely on a ground-truth signal generated by the vehicle's diagnostic protocol. However, maritime components do not transmit an open diagnostic protocol. Hence, in our application of linear regression to infer bits correlated with values of interest, we assume that ground-truth signals can instead be acquired from an external device, such as a GPS, or from captured metadata, such as timestamp and packet length.

The majority of existing APRE techniques have been evaluated on traditional IT protocol, such as for file sharing, which may not necessarily translate to maritime protocols. For some techniques, authors have released code (Nemesys [26] and NetPlier [27]). However, these techniques only infer field boundaries, but we require syntax and semantic information for our security research. Advances in APRE have used deep-learning methods to infer field semantics, however code is not provided [28], [29]. In particular, our APRE method shows that basic statistical techniques, with some contextual information, are sufficient to generate desired outputs.

IV. Method

A. Research environment

Using a unique environment designed for maritime cybersecurity research [30], we generated network traffic, recorded it for analysis and addressed our attacks, as depicted in Figure 1. During the simulator-generated network-traffic capture, the packets and the MFD (showing ECDIS and RADAR screens) are identical with those used on ships to transfer and display navigation related data, respectively.

These packets were collected, filtered (based on the IP address and port of the MFD) and analysed, to facilitate reverse engineering and consequently modified for protocol attacks to be launched by the researcher's computer in Figure 1.

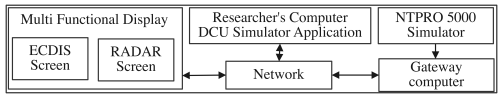


Figure 1. Logical schema of the research environment for the proprietary protocol.

B. DCU Simulator Application

Since the proprietary protocol relies on the Transmission Control Protocol (TCP) and the DCU acts as a server that sends TCP-push packets in this architecture, we developed a tool to conduct replay and injection attacks. This tool (available on request) waits for a connection request on the regular port used by the DCU (TCP/50019). When the connection is established by the MFD, an initialisation procedure starts, in which our software replays the relevant answers extracted from previously recorded and processed communication. Next, the tool starts reading packet payloads from a file, extending them with the vendor-specific header (Section VI-A) and sends them as TCP-push packets to the MFD. The tool allowed us to examine the system's response to the modified payloads.

C. Protocol Reverse Engineering

A possible way to discover details of an unknown communication protocol is to perform reverse engineering by extracting the application-level protocol used by a product and inferring the protocol's specification. These details are essential for many network security applications [31], [32]. Our work applies this approach to find the details of the introduced proprietary protocol; since technical descriptions, white papers, and blogs are unavailable. The fields of the proprietary protocol were identified by *manually reverse engineering* the transferred data. During this procedure, network traffic between the DCU and the MFD was analysed with a special focus on the vendor-specific header. The functions and formats of the different fields within the header are inferred based on careful visual inspection of each byte's behaviour over time. Our findings are introduced in Section VI-A. Protocol reverse engineering is known as a challenging task and the manual approach of "eyeballing" packet bytes tends to be tedious, time-consuming, and error-prone [33].

In the case of the proprietary protocol, our manual RE required a number of days. Whereas, our statistical APRE approach takes only seconds, and so is a significant time-save.

To demonstrate our APRE approach, in Figure 2, we show that by fitting a linear regression with respect to the bit values and sensor labels ('Heading Values' in Figure 2), when filtered by different *parameter identification/group numbers* (PIDs/PGNs) [34], we have sufficient information to find the location of the interrogated field correlated to the sensor of interest.

Coefficients that did not significantly affect the score when ignored were removed by lasso regularisation. Since the field values do not span the full range of the bits (2^{16} in Figure 2), the regression infers a non-zero intercept and bit 21 is treated as a 'sign' bit. Although, bit 21 is an unsigned field and the true sign bit is at index 16, our inference is sufficient for generating in-distribution values, within the observed sensor range. The payloads corresponding to an incorrect PID will not produce a reasonable correlation (R^2 score $<<$ 1.0) and can be ignored. To finally use our inference to spoof a specific value, we can reconstruct the payload by ordering the weights from highest to lowest magnitude and assigning a '1' if that weight brings us closer to the desired value.

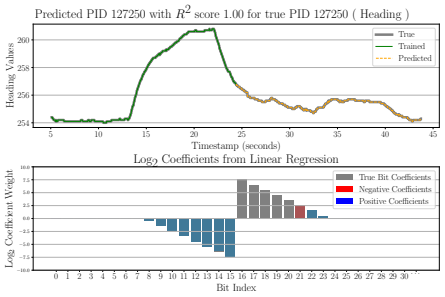


Figure 2. Demonstration of automatically inferring the *Heading* field by looking for the PID with the best correlated payload.

V. Executed Protocol Attacks

The setup of a foothold on a real ship is out of scope, so we assume malicious software or a secretly-installed attacker device can be used to generate the traffic in our attacks.

The discovered protocol specification is required to demonstrate its vulnerabilities. Several threat modelling methodologies, such as the CIA-triad (confidentiality, integrity and availability) [35] and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) [36], provide a framework of various attacks. To cover these categories, we conduct four attacks against the system: replay, injection, modification, and eavesdropping.

A. Replay Attack

This attack is based on retransmission of a previously recorded packet(s). To execute this attack, the relevant packets were filtered out from the network traffic and were retransmitted on the network with Tcpreplay [37]. Because of the underlying TCP protocol, the MFD dropped the replayed packets. This happens because Tcpreplay does not adjust the packet headers before the packets are replayed, and as a result, valid TCP sessions cannot be created [37]. However, we could replay the original IEC61162-1 packets with our self-developed DCU simulator application (Section IV-B) to create valid sessions.

B. Injection Attack

In the case of false data injection, the malicious actor has sufficient protocol knowledge to send false data. Similarly, a spoofing attack is when a person or program successfully identifies as another entity by falsifying data to gain trust [38], [39]. During our experiments, the *sensor values*: wind speed and direction, water depth, heading and turning values were changed to predefined values. Whereas, the *data channel* and *timestamp* were changed with dynamic values. These artificially generated packets were sent to the MFD and it could not detect the attack. There was no warning or other indication of improper behaviour or false value representation.

C. Modification

In the case of a modification attack, the transferred data is caught by the malicious actor, who then modifies and forwards it to the receiver. To analyse this method, an Address Resolution Protocol (ARP)-based Man-In-The-Middle (MITM) attack is executed to pipe the communication over the researcher's computer.

D. Eavesdropping

The protocol transfers the sentences in clear-text format without encryption, making eavesdropping trivial. A successful ARP-level MITM attack was needed to eavesdrop on the communication to address the information disclosure aspect.

VI. Results

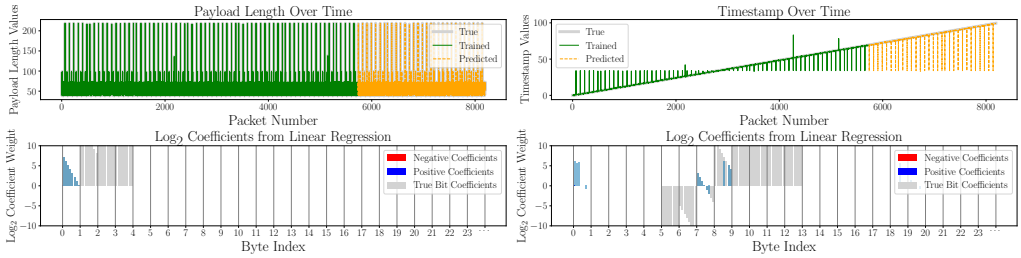
We show our results from manual and automated reverse engineering of the proprietary protocol, as well as the results of the carried-out attacks and their possible consequences.

For data visualisation, a Navi-Sailor 4000 MFD was used, meaning other vendors' products might not be sensitive to the introduced attack. Despite this fact, the vendor-specific protocol enabled the execution of the following attacks against the communication between the DCU and the Navi-Sailor 4000. To execute these attacks, deep knowledge is needed about the protocols that can be gained from the protocol description *(if it exists)*. In our case, reverse engineering of the proprietary protocol was needed to understand the relevant fields and execute the attacks successfully.

A. Manual Reverse Engineering of Proprietary Protocol

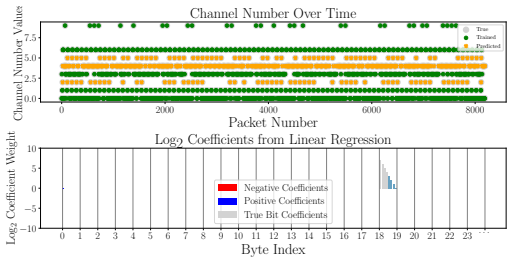
The first part of our contribution is the reverse-engineered details of a proprietary protocol developed by a market-leading vendor in the maritime sector. Its details will be only partly discussed in order to respect commercial confidentiality.[1] In the current application, it is used for data exchange between the MFD and the DCU. The DCU receives the data on its serial ports in IEC61162-1 sentence format and extends the received sentences with a header, as depicted in Table I, to create payloads to be transferred over TCP to the ECDIS.

[1]The company's Product Security Incident Response Team (PSIRT) has been informed about our research and findings to start the Coordinated Vulnerability Exposure procedure.

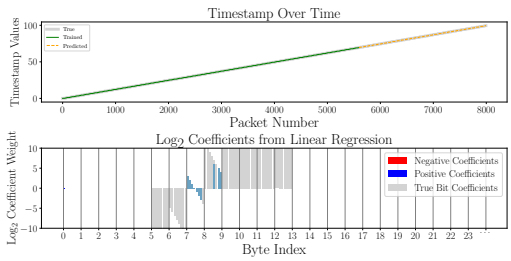


(a) Inferring the *Payload Length* field.

(b) Inferring the *Timestamp* field.



(c) Inferring the *Channel Number* field.



(d) Correcting the *Timestamp* field.

Figure 3. We find which bits of the proprietary packet header had the strongest correlation with the predicted variable. Grey bars indicate where the full field exists and its true coefficients. Blue bars indicate our predicted coefficients of the interrogated field. Timestamps were corrected by removing null values.

Table I
PROPRIETARY COMMUNICATION PACKET STRUCTURE.

Offset	Function	Example value
00	Full length of the payload	44 00 00 00
04	Unknown/static	00
05	Timestamp Continuously increasing value	fe a7 cc 6e 9c 00 00 00
13	Sender's (DCU) IP	0a 8c 21 07
17	Message type	01
18	Channel number arrived	04
19	Length of 61162-1 data	31 00
21	Static	13 00
23	IEC61162-1 data	24 56 4d 2c 0d 0a

The communication consists of two sessions. After the successful communication establishment, a set of system-related information is exchanged, and then the DCU starts sending the data via TCP push packets.

The analysed proprietary protocol embeds structures in the form of IEC61162-1 sentence, so during the reverse engineering, we focused only on the header generated by the DCU, since the rest of the payload is identical to the original messages received on the serial ports.

B. Automated Protocol Reverse-Engineering Results

The manually reverse-engineered protocol header, as seen in Table I, can also be inferred by automated techniques. By training a linear-regression model on the payload bits, we use the packet length to infer the *payload length* in Figure 3a, and *61162-1 data length*. We use the relative packet arrival time to infer the *timestamp* field automatically in Figure 3d, and the *Channel Number* values for the field in Figure 3c. Note that for the timestamp, length, and channel fields, we restrict the bit coefficients in the linear model to be positive, since we expect the field type to be unsigned.

In Figure 3a, we correlate the bits with the packet payload length, which is a known quantity. Since correlating with the payload length resulted in coefficients at byte offset 0, we ignore this byte to find other candidate fields correlated with payload length. By doing so, the linear regression model produced similar weights at byte offset 19 for the *61162-1 data length* field in Figure 4.

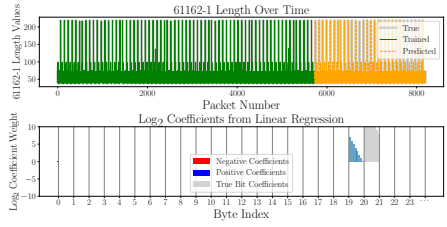


Figure 4. In 3a, we correlate the bits with the packet payload length, which is a known quantity. Since correlating with the payload length resulting in coefficients at byte offset 0, here we ignore this byte to find other candidate fields correlated with payload length. By doing so, the linear regression model produces weights at byte offset 19, correctly inferring the *61162-1 Length* field.

In Figure 3b, we correlate the bits with the timestamp

associated with each packet. In the payload, the timestamp field spans 8 bytes. Linear regression is unable to discern the lower-order bytes (5-6) since these control the millisecond field which is a negligible factor for the regression's cost function. The higher order bytes (9-12) are unexplored in the dataset since the trace spans 100 seconds. In Figure 3d, we correct the timestamp field inference by removing the outliers (packets with zeros in the timestamp field) found in the training set in Figure 3b, such that only packets that do include the timestamp are included in our correlation. The timestamp field contained outliers because the timestamps are zero in the packets sent by the MFD to the DCU, which were included to provide a realistic packet capture. However, these zero-timestamp packets can be found by filtering the relevant source and destination IPs.

To determine the channel number field, we suppose there exists knowledge of which packets belong to a particular channel. In this case, we know which packets belong to channel 0, 1, 3, 6 and 9. This choice is important so that the bits cover the full range of channels (0-9). The linear regression, in Figure 3c, correctly determines the 4 bits and their coefficients to compute the channel number exactly. Hence APRE can infer the *channel number* field, supposing we have sufficient information to know which packets are attributed to a subset of the channels.

Our APRE approach successfully identified the dynamic parts of the messages—length of the payload, NMEA data and the timestamp—and we could infer their values by applying linear regression. The ease of automatic field inference, which took seconds for each field, has clearly lowered the time-cost for security researchers to support manual reverse engineering and, by extension, protocol vulnerability mining. However, APRE techniques struggle to determine static values, such as the proprietary protocol's source IP field. Inferring this field requires prior knowledge of the IP of the device.

In the case of the analysed proprietary protocol, the manual RE required a number of days. In contrast, our elementary APRE approach takes seconds; a significant time-saving.

C. Attacks and Discovered Weaknesses

To demonstrate our success in manual RE we successfully addressed simple attacks (Section V) against an ECDIS by exploiting the protocol weaknesses. All the introduced vulnerabilities below apply to autonomous ships since the same protocols are used there [40]. In extreme cases, when there are no personnel on board to handle an attack, losing communication and control may lead to losing the entire cargo and the vessel. We explain how each attack result affects relevant STRIDE categories.

Spoofing: The replay attack, in which the prerecorded network traffic was used, was successful. The MFD showed the replayed data regardless of the actual sensor value.

The injection attack was successful. The MFD showed the data from the injected packets regardless of the original sensor value. If these packets were injected more than five times a second, they *unnoticeably* suppressed the original sensor values on the MFD. The ECDIS injection attack was also successful; the MFD showed the injected fake AIS targets.

The modification attack was successful. The MFD showed the modified values.

Information Disclosure: The eavesdropping is successful against the protocol, meaning these protocols do not support confidentiality-related security goals.

Denial of Service (DOS): Although this paper focuses on application layer protocols, it is worth mentioning that the analysed proprietary protocol relies on TCP, it still operates with TCP push packets that are not buffered by TCP/IP stack, allowing an attacker to overload the application rapidly. These preconditions make onboard communication unreliable. The sensors or data aggregators cannot check the data's validity and reliability. The same applies to the navigational system without content control: the ECDIS was flooded by packets containing modified sensor values; this can cause DOS because of the above-mentioned reasons.

Summary: Several attacks were successfully executed against the ECDIS by exploiting the proprietary protocol, hence the protocol has limited resistance to cyber-attacks.

VII. Discussion & Further Work

Our objective was to examine the protocol and determine its vulnerabilities against common cyber-attacks. As a result, we shed light on the protocol's weaknesses. We can conclude our results: the analysed protocol have the same shortcomings as many other industrial protocols—it is not designed to resist cyber-attacks.

Although our research directly supports only onboard cyber security, this could affect the overall security of the maritime sector due to its reliance on networked devices for autonomy.

Based on our results we are planning to analyse other maritime related protocols to find their weaknesses, and we plan to share a structured analysis of the attacks and possible ways to avoid them.

VIII. Conclusion

In our paper we analysed a proprietary, application-layer communication protocol used in maritime navigational instruments. This protocol was reverse engineered by manual and automated methods. We demonstrated that APRE can support manual reverse engineering and, by extension, protocol vulnerability mining. Our paper shares the structure of a proprietary protocol which can be used for a third-party IDS/IPS application-level parser development. At the same time our results shed light on the fact that ARPE can support such IDS/IPS development, by automatically inferring the protocol's field boundaries and semantics as necessary. Regarding the proprietary protocol, our paper did not introduce the initialisation part of the communication to respect commercial confidentiality. Still, this limitation does not negatively affect the usability of our results.

Acknowledgment

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

REFERENCES

[1] W. Loomis, *Raising the colors: signaling for cooperation on maritime cybersecurity*. Washington, DC: Atlantic Council, 2021.

[2] M. Susan, "Cyber-Physical Systems Must be Part of Your Security Strategy," 2021. [Online]. Available: https://www.gartner.com/smarterwithgartner/develop-a-security-strategy-for-cyber-physical-systems

[3] Dragos, "Ics/iot cybersecurity, year in review 2022," in *Annual review 2022*. Dragos Inc., 2023.

[4] S.-B. Hong, "A study on the effects of e-navigation on reducing vessel accidents," 2015.

[5] B. Svilicic, 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, 2019. [Online]. Available: https://www.mdpi.com/2077-1312/7/10/364

[6] M. S. Lund, J. E. Gulland, O. S. Hareide, ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. Beijing, China: IEEE, 2018, pp. 1–5.

[7] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, no. 3, pp. 519–530, 2021. [Online]. Available: https://doi.org/10.12716/1001.15.03.04

[8] M. J. C. Ørnulf Jan RØDSETH, "Design challenges and decisions for a new ship data network," 2011.

[9] K. Tran, S. Keene, E. Fretheim, and M. Tsikerdekis, "Marine network protocols and security risks," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 239–251, 2021. [Online]. Available: https://www.mdpi.com/2624-800X/1/2/13

[10] J. Antunes, N. Neves, and P. Verissimo, "Reverse engineering of protocols from network traces," in *2011 18th Working Conference on Reverse Engineering*. Limerick, Ireland: IEEE, 2011, pp. 169–178.

[11] R. Langley, "Nmea 0183: A gps receiver," *GPS world*, vol. 6, no. 7, pp. 54–57, 1995.

[12] N. M. E. Association, "Nmea 0183," National Marine Electronics Association, Standard, 1987.

[13] I. E. Commission, "Iec 61162-1 maritime navigation and radiocommunication equipment and systems - digital interfaces - part 1: Single talker and multiple listeners," in *International Standard*. Geneva, Switzerland: International Electrotechnical Commission, 2002.

[14] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York, NY: John Wiley & Sons, Inc., 2001.

[15] B. M. Thompson, "Gps spoofing and jamming," 2014.

[16] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of ais automated identification system," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 436–445. [Online]. Available: https://doi.org/10.1145/2664243.2664257

[17] A. Grant, P. Williams, N. Ward, and S. Basker, "Gps jamming and the impact on maritime navigation," *Journal of Navigation*, vol. 62, no. 2, p. 173–187, 2009.

[18] M. Pini, L. Pilosu, L. Vesterlund, D. Blanco, F. Lindström, and E. Spaltro, "Robust navigation and communication in the maritime domain: The triton project," in *2014 IEEE Joint Intelligence and Security Informatics Conference*. The Hague, The Netherlands: IEEE, 2014, pp. 331–331.

[19] C. Frøystad, K. Bernsmed, and P. H. Meland, "Protecting future maritime communication," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3098954.3103169

[20] E. W. G. for Mutual Exchange and D. of AIS & Data, "Ais data format - iec standard 61162-450 for ethernet interconnections," 2019.

[21] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*. Paris, France: IEEE, 2015, pp. 1–6.

[22] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. Beijing, China: IEEE, 2017, pp. 1–6.

[23] L. Yu, Y. Liu, P. Jing, X. Luo, L. Xue, K. Zhao, Y. Zhou, T. Wang, G. Gu, S. Nie, and S. Wu, "Towards automatically reverse engineering vehicle diagnostic protocols," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 1939–1956.

[24] M. E. Verma, R. A. Bridges, J. J. Sosnowski, S. C. Hollifield, and M. D. Iannacone, "CAN-D: A Modular Four-Step Pipeline for Comprehensively Decoding Controller Area Network Data," Jun. 2021.

[25] P. Ngo, J. Sprinkle, and R. Bhadani, "CANClassify: Automated Decoding and Labeling of CAN Bus Signals," *Journal of Engineering Research and Sciences*, vol. 1, no. 10, pp. 5–12, Oct. 2022.

[26] S. Kleber, H. Kopp, and F. Kargl, "NEMESYS: Network message syntax reverse engineering by analysis of the intrinsic structure of individual messages," in *12th USENIX Workshop on Offensive Technologies (WOOT)*. Baltimore, MD: USENIX Association, Aug. 2018.

[27] Y. Ye, Z. Zhang, F. Wang, X. Zhang, and D. Xu, "NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces," in *Network and Distributed System Security Symposium*. Virtual: Internet Society, 2021.

[28] C. Yang, C. Fu, Y. Qian, Y. Hong, G. Feng, and L. Han, "Deep learning-based reverse method of binary protocol," in *Security and Privacy in Digital Economy*. Singapore: Springer Singapore, 2020, pp. 606–624.

[29] S. Zhao, J. Wang, S. Yang, Y. Zeng, Z. Zhao, H. Zhu, and L. Sun, "ProsegDL: Binary Protocol Format Extraction by Deep Learning-based Field Boundary Identification," in *30th IEEE International Conference on Network Protocols (ICNP)*. Lexington, KY, USA: IEEE, Oct. 2022, pp. 1–12.

[30] G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam, "Multi-purpose cyber environment for maritime sector," *iccws*, vol. 17, no. 1, pp. 349–357, Mar. 2022.

[31] J. Caballero, H. Yin, Z. Liang, and D. Song, "Polyglot: automatic extraction of protocol message format using dynamic binary analysis," in *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*. Alexandria, Virginia, USA: ACM Press, 2007, p. 317. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1315245.1315286

[32] H. Gascon, C. Wressnegger, F. Yamaguchi, D. Arp, and K. Rieck, "Pulsar: Stateful black-box fuzzing of proprietary network protocols," in *Security and Privacy in Communication Networks*, B. Thuraisingham, X. Wang, and V. Yegneswaran, Eds. Cham: Springer International Publishing, 2015, pp. 330–347.

[33] Y. Wang, X. Yun, M. Z. Shafiq, L. Wang, A. X. Liu, Z. Zhang, D. Yao, Y. Zhang, and L. Guo, "A semantics aware approach to automated reverse engineering unknown protocols," in *2012 20th IEEE International Conference on Network Protocols (ICNP)*. Austin, TX, USA: IEEE, 2012, pp. 1–10.

[34] "Understanding pgns: Nmea 2000 and j1939 - actisense," https://actisense.com/news/understanding-pgns-nmea-2000-and-j1939/, (Accessed on 07/20/2024).

[35] M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2021. [Online]. Available: https://books.google.ee/books?id=Hwk1EAAAQBAJ

[36] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamillaand, and A. M. Satyam, *Improving Web Application Security*. Microsoft Corporation, 2003. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330

[37] F. Klassen, "Tcpreplay - pcap editing and replaying utilities," Appneta, Dec 2022. [Online]. Available: https://tcpreplay.appneta.com/

[38] K. Jindal, S. Dalal, and K. K. Sharma, "Analyzing spoofing attacks in wireless networks," in *2014 Fourth International Conference on Advanced Computing & Communication Technologies*. Los Alamitos, CA, USA: IEEE Computer Society, 2014, pp. 398–402.

[39] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[40] Ø. J. Rødseth and Á. Tjora, "A system architecture for an unmanned ship," in *Proceedings of the 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT 2014)*. Hamburg, Germany: Technische Universität Hamburg-Harburg, 2014, pp. 291–302.

Appendix 7

Publication VII
G. Visky, D. Khisteva, R. Vaarandi, and O. M. Maennel. Towards an open-source intrusion detection system integration into marine vehicles. In *2024 International Symposium ELMAR*, pages 263–268, 2024

Towards an Open-source Intrusion Detection System Integration into Marine Vehicles

Gábor Visky[1], Dariana Khisteva[1], Risto Vaarandi[1], Olaf M. Maennel[2]

[1] Tallinn University of Technology, Tallinn, Estonia
[2] University of Adelaide, Adelaide, Australia

gabor.visky@taltech.ee, dariana.khisteva@taltech.ee, risto.vaarandi@taltech.ee, olaf.maennel@adelaide.edu.au

***Abstract*—The International Maritime Organisation (IMO) issued regulations to enhance cyber security in the maritime domain. Shipping companies look for compliance with the regulations. Together with industry and academia, they make serious efforts to manage this challenge, but they face difficulties, especially in the case of legacy products.**

Our research has thoroughly examined the obstacles and has proposed a possible solution. We found that extending ships' legacy control and navigational systems with an open-source intrusion detection system can significantly contribute to meeting the sector's requirements.

***Keywords*—Intrusion Detection System, IDS, Cyber Security, Maritime**

I. Introduction and motivation

Modern society heavily depends on water surface transportation, carrying around 80% of the world's trade [1]. To improve its efficiency, during the recent decades, maritime systems have become increasingly digitalised and interconnected [2–4], bringing cybersecurity concerns into the marine sector [5]. To handle it IMO issued regulations –introduced in Section II– push shipbuilders and shipping companies to improve cyber security in the sector.

Many vendors [6], [7], universities and research institutions [8], [9] make serious efforts to ease this pain for new products. However, many ships rely on obsolete technologies produced without cyber security considerations, making them vulnerable to cyber-attacks.

Because of their complexity, ships' navigational and control systems cannot be upgraded overnight, and they can only be extended with security solutions after a deep analysis of the impacts. So, vendors producing such systems are hesitant about this question regarding old products.

While cyber security companies provide solutions for various sectors focusing on information technologies (IT), tailored offerings for water vehicles are scarce. These solutions must be fine-tuned since the attack surface in the maritime environment contains not only IT but navigational, surveillance and operational technology (OT) and industrial control systems (ICS) [10]. The existing commercial products lack this specialisation; their majority handle only IT networks with limited flexibility, unlike open-source solutions, which offer greater adaptability to meet ships' OT networks' unique needs.

The issued regulations, the need for compliance, and the currently available technical solutions motivated our research. It examines the state of the art through an extensive literature review, investigates the current practice through expert interviews and ship visits, and analyses it. As a response to the challenge, it proposes an open-source IDS integration. It introduces critical considerations for this extension and highlights crucial factors for seamless and practical integration.

979-8-3503-7542-8/24/$31.00 ©2024 IEEE

II. Background

A. IMO regulation

To support effective cyber risk management and safeguard shipping from cyber threats and vulnerabilities in 2017. IMO issued a guideline containing high-level recommendations on maritime cyber risk management [11], [12]. However guidelines are just recommendatory.

The Maritime Safety Committee in June 2017, also adopted the resolution for Maritime Cyber Risk Management in Safety Management Systems, encouraging administrations to address cyber risks appropriately in existing safety management systems, no later than the first annual verification of the company's Document of Compliance after 1 January 2021 [13].

Cyber security risk assessment is being partly regulated by the International Ship and Port Facility Security (ISPS) Code established by the IMO [14].

B. Intrusion Detection Systems (IDS)

An IDS detects and logs predefined activities in the network, system parameters or user activities.

The network-based IDS (NIDS) monitors network activities, collects network-related data, and detects malicious traffic on a network [15]. Host-based IDS (HIDA) detect possible attacks into individual computers on which the intrusion detection systems run [16]. It deals with system parameters (memory content and usage, CPU load, network traffic, processes, etc.) and user actions.

These devices identify possible hostile activities by using different anomaly detection methods, rule violation detection or signatures recognition [17], [18].

If needed and programmed to, it notifies staff members to check on certain alerts and take further actions. It is important to mention intrusion prevention systems (IPS). The goal of IPSs is similar to what IDSs do however, it is also permitted to take such predefined actions as blocking or altering the given traffic [15], [19].

2024 International Symposium ELMAR | 979-8-3503-7542-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ELMAR62909.2024.10694518

C. Related Work

We searched for publications from the last 25 years in electronic libraries about IDS solutions for ships or vessels. Because of the low number of hits, we extended our query to the operational technology to increase our scope.

Potamos et al. introduce a framework for maritime cyber threat detection, focusing on human skills' building and systems' cyber threat detection capabilities. The research recommends deploying the security monitoring sensors at appropriate network positions in each segment to collect the IT and OT network traffic. The study does not detail the technical details or the expectations for such a system [20].

Jeffrey et al. in [21] proposes a hybrid anomaly detection methodology for cyber-physical systems. Their solution supports many industries, but ship-related details need to be considered.

Many publications evaluate sensor data anomaly detection based on different features, like NMEA sentence integrity for GPS spoofing detection [22], and introducing defence solutions, such as IDS for attack detection [23].

Jacq et al. in [24] research the concept of naval systems' situational awareness and discuss the HIDS shortages. They can only be installed with causing a warranty disruption. On the contrary, they suppose NIDS is a feasible extension.

Amro et al. in [25] also consider NIDS a more suitable option, as it can be added to the networks for monitoring NMEA traffic and detecting anomalies.

These publications motivate our research to highlight the obstacles to these systems, and answer, why they are not installed on ships, and how the situation could be improved.

III. Method

To improve our understanding of the current situation and practice, we applied a combined approach based on literature review, expert interviews, and ship visits. We extended our scope and examined the details to identify potential technological obstacles that are inevitable for solution-seeking.

A. Literature survey

As it is introduced in Section II-C we conducted an exhaustive literature survey through numerous electronic libraries to uncover defensive solutions implemented aboard ships. This rigorous exploration delved deep into the strategies and technologies employed to safeguard vessels against cyber threats.

B. Expert interviews

To map the current practice, we conducted several semi-structured interviews with ship crews and ship integrator company representatives. We focused on the methodologies, rules and regulations and the common practice to find potential obstacles, bad and good practices. We aimed to map the following groups:

- Network topology of the ship;
- IT and OT systems connected to the vessel's network;
- Computer-, operating system- and software-related information including updates, users, authorisation mechanics;
- Ship's external communication.

C. Ship visits

To see the ship control systems' practical implementation, we visited two passenger ferries run by the Estonian market-leading TS Laevad company. During these visits, we gained a deep insight into the technology applied and learned about the cyber security measures on the ships.

IV. Results

A. Literature survey

The result of the literature survey is detailed in Section II-C. We can conclude its results in the lack of the relevant literature, that introduces appropriate defensive cyber security solutions for ships.

B. Ship visits and expert interviews

During the ship visits and expert interviews, we were looking for additional details to have a deep insight into the current situation.

1) Ship networks: A ship can have several independent networks for different purposes. We identified the following networks on the visited ships.

Administrative network is a tree topology network that is a part of the company's virtual private network (VPN) and has multiple purposes. It provided a constant communication channel with the headquarters. The computers in this network supported the administrative tasks, like status reporting, map update downloading, etc. This network also provides a monitored internet connection for administrative purposes.

The network is constantly connected in ports over WiFi and during voyages —when the service is available— over 4G or 5G mobile networks. Satellite communication is not used for this communication.

Navigational network is a (partly) isolated network connecting navigation-related devices, like Electronic Chart Display and Information Systems (ECDIS), Integrated Navigation Systems (INSs), Multi-Functional Displays (MFDs) and Data Collector Units (DCUs), and RADAR together. This network has a redundant ring topology and receives propulsion-related data from the Propulsion Control Network over a single-way connection.

Propulsion Control Network is a (partly) isolated, redundant network, providing communication between the bridge and the propulsion automation system. The propulsion of the passenger ferry can operate in fully manual mode, meaning the propulsion and its direction–in the case of emergency– can be controlled by physical switches in the engine room. This network sends propulsion-related data to the Navigational Network over a single-way connection.

Cargo handling network is an isolated network composed of wired and wireless devices. This network supports cargo-handling and administration. The cargo-related data sent from the shore in special data format is imported to the offline cargo management system.

Public WiFi network is an isolated network, providing Internet over a WiFi infrastructure for the passengers. It has network devices that manage the users' logical separation.

Network for independent support company is an isolated wired and wireless network providing the network for the restaurant of the ferry supporting order management, payment, etc.

2) IT and OT systems: On the visited ship all the different systems were isolated. We identified the administrative system, the public WiFi and the independent company's system as an IT system, and the navigation, the propulsion, the control (heating, ventilation, and air conditioning (HVAC), security and safety, etc.), the cargo handling and the power generation systems as OT systems.

3) Ship computers and operation systems: We identified different operating systems–Windows 7 or later—with different computer security measures. Depending on the subsystem, updated and obsolete, unsupported ones were found. In navigation and control, we found computers without any security solutions, like host-based IDS, antivirus, or end-point protection.

The regularity of the software updates depended on the subsystem. In the case of isolated systems, the update was done during regular maintenance.

Additional software installation was strictly restricted, the software installation needed elevated rights.

Only administrative controls have been placed on the use of data storage devices: a dedicated device was allowed to be used for data exchange. The USB connectors of the OT computers were secured against random access.

On the administrative computers each user had individual account originated from the domain, but on the ECDIS only administrator and user account existed.

C. Identified obstacles

We identified the following obstacles limiting the cyber security measures.

1) Legacy technology: As of early 2023, the average ship's age was 22.2 years, with over half older than 15 years and around 40% older than 20 years. In January 2023, global maritime trade was transported on board 105,493 vessels of 100 gross tons (GT) and above. This means more than 50,000 ships in this tonnage are older than 15 years [26].

According to experts, these ships have legacy technologies and suffer from the above-mentioned shortages in their networks.

2) Troubleshooting: Due to the constrained crew size on ships, there is often no room for cyber or IT specialists. Therefore, sailors typically address system issues by swapping out faulty units with onboard spares. This approach, coupled with the scarcity of spare parts during voyages, needs devices with simple configurations for easy installation, posing challenges for implementing diverse security measures.

For example, the unique identifier of the actual network devices (medium access control address) cannot be registered into a network endpoint protection (EPP) solution to avoid using unregistered devices because the spare part's unique identifier is often unknown before troubleshooting.

3) Technology readiness: The currently used legacy devices are not prepared for cyber challenges, as a decade ago, cyber security was completely outside the sector's scope.

4) Other restrictions: Since the ship control systems must be certified by authorities restricting the changes or updates on these systems.

Ship navigation- and control software developer companies face significant challenges. They must test their product on a specific setup, and this environment is also required on the ships. These conditions can hinder the necessary improvements to address the evolving cyber challenges.

V. Discussion

A. Conclusion of the highlighted obstacles

During the data collection, we surveyed the literature and we were not able to find an appropriate cyber security solution for ships.

The introduced practice meets the security requirements; however, in the expert's opinion, this level of network segregation is infrequent and can be found only on the latest generation of ships. Usually, the ship-related network covers every operational function, like navigation, propulsion, and cargo management, and there is another separate administrative network with an Internet connection. In particular cases, even this separation does not take place.

In the maritime shipping industry, safety takes precedence over security, meaning a cyber incident cannot threaten the mission: e.g., a ship may continue operating even with malicious code running on it.

Another challenge is the mandatory certification that blocks modifications–like installing defence solutions–on ships. Ship control software developer companies often require a given product environment, restricting continuous security updates. In some cases, the built-in endpoint protection features must be disabled.

The simplified troubleshooting methods do not allow detailed security settings.

B. Proposed solution

IMO issued its recommendatory regulatory, pushing the sector towards a more cyber secure word forcing compliance. At the same time, we identified several obstacles. To handle this situation, we propose the following solutions.

1) Network segregation: This practice meets the security requirements; however, setting up such a topology requires relatively high investment, especially on legacy ships where significant hardware updates and extensions (for example, new cables) are needed.

2) Network segmentation: The logical segmentation of ship networks increases the cyber security of the ship and makes lateral movement more complicated, but it does not make it impossible. In the case of a compromised network device, the logical segmentation becomes useless. Since the solution needs a detailed setup, it would be hard to introduce because of the troubleshooting practices.

3) Intrusion Detection System: Both above-mentioned solutions have the same shortages. Both would need the audit of the ship for the re-certification and despite the effort, these measures would not elevate cyber awareness. This limitation, along with the troubleshooting-related ones introduced in Section IV-C2 can be overcome with IDSs or IPSs, installed during ship manufacturing or renovation or scheduled maintenance, which can indicate anomalies, and alert the crew.

VI. Towards an NIDS

Analysing the literature, experts' opinions, and the current situation led us to an optimal solution: a NIDS installed on ships' networks. Our paper's other main contribution is its investigation.

A. Commercial NIDS

The market offers several commercial NIDS [27–30]. These products' common characteristic is the high capacity and scalability that is not needed on a ship because of its limited network size. These solutions need security information and event management usually deployed in Security Operation Centres (SOC). Since the SOC is located on the shore, this solution needs high communication bandwidth, which is rarely available over satellite communication.

The other shortage of this solution is the trend that they are heavily connected to the Cloud, which also needs high-speed external communication. Furthermore, these systems do not consider maritime-related details and are hardly extendable with special OT-related anomaly detection modules.

B. Open source NIDS

The deployment of an open-source NIDS, known for its reliability, can effectively overcome these limitations. In our comprehensive research, we examined three widely used solutions: Snort [31], Zeek [32], and Suricata [33], all of which have proven their worth in the field of network security.

Snort is signature-based, initially created by Sourcefire, and now belongs to Cisco. It has five main components: packet capture, decoder, preprocessor, detection engine, and output. A possible drawback lies in the created rules that are not part of the Snort distribution itself but originate from different sources. These rules might be redundant and lack anomaly-based detection capabilities. On the positive side, Snort can handle industrial protocols, like DNP3 with appropriate regulations [34].

Suricata is also a signature-based NIDS. In its packet decoder, every packet is converted to a data structure supported by Suricata. Its rules support layer 3, 4 and 7 of the OSI model [35]. Suricata uses a rule model similar to Snort; their signature languages are identical, and they can use the same suppliers. This also brings up the abovementioned redundant rule issue in the case of Suricata.

Both solutions can keep up with dense network traffic and have multi-threading features and good documentation.

Zeek, an anomaly-based NIDS, is specifically designed to adapt to dense live network traffic, making it a versatile solution. It is highly customisable and uses its own scripting language, further enhancing its adaptability. It is adaptable to an industrial environment and can support industrial protocols, like the Modbus protocol [36]. Since it is anomaly-based, it can detect attacks without known signatures, providing a robust security solution. Zeek also boasts good official documentation, ensuring ease of use despite its advanced features. However, it requires a significant amount of storage space and installation effort, which should be taken into consideration.

At this point, we need further analysis to decide on the optimal product. Since Cisco transformed Snort into commercial use, it can be more easily integrated into a ship control system.

At the same time, the signature update procedure introduces difficulties because of the limited bandwidth during the voyage and the need for an expert because of the isolated networks. An anomaly-based solution might be better for ships since it can support anomaly detection not only in the lower network layers but also in the application layer.

C. NIDS placement

On the visited ships, we identified several separate IT and OT networks. The current study focuses on critical OT navigation and control networks. A common characteristic is the wide range of protocols, but topology-wise, they are different. The control network had a tree topology, while the navigation network had a ring topology.

The very low bandwidth on these networks allows the deployment of IDSs with moderated hardware resources to each network, which would keep these networks isolated, or a centralised, more powerful solution with passive taps can be used.

One of the challenges we encountered was the network data collection. While network devices can mirror the network traffic on a dedicated port, the segmented tree topology does not support the routing of these data streams. This underscores the necessity of deploying a monitoring network, which would enable efficient traffic monitoring and identification of potential attacks or anomalies.

In the case of the navigation network on the ferries we visited, we found that it relied on Moxa Turbo Ring technology. This technology plays a crucial role in providing a fast, redundant communication infrastructure. The ring redundancy feature ensures non-stop operation of networks with an extremely fast recovery time. A dedicated switch is responsible for avoiding infinite loops, and it can also provide a traffic mirror for the IDS, enhancing network security [37].

VII. Conclusion and Future Work

We identified several obstacles to improving cyber security in the sector and evaluated the concept of integrating an open-source IDS. We can conclude our findings as follows.

Extending the ship network with IDS solutions connected over sensors with passive taps to the different networks can improve the ship's cyber awareness and possibly be feasible at limited costs without harming the network isolation.

An open-source IDS can be extended with maritime-specific add-ons to increase its anomaly detection capabilities; however, these solutions still need to be certified.

IDS can be placed on a bridge but with limited functionalities: it can serve only as a passive monitoring and logging tool. In this case, we cannot prevent attacks. However, the solution can help forensics and incident analysis, and it can be an initial step to gain "credit of trust".

From an economic perspective, an advantage of open-source tooling is that it is free. However, experts have expressed some doubt about the cost of human hours implementing this type of solution onboard. Calculating and prognosing human efforts is outside the scope of this research paper.

Since this research brought up a concept, the performance and the applicability of the different IDSs need to be researched.

ACKNOWLEDGEMENT

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

REFERENCES

[1] H. N. Psaraftis, *The Future of Maritime Transport*. Elsevier, 2021, p. 535–539. [Online]. Available: http://dx.doi.org/10.1016/b978-0-08-102671-7.10479-8

[2] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166

[3] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100571, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555

[4] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22

[5] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean &; Coastal Management*, vol. 236, p. 106493, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1016/j.ocecoaman.2023.106493

[6] "Maritime cyber security," https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/, 06 2022, (undefined 7/4/2024 13:20).

[7] "Introduction cooperation on maritime cybersecurity atlantic council," https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/, 10 2021, (undefined 7/4/2024 13:22).

[8] "Maritime cyber resilience prosjektbanken," https://prosjektbanken.forskningsradet.no/project/FORISS/295077, (undefined 7/4/2024 13:29).

[9] "Maricybera," https://maricybera.taltech.ee/, 04 2021, (undefined 7/4/2024 13:30).

[10] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime cyber threats detection framework: Building capabilities," in *Information Security Education - Adapting to the Fourth Industrial Revolution*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds. Cham: Springer International Publishing, 2022, pp. 107–129.

[11] I. M. O. (IMO), "Msc-fal.1-circ.3 - guidelines on maritime cyber risk management," 7 2017, [Accessed: 15-11-2020].

[12] ——, "Msc-fal.1/circ.3/rev.2 - guidelines on maritime cyber risk management," 6 2022, [Accessed: 11/04/2024].

[13] International Maritime Organization, "Resolution msc.428(98) - maritime cyber risk management in safety management systems," 7 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.

[14] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *Journal of Navigation*, vol. 72, no. 5, p. 1108–1120, Feb. 2019. [Online]. Available: http://dx.doi.org/10.1017/S0373463318001157

[15] "Chapter 1 - introduction to intrusion detection systems," in *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*, J. Burton, I. Dubrawsky, V. Osipov, C. Tate Baumrucker, and M. Sweeney, Eds. Burlington: Syngress, 2003, pp. 1–38. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781932266696500215

[16] D.-Y. Yeung and Y. Ding, "Host-based intrusion detection using dynamic and static behavioral models," *Pattern Recognition*, vol. 36, no. 1, pp. 229–243, 2003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320302000262

[17] A. S. Ashoor and S. Gore, "Importance of intrusion detection system (ids)," *International Journal of Scientific and Engineering Research*, vol. 2, no. 1, pp. 1–4, 2011.

[18] M. Pihelgas, "A comparative analysis of open-source intrusion detection systems," *Tallinn: Tallinn University of Technology & University of Tartu*, 2012.

[19] I. Mukhopadhyay, K. S. Gupta, D. Sen, and P. Gupta, "Heuristic intrusion detection and prevention system," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 2015, pp. 1–7.

[20] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime cyber threats detection framework: Building capabilities," in *Information Security Education - Adapting to the Fourth Industrial Revolution*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds. Cham: Springer International Publishing, 2022, pp. 107–129.

[21] N. Jeffrey, Q. Tan, and J. R. Villar, "A hybrid methodology for anomaly detection in cyber–physical systems," *Neurocomputing*, vol. 568, p. 127068, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231223011918

[22] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, and J. Bauer, "Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring," *Journal of Marine Science and Engineering*, vol. 11, no. 5, p. 928, Apr. 2023. [Online]. Available: http://dx.doi.org/10.3390/jmse11050928

[23] C. Boudehenn, O. Jacq, M. Lannuzel, J.-C. Cexus, and A. Boudraa, "Navigation anomaly detection: An added value for maritime cyber situational awareness," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1–4.

[24] O. Jacq, D. Brosset, Y. Kermarrec, and J. Simonin, "Cyber attacks real time detection: towards a cyber situational awareness for naval systems," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, Jun. 2019. [Online]. Available: http://dx.doi.org/10.1109/CyberSA.2019.8899351

[25] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104

[26] U. Nations, "Review of maritime transport 2023," 2023. [Online]. Available: https://unctad.org/system/files/official-document/rmt2023_en.pdf

[27] "Next-generation firewalls - palo alto networks," https://www.paloaltonetworks.com/network-security/next-generation-firewall, (Accessed on 04/21/2024).

[28] "Mdr solutions & services from alert logic," https://www.alertlogic.com/managed-detection-and-response/, (Accessed on 04/21/2024).

[29] "Cisco secure firewall - cisco," https://www.cisco.com/site/ca/en/products/security/firewalls/index.html, (Accessed on 04/21/2024).

[30] "Apiiro | secure your development and delivery to the cloud," https://apiiro.com/, (Accessed on 04/21/2024).

[31] "Snort - network intrusion detection & prevention system," https://www.snort.org/, (Accessed on 04/21/2024).

[32] "The zeek network security monitor," https://zeek.org/, (Accessed on 04/21/2024).

[33] "Home - suricata," https://suricata.io/, (Accessed on 04/21/2024).

[34] H. Li, G. Liu, W. Jiang, and Y. Dai, "Designing snort rules to detect abnormal dnp3 network data," in *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*, 2015, pp. 343–348.

[35] D. Fadhilah and M. I. Marzuki, "Performance analysis of ids snort and ids suricata with many-core processor in virtual machines against

dos/ddos attacks," in *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020, pp. 157–162.

[36] Z. Hill, J. Hale, M. Papa, and P. Hawrylak, "Using bro with a simulation model to detect cyber-physical attacks in a nuclear reactor," in *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 22–27.

[37] "moxa-turbo-ring-tech-note-v1.0.pdf," https://www.moxa.com/Moxa/media/PDIM/S100000119/moxa-turbo-ring-tech-note-v1.0.pdf, (Accessed on 04/23/2024).

Appendix 8

Publication VIII
G. Visky, B. Adam, R. Vaarandi, M. Pihelgas, and O. Maennel. Open source intrusion detection systems' performance analysis under resource constraints. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, pages 201–208, 2024

Open Source Intrusion Detection Systems' Performance Analysis Under Resource Constraints

Gabor Visky[1], Balint Adam[1], Risto Vaarandi[1], Mauno Pihelgas[1], Olaf M. Maennel[2]
[1] Tallinn University of Technology, Tallinn, Estonia
[2] University of Adelaide, Adelaide, Australia
gabor.visky@taltech.ee, balint.adam@taltech.ee, mauno.pihelgas@taltech.ee,
risto.vaarandi@taltech.ee, olaf.maennel@adelaide.edu.au

***Abstract*—The International Maritime Organisation (IMO) issued regulations to enhance cyber security in the maritime domain. Researchers suggest deploying open-source intrusion detection systems (IDSs) aboard to ensure the ships' operational technology network (OTN) complies with these regulations and enhances cyber security readiness.**

According to previous studies, selecting the optimal IDS is a complex procedure. Our research examines and compares the performance of three open-source IDSs under restricted resources to identify their resource needs, dropped packet ratio, and other software characteristics in virtual and physical environments.

Our findings indicate that two of the examined software options can effectively handle the network traffic of ships' OTNs under restricted resources. However, it's worth noting that a Raspberry PI, while a popular choice, may not be the most optimal hardware for this purpose.

***Keywords*—Intrusion Detection System, IDS, Cyber Security, Performance, Maritime**

I. Introduction and motivation

Modern society relies significantly on waterborne transportation, which handles approximately 80% of global trade. [1] To enhance efficiency, maritime systems have become increasingly digitalized and interconnected over recent decades, introducing significant cybersecurity concerns into the sector. [2–5]

Many actors in the field, companies [6], [7], universities and research institutions [8], [9] make serious efforts to ease this pain for new products. However, many ships rely on obsolete technologies produced without cyber security considerations, making them vulnerable to cyber-attacks. Because of their complexity, ships' navigational and control systems cannot be upgraded at a night, and they can only be extended with security solutions after a deep analysis of the impacts. So vendors, producing such systems are hesitant about this question regarding the old products.

While cybersecurity companies provide tailored solutions for various sectors focusing on information technologies (IT), specialised offerings for waterborne vessels remain limited. These solutions must be fine-tuned since the attack surface in the maritime environment contains not only IT but navigational, surveillance and operational technology (OT) and Industrial Control Systems (ICS). [10] The existing commercial products lack this specialisation. Their majority handle only IT networks with limited flexibility, unlike open-source solutions, which offer greater adaptability to meet the unique needs of ships' OTNs.

Jacq et al. in [11] research the concept of naval systems' situational awareness and discuss that the HIDS' cannot be installed without causing a warranty disruption, but they suppose NIDS is a feasible extension.

Amro et al. in [12] also consider NIDS a more suitable option, as it can be added to the networks for monitoring NMEA traffic and detecting anomalies.

Our previous research highlighted the open-source IDS integration as a response to the challenge and identified the performance analysis of such devices as a research gap. Our current study addresses this gap and compares three open-source IDS's performance and resource needs.

II. Background

A. Intrusion Detection Systems (IDS)

An IDS identifies and logs predefined activities in network parameters, system configurations, or user behaviours.

A Network-based IDS (NIDS) monitors network activity, collects network-related data, and identifies malicious traffic. [13] It serves as the first line of defence by scrutinising all network traffic and flagging any suspicious patterns.

Conversely, a Host-based IDS (HIDS) focuses on detecting potential attacks on individual computers where the IDS is installed. [14] This system monitors system parameters such as memory content and usage, CPU load, network traffic, processes, and user actions, providing a deeper, more localised level of security analysis.

These devices—using different anomaly detection methods, rule violation detection, or signatures recognition— identify possible hostile activities. [15], [16]

An IDS detects and logs predefined activities and, if programmed, can also notify staff members to investigate specific alerts and take further actions. It is also essential to mention Intrusion Prevention Systems (IPS), which are additionally authorised to execute predefined actions such as blocking or modifying suspect traffic. [13], [17] This proactive capability allows IPSs to alert administrators about potential threats and actively intervene to mitigate them.

B. Examined IDSs

In this research, we examined the following three popular IDSs. **Snort** is signature-based, originally created by Sourcefire and now belongs to Cisco. It has five main components: packet capture, decoder, preprocessor, detection engine, and output. A possible drawback lies in the created rules, which might be redundant and the lack of anomaly-based detection capabilities. It can handle industrial protocols, like DNP3 [18] with appropriate rules.

Suricata is also signature-based; it also uses a packet decoder and detection engine. In its packet decoder, every packet is converted to a data structure supported by Suricata. Rules used by the IDS support layer 3, layer 4 and layer 7 of the OSI model. [19]

Zeek is anomaly-based NIDS, designed to analyse dense live network traffic. It is adaptable to an industrial environment and can support industrial protocols, like Modbus protocol. [20] It is highly customisable and uses its own scripting language. Since it is anomaly-based, it can detect attacks without known signatures. Zeek has good official documentation. However, it needs a lot of storage space and takes more effort to install.

C. Related Work

We searched for publications from the last 25 years in electronic libraries about IDS performance analysis and found rich relevant literature.

Borkar et al. published a survey on IDSs and IPSs that gives an overview of the field but does not focus on the performance of such a system. [21] Many publications introduce performance evaluation on different anomaly detection methods. [22], [23]

We found studies that evaluate the IDSs on different datasets, but these researches focus on the detection efficiency and the number of dropped packet ratio, but not on the resource needs. [24–27]

Tripathi et al. in [28] introduced the integration of a Snort and a Honeypot, running on a Raspberry PI (RPi) minicomputer. The research proved the feasibility of an IDS on limited resources but analysed only one solution.

Kyaw et al. [29] also worked with RPi when researching Snort and Bro IDSs. The research shows some similarity to our own, but we also analysed Suricata and used Snort 3 and Zeek, the successor of Bro.

Pihelgas's thesis compares similar IDSs, like our research, but it also focuses on previous software versions. [16]

III. Method

A. Installed IDS Software

In our research we examined three widely used solutions: Snort [30], Zeek [31], and Suricata [32], with their default configurations along with some minor changes, related to the generated logs so they used all of their included default signatures, except Snort version 3. Since there were no default signatures included, the snort3-community-rules.tar.gz packet was used. [33]

B. Research environment

The research was conducted in two independent environments.

1) Virtualised Environment: The first part —serving method testing and baseline preparation— was conducted in a virtual environment, depicted in Figure 1. An Ubuntu Server operating system (OS) hosted the VMware Player virtualisation environment together with the three —Debian based Linux distributions— guest OSs. We chose this OS because, in the physical testing environment, the IDSs are installed on RPIs and their OS —the Raspbian— is also Debian-based. All virtual machines (VMs) —organised into the same network— had the same specifications, 4GB random access memory (RAM), a CPU with 4 cores and 30GB storage space. Each VM had an IDS installed along with the traffic generator.

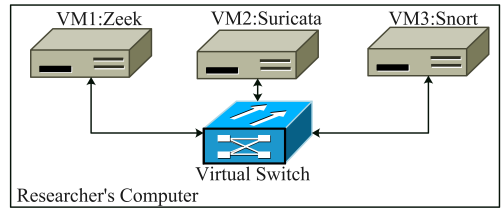


Figure 1. Virtual testing environment.

The hardware-based environment consisted of one computer (PC) and three RPis, with Raspbian Lite (Legacy) which is a Debian version 10 (Buster) based OS, providing us restricted resources. All the computer was organised into the same network, connected with a switch.

2) Physical Environment: The physical environment consisted of three RPi4s, one switch and one PC for network traffic generation, data collection and analysis, as can be seen in Figure 2.

After the necessary software and IDSs were installed, the RPIs were connected to three different ports of the switch. All those ports received the same traffic from the generator, which was also connected to the switch.

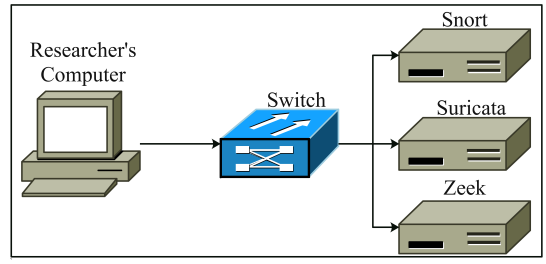


Figure 2. Physical testing environment.

C. Network traffic generation

The network traffic was generated by replaying packet capture (PCAP) files. The PCAP without malicious activity was recorded during the Crossed Swords Cyber Exercise, while the other two PCAPs, containing malicious packets originated from the Secure Water Treatment (SWaT) dataset [34].

D. Monitored resources

During our research, we measured and logged the following values: total time elapsed (real-time), the total time that the central processing unit (CPU) spent in user and kernel modes, average CPU usage, and maximum resident set the size of the process during its lifetime (maximum memory used). These monitored resources cover the critical parts that could be bottlenecks of the hardware in live deployment.

To gain the most accurate results, the measurements started with a cron job[1] and stopped automatically when the given script finished execution.

During the testing phase, the *GNU time utility* recorded the measurements to files containing all the data needed for further analysis.

IV. Results

To speed up the analysis and minimise human errors, self-developed Python scripts to process the collected logs. These logs were separated into multiple files using unique scripts that were created to sort the values of individual resources to separate files and calculate the mean value of the given resource.

A. Results measured in the virtual environment

In the virtual environment, each IDS was tested 20 times on PCAP files without malicious activity to ensure reliable data for the average calculation, leading to the following results. This method helped to understand the IDSs' nature without resource constraints.

Figure 3. shows the time needed to process the sample files in the virtual environment. Snort had the longest run time with ($t_{Snort} = 12,197.93s$) with Suricata was the second ($t_{Suricata} = 10,561.78s$) and Zeek ($t_{Zeek} = 9,431.78s$) in the third place with the shortest runtime. The running time does not represent the same difference. Snort and Suricata needed the same average time ($\overline{t_{Snort}} = 9,941.17s, \sigma = 345.49$) and Suricata ($\overline{t_{Suricata}} = 9,937.27s, \sigma = 171.82$), so the difference is just $t_{diff} = 3.9s$, while Zeek ($\overline{t_{Zeek}} = 9,002.84s, \sigma = 150.47$) has a shorter runtime $\Delta t_{Snort,Zeek} = 938,33s$ on the same PCAP file.

Figure 4. depicts the average and the maximum CPU usage of the different software. In the maximal CPU load, we cannot see a significant difference between Snort and Suricata; they made almost similar CPU load, while Zeek needed were significantly less ($CPU_{max_{Zeek}} = 8.08\%$). Regarding the average values Suricata ($\overline{CPU_{Suricata}} = 20.89\%, \sigma = 0.79$) has

[1]A job scheduler on Unix-like operating systems

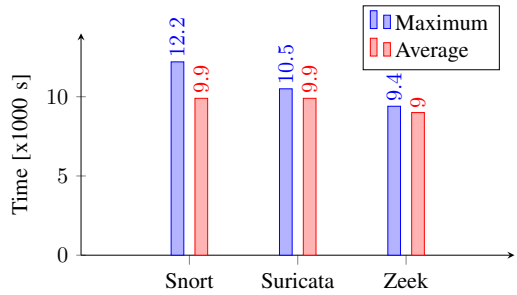


Figure 3. Elapsed time

fallen behind Snort ($\overline{CPU_{Snort}} = 12.06\%, \sigma = 1.58$) compared to the maximum values however, Zeek ($\overline{CPU_{Zeek}} = 6.94\%, \sigma = 0.5$) still had the best numbers out of the three.

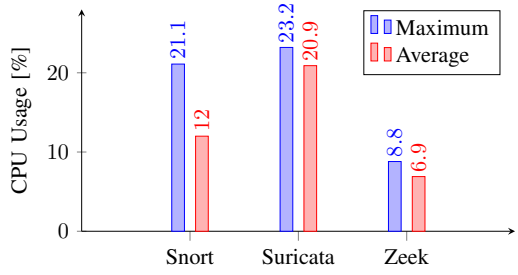


Figure 4. CPU usage

A process can operate in one of two modes: user mode or kernel mode. In user mode, a process runs with restricted access to system resources, which enhances safety by limiting the impact of crashes; any damage can be managed and rectified by the kernel. While in kernel mode, it enjoys full access to the processor and main memory. This unrestricted access is advantageous because it allows the process to perform system calls needed to manage system resources, such as reading and writing files. [35]

Figure 5 shows the maximum and average time spent in kernel mode. The time spent in kernel mode is proportional to the overall CPU usage. Regarding the maximal values Snort ($t_{Snort} = 1,284.92s$) and Suricata ($t_{Suricata} = 1,299.96s$) are very close to each other, while Zeek ($t_{max_{kernel_{Zeek}}} = 251.09s$) spends the least amount of time in the kernel space. The average values follow the similar pattern Snort spent ($\overline{t_{Snort}} = 612.78, \sigma = 102.47$), while Suricata ($\overline{t_{Suricata}} = 981.26, \sigma = 67.64$) and Zeek ($\overline{t_{Zeek}} = 197.53, \sigma = 40.20$) in kernel mode.

In case of user mode, we observed that Snort spent the longest time in the user space ($t_{max_{Snort}} = 1,290.49$), Suricata was the next ($t_{max_{Suricata}} = 1,253.45$), and Zeek ($t_{user_{Zeek}} = 578.62$) spent the least time there.

However, if we compare the graphs of time spent in kernel and user mode, the results show that Snort and Suricata spent

nearly identical amounts of time in both spaces. In contrast, Zeek spent significantly more time in user than kernel mode.

The average values follow a similar pattern. Suricata spent the most time in user space ($\overline{t_{Suricata}} = 1,146.1, \sigma = 67.64$), Snort had a much better result ($\overline{t_{Snort}} = 646.28, \sigma = 102.47$), and Zeek the least time there ($\overline{t_{Zeek}} = 471.77, \sigma = 40.20$).

By monitoring these resources, we can gain a deeper understanding of how the process operates in the kernel and what risks it carries. If a process spends relatively more time in kernel mode, there is a bigger chance of some operations failing and crashing the system. However, if the opposite is true, then the process might not get access to resources that would be needed for optimal operation.

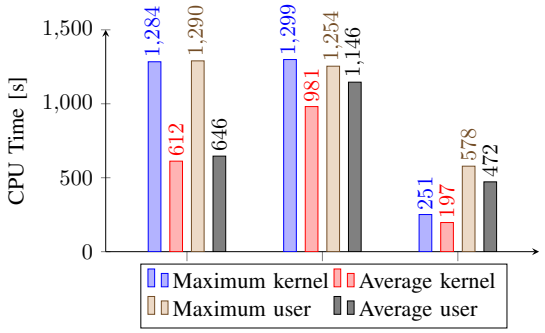


Figure 5. CPU usage

Figure 6. shows the maximum and average memory consumption, which does not show a significant difference for each IDS. Snort used ($Memory_{max} = 104MB$, $\overline{Memory} = 102MB, \sigma = 426.44$) and Suricata ($Memory_{max} = 98MB$, $\overline{Memory} = 96MB, \sigma = 359.42$) produced very similar values, with a slight advantage of Snort, while Zeek used ($Memory_{max} = 240MB$, $\overline{Memory} = 238MB, \sigma = 561.17$)), far the most amount of memory.

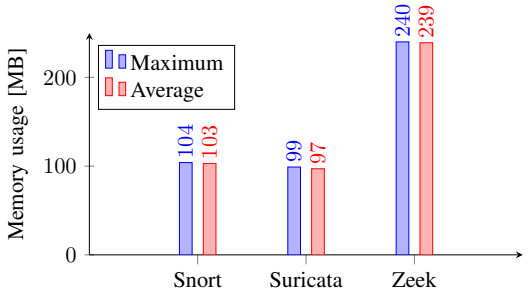


Figure 6. Memory usage

B. Results from the physical environment

In the physical environment, the IDSs underwent a stress test, in which we investigated 1) the effects of restricted resources and 2) the effect of malicious packets. For this experiment, two PCAP files were used twice, first without and then with malicious packets. In this case, besides the resource consumption, the number of dropped packets was measured.

In this segment of our research, we did not consider the total time elapsed as there was only one traffic generator involved. Once it completed simulating a given PCAP, it simultaneously stopped all the IDSs. This approach allowed us to focus on the crucial aspects of the IDS performance, enhancing the significance of our findings.

The physical environment was first tested *without attacks* with the similar PCAP files we used in the virtual environment, then with another PCAP recorded in an industrial environment. This gave a comprehensive result of how a given IDS can perform with limited hardware resources. The results are summarised in Table II.

In this phase, the IDSs were not able to process every packet. Besides the resource consumption, the dropped packet ratio—introduced in Table I. — indicates the performance.

Table I. Summary of the dropped packets.

IDS	PCAP 1		PCAP 2	
	Without malicious packets	With malicious packets	Without malicious packets	With malicious packets
Snort	22-214	0	39-208	0
Suricata	0	0	0	0
Zeek	1990-1995	8750-8780	1991-1995	8540-8560

During this experiment—without attacks — with PCAP1, Suricata did not drop any packets, contrary Snort dropped 22-214, while Zeek 1990-1995 packets, while with PCAP2 Suricata dropped 0 packets while Snort 39-208 and Zeek 1991-1995 packets. With malicious activity, Snort improved its performance and did not drop any packet, while Suricata remained the same, but Zeek brought a worse result, dropping or not processing more than 8000 packets, which is 0.07% of the total packets that the IDS dealt with.

V. Discussion

The initial experiment took place in a virtual environment, where we replayed prerecorded network traffic captures (which did not include any malicious packets) to various IDSs operating on virtual machines configured with identical resources.

The IDSs' resource consumption restricted the replay's speed, thereby also limiting the overall execution speed.

During the tests, Zeek's average CPU usage was 6.94%, compared to Snort's 12.06% and Suricata's 20.89%. Despite Snort and Suricata having similar average execution times of 9,941.17 seconds and 9,937.27 seconds, respectively, Zeek completed the tasks more quickly, with an average time of 9,002.84 seconds. Additionally, Suricata spent the most time in kernel space, using 46.13% of its capacity, followed by Snort at 48.61%, and Zeek at 29.51%. This significant difference in time spent in kernel mode suggests a higher likelihood of critical system failure when using Suricata.

Given that Zeek used the least CPU, it logically spent the least amount of time in kernel space. The durations spent in

Table II. Summary of the results

	Virtual Environment			Physical environment											
				Without maliciopus packets						With malicous packets					
				PCAP1			PCAP2			PCAP1			PCAP2		
	Snort	Suricata	Zeek	Snort	Suricata	Zeek	Snort	Suricata	Zeek	Snort	Suricata	Zeek	Snort	Suricata	Zeek
Max CPU usage [%]	21	23	8	44	45	40	44	45	40	29	15	9	28	15	10
AVG CPU usage [%]	12.06	20.89	6.94	43.01	32.5	39.2	43.02	31.91	39.6	29.00	15.00	8.35	28.00	15.00	8.14
Max time in kernel mode [s]	1,284.92	1,299.96	251.09	895.97	716.99	778.91	888.98	718.96	787.26	275.73	119.35	89.37	263.15	116.94	103.85
AVG time in kernel mode [s]	612.78	981.26	197.53	870.87	496.02	760.64	874.37	489.5	768.67	272.41	117.08	86.64	260.81	113.01	86.53
AVG time in kernel mode [%]	48.67	46.13	29.51	61.84	46.56	59.15	61.97	46.76	59.44	59.81	47.87	62.23	59.68	47.83	64.26
Max time in user mode [s]	1,290.49	1,253.45	578.62	560.65	765.73	538.41	546.32	772.74	540.41	185.28	129.33	56.57	182.54	125.45	49.71
AVG time in user mode [s]	646.28	1,146.10	471.77	537.34	569.31	525.27	536.68	557.31	524.43	183.04	127.49	52.58	176.23	123.25	48.13
AVG time in user mode [%]	51.33	53.87	70.49	38.16	53.44	40.85	38.03	53.24	40.56	40.19	52.13	37.77	40.32	52.17	35.74
Max memory usage [GB]	1.05	0.9863	2.4	0.858	0.674	2.13	0.895	0.681	2.22	8.56	5.45	210.00	7.798	5.46	2.06
AVG memory usage [GB]	1.03	0.9673	2.39	0.857	0.666	2.13	0.8906	0.7644	2.15	0.837	0.541	2.09	0.765	0.5412	2.06

user mode reflect a similar pattern to those in kernel mode; Suricata leads with 1146.1 seconds, followed by Snort at 646.28 seconds, and Zeek at 471.77 seconds. Although the execution times of Snort and Suricata are nearly identical, it is evident that Suricata utilizes the processor significantly more than both Snort and Zeek.

Observing the maximum memory usage reveals some drawbacks of Zeek. While it is less demanding on the CPU, it requires significantly more memory compared to Suricata and Snort. Specifically, Suricata utilized an average of 96.73MB, Snort used 102.81MB, and Zeek used 238.90MB of memory.

The remainder of the experiments took place in a physical setting, where an independent computer replayed two prerecorded network traffic files multiple times. All three IDSs—Zeek, Suricata, and Snort—were tested with these PCAP files, both with and without malicious packets included.

In the physical tests, when malicious packets were incorporated into the PCAP files, Zeek showed superior performance in terms of average CPU usage at 8.25%, outperforming both Suricata (15.00%) and Snort (28.50%). Conversely, in the virtual environment with higher network traffic, none of the IDSs exceeded a CPU usage of 25%.

Suricata performed more poorly on a busier network than on one containing malicious packets, whereas Snort managed heavier traffic more efficiently in terms of CPU usage compared to handling attack-laden packets. The CPU usage of Zeek only slightly increased under busier network conditions. From these observations, it can be inferred that Snort is more capable of handling high traffic loads with lower CPU consumption compared to Suricata. However, when it comes to analyzing packets, particularly those with attacks, Suricata outperforms Snort. While attacks also impact Zeek, the effect on its CPU usage is relatively modest.

The time each IDS spent in kernel mode correlates with its CPU usage. Snort recorded the highest average time in kernel mode at 266.41 seconds, followed by Suricata at 115.05 seconds and Zeek at 88.08 seconds. The disparity in CPU usage between Snort and Suricata is more pronounced than in the virtual environment, though the ratio of time spent in kernel mode is less significant. This suggests that while Snort consumes more CPU, it does not engage as extensively in kernel processes as Suricata. Similarly, the average time spent in user mode mirrors the trends seen in kernel mode, with Snort logging 183.04 seconds and 176.23 seconds, Suricata at 127.49 seconds and 123.25 seconds, and Zeek at 52.58 seconds and 48.13 seconds, respectively. Just as with kernel mode, the differences in time spent between Snort and Suricata in user mode are more minor than those observed on networks experiencing heavier traffic.

As in the virtual environment, Zeek required the most memory, using 209.41MB and 206.22 MB, respectively. Snort's memory usage was lower, at 83.72MB and 76.45MB, while Suricata used the least, with 54.15 MB and 54.12 MB. Compared to the virtual environment, the overall memory consumption by the IDSs was reduced. Proportionally, Suricata's memory usage decreased more significantly than Snort's. This data suggests that the heavier network traffic increases memory consumption more than merely analysing packets.

During the stress tests, Snort and Suricata did not drop any packets, unlike Zeek. As explained earlier, the dropped packages are only around 0.07% of the whole traffic analysed. However, compared to the other IDSs, Zeek lost between 8760 and 8780 packets with PCAP 1 and between 8540 and 8560 with PCAP 2.

In the physical testing environment where the PCAPs did not contain malicious packets, the results show that Snort used an average of 43.01% of the CPU, while Suricata used 32.5%. In a deviation from previous tests, Zeek used 39.2% of the CPU, more than Suricata and only slightly less than Snort. With the second PCAP file, the results were similar: Snort utilized 43.02%, Zeek 39.6%, and Suricata 31.91% of the CPU on average. The average time spent in kernel mode mirrored the CPU usage percentages. Snort operated in kernel mode for 870.87 seconds and 874.37 seconds, Zeek for 760.64 seconds and 768.67 seconds, while Suricata spent 496.02 seconds and 489.5 seconds on kernel processes. In user

mode, Suricata led with times of 569.31 seconds and 557.31 seconds, closely followed by Snort with 537.34 seconds and 536.68 seconds, and Zeek with 525.27 seconds and 524.43 seconds. This indicates a narrower disparity in time spent in user mode compared to the significant differences observed in CPU usage across the IDSs.

On average, the trends of the maximum memory used by a given IDS are very similar to the previous test runs. Zeek once again consumed the most memory with 212.63MB and 215.09 MB. Snort used 85.65 MB and 89.05MB, and Suricata, as before, needed the least amount of memory, 66.52 MB and 67.44 MB. Considering how much more CPU Zeek utilised during these test runs, the memory usage not only decreased but increased compared to the runs where malicious packets were on the network.

Despite the heavier network traffic, Suricata successfully processed all the packets that passed through it. Initially, Snort experienced some packet loss, failing to process between 20 to 200 packets as indicated by the default data from the IDS; however, this number decreased to zero in subsequent runs. In contrast, Zeek consistently failed to process a significantly higher number of packets, with losses ranging from 1980 to 1996 packets. This drop rate was substantially higher than that observed in the other IDSs.

VI. Conclusion and Future Work

Before concluding, it is essential to mention some phenomena that, although unrelated to the collected data, are nonetheless noteworthy.

We encountered several setbacks when the IDSs were being installed on the RPI4s. Notably, the most current version of the Raspbian OS was incompatible with Snort, necessitating the installation of a legacy version of the OS on the devices because the *Atomic operations library* could not execute correctly on such a device and prevented the installation of Snort version 3 from the source code.

The Suricata, by default, creates different logs. *Eve.json* contains detailed information about every packet the IDS analysed. During two weeks of operation, this file reached the size of over 42GB. Turning off the different logs according to the needs can spare disk space.

Zeek needs a lot of storage space compared to the other IDSs. In virtual environments, Snort and Suricata needed 8GB of storage, while Zeek required more than 10GB of free space for installation. Zeek's installation time was also the longest. On the VMs, it lasted about one hour, while on the RPI4s, it took more than two hours.

RPi4s have limitations. Although they are straightforward to assemble, install, and configure for basic use, microSD cards are unsuitable as storage when the device performs continuous read and write operations over several weeks. This leads to a significant issue: the devices lose their ability to perform essential functions, necessitating reinstallation.

In a virtual environment, where hardware constraints are less restrictive than an RPi, Suricata places the highest demand on the CPU, while Zeek is more intensive on memory usage. Snort emerges as an optimal solution, consuming considerably less CPU than Suricata and requiring far less memory than Zeek.

Suricata was the superior performer in a physically constrained environment when faced with malicious network traffic, utilising less CPU and memory than Snort and significantly less memory than Zeek. However, in terms of CPU efficiency, Zeek outperformed both other IDSs. Despite Zeek's lower CPU consumption, it could have handled the traffic more effectively, dropping some packets while neither Snort nor Suricata dropped any. Therefore, in scenarios with lighter traffic but potential targeted attacks, Suricata proved to be the most effective option for an RPi deployment.

In other tests, where the physical testing environment's network was not attacked but experienced much heavier traffic, Zeek consumed significantly more CPU. Although Snort still used more CPU than Suricata, the difference between them was more minor. During attack scenarios, the CPU usage gap between the two IDSs was 14% and 13%. This gap narrowed to 11% and 12% in a busier network, indicating that Suricata's CPU usage increases with heavier traffic. Unlike in previous tests, Zeek's memory usage did not decrease; instead, it increased further, marking it as the most demanding IDS regarding hardware resources. It also dropped the most packets among all the IDSs tested during the research. Meanwhile, Suricata also outperformed Snort version 3 regarding memory consumption by approximately 22MB. Snort began dropping packets during a few runs as network traffic increased.

Overall, Suricata outperformed the other IDSs in the RPis. However, its documentation for developing new modules could be more specific, leaving Snort and Zeek as alternatives. Although Zeek performed poorly, thanks to its detailed documentation, it might be considered if the primary goal is to develop new data processing methods. Snort not only performed better than Zeek but also offered comprehensive documentation on creating specific types of preprocessors.

Based on the collected data, Snort is the optimal choice for defending ships' OT networks with limited hardware resources. Since the particular use case needs a pre-processor —to handle marine-specific protocols— and anomaly detector development further research is needed to define the optimal solution.

Acknowledgement

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

Disclosure of Interests

The authors have no competing interests to declare that are relevant to the content of this article.

References

[1] H. N. Psaraftis, *The Future of Maritime Transport*. Elsevier, 2021, p. 535–539. [Online]. Available: http://dx.doi.org/10.1016/b978-0-08-102671-7.10479-8

[2] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166

[3] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100571, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555

[4] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22

[5] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean &; Coastal Management*, vol. 236, p. 106493, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1016/j.ocecoaman.2023.106493

[6] "Maritime cyber security," https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/, 06 2022, (undefined 7/4/2024 13:20).

[7] "Introduction cooperation on maritime cybersecurity atlantic council," https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/, 10 2021, (undefined 7/4/2024 13:22).

[8] "Maritime cyber resilience prosjektbanken," https://prosjektbanken.forskningsradet.no/project/FORISS/295077, (undefined 7/4/2024 13:29).

[9] "Maricybera," https://maricybera.taltech.ee/, 04 2021, (undefined 7/4/2024 13:30).

[10] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime cyber threats detection framework: Building capabilities," in *Information Security Education - Adapting to the Fourth Industrial Revolution*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds. Cham: Springer International Publishing, 2022, pp. 107–129.

[11] O. Jacq, D. Brosset, Y. Kermarrec, and J. Simonin, "Cyber attacks real time detection: towards a cyber situational awareness for naval systems," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, Jun. 2019. [Online]. Available: http://dx.doi.org/10.1109/CyberSA.2019.8899351

[12] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104

[13] "Chapter 1 - introduction to intrusion detection systems," in *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*, J. Burton, I. Dubrawsky, V. Osipov, C. Tate Baumrucker, and M. Sweeney, Eds. Burlington: Syngress, 2003, pp. 1–38. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781932266696500215

[14] D.-Y. Yeung and Y. Ding, "Host-based intrusion detection using dynamic and static behavioral models," *Pattern Recognition*, vol. 36, no. 1, pp. 229–243, 2003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0031320302000262

[15] A. S. Ashoor and S. Gore, "Importance of intrusion detection system (ids)," *International Journal of Scientific and Engineering Research*, vol. 2, no. 1, pp. 1–4, 2011.

[16] M. Pihelgas, "A comparative analysis of open-source intrusion detection systems," *Tallinn: Tallinn University of Technology & University of Tartu*, 2012.

[17] I. Mukhopadhyay, K. S. Gupta, D. Sen, and P. Gupta, "Heuristic intrusion detection and prevention system," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 2015, pp. 1–7.

[18] H. Li, G. Liu, W. Jiang, and Y. Dai, "Designing snort rules to detect abnormal dnp3 network data," in *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*, 2015, pp. 343–348.

[19] D. Fadhilah and M. I. Marzuki, "Performance analysis of ids snort and ids suricata with many-core processor in virtual machines against dos/ddos attacks," in *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020, pp. 157–162.

[20] Z. Hill, J. Hale, M. Papa, and P. Hawrylak, "Using bro with a simulation model to detect cyber-physical attacks in a nuclear reactor," in *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 22–27.

[21] A. Borkar, A. Donode, and A. Kumari, "A survey on intrusion detection system (ids) and internal intrusion detection and protection system (iidps)," in *2017 International Conference on Inventive Computing and Informatics (ICICI)*, 2017, pp. 949–953.

[22] T. Tun, K. K. Wai, and M. S. Khaing, "Performance of machine learning using preprocessing and classification for intrusion detection system," in *2023 IEEE Conference on Computer Applications (ICCA)*, 2023, pp. 260–265.

[23] S. V. Siva reddy and S. Saravanan, "Performance evaluation of classification algorithms in the design of apache spark based intrusion detection system," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 443–447.

[24] A. Garg and P. Maheshwari, "Performance analysis of snort-based intrusion detection system," in *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 01, 2016, pp. 1–5.

[25] D. H. K. Raharjo, A. Nurmala, R. D. Pambudi, and R. F. Sari, "Performance evaluation of intrusion detection system performance for traffic anomaly detection based on active ip reputation rules," in *2022 3rd International Conference on Electrical Engineering and Informatics (ICon EEI)*, 2022, pp. 75–79.

[26] B. M. Beigh and M. A. Peer, "Performance evaluation of different intrusion detection system: An empirical approach," in *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1–7.

[27] O. Bouziani, H. Benaboud, A. S. Chamkar, and S. Lazaar, "A comparative study of open source idss according to their ability to detect attacks," in *Proceedings of the 2nd International Conference on Networking, Information Systems &; Security*, ser. NISS19. ACM, Mar. 2019. [Online]. Available: http://dx.doi.org/10.1145/3320326.3320383

[28] S. Tripathi and R. Kumar, "Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer," in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 2018, pp. 80–85.

[29] A. K. Kyaw, Y. Chen, and J. Joseph, "Pi-ids: evaluation of open-source intrusion detection systems on raspberry pi 2," in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 165–170.

[30] "Snort - network intrusion detection & prevention system," https://www.snort.org/, (Accessed on 04/21/2024).

[31] "The zeek network security monitor," https://zeek.org/, (Accessed on 04/21/2024).

[32] "Home - suricata," https://suricata.io/, (Accessed on 04/21/2024).

[33] cisco. Snort rules. Accessed: 2022-04-25. [Online]. Available: https://www.snort.org/downloads/#rule-downloads

[34] S. U. of Technology and i. Design (SUTD). Terms of usage of dataset. Accessed: 2022-04-21. [Online]. Available: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/

[35] B. Ward, *How Linux works : what every superuser should know*. San Francisco, CA: No Starch Press, 2015.

Appendix 9

Publication IX
G. Visky, A. Rohl, S. Katsikas, and O. Maennel. AIS data analysis: Reality in the sea of echoes. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

AIS Data Analysis: Reality in the Sea of Echos

Gabor Visky[1], Alexander Rohl[2], Sokratis Katsikas[3], and Olaf Maennel[2]

[1]Tallinn University of Technology Tallinn, Estonia
[3]Norwegian University of Science and Technology, Gjøvik, Norway
[2]University of Adelaide, Adelaide, Australia
Email:gabor.visky@taltech.ee, alexander.rohl@adelaide.edu.au,
sokratis.katsikas@ntnu.no, olaf.maennel@adelaide.edu.au

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639765

***Abstract*—The global trend of progressive digitalisation of the world is affecting many industries, including the maritime transport sector. Electronic navigation equipment used on board modern ships has undoubtedly decreased naval accidents over the years, but these devices may suffer from cyber security vulnerabilities. The Automatic Identification System (AIS) is a well-studied navigational system with considerable weaknesses. Many publications discuss different methods for detecting anomalies in AIS. Still, validation is often missing or based on synthetic data because of the lack of publicly available AIS datasets, collected from real environments. To satisfy the need for such a dataset, we collected AIS data for six months with a receiver installed near the shore. This paper presents both the dataset and the analysis of the collected data from different perspectives; highlighting the differences between the expected and realistic features of AIS data. In our research we identified several anomalies regarding the AIS transmission propagation and periodicity, and the ship's positional data. We believe that our realistic dataset, with its labelled anomalies, will serve as an ideal testbed for developing AIS-related anomaly-detection systems.**

***Index Terms*—Automatic Identification System, AIS, maritime, dataset, data analysis, anomaly detection**

I. Introduction

Although cybersecurity is a growing concern for the maritime sector, many vendors and research institutions are making serious efforts to ease this pain. The Automatic Identification System (AIS) was introduced to increase safety at sea. Ships equipped with this system regularly broadcast their unique identifier and various data, such as: position, course over ground, draught, cargo, name and call sign. Although this system is meant to increase safety and many services rely on it, it has been shown to be insecure in several respects. Transmitted AIS data can be modified or spoofed, meaning the dissemination of false vessel information. Much research focuses on operational-technology-related anomaly detection, including AIS [1]–[5]. These publications suffer from a similar shortage; the applied results are either not validated at all or they are validated on (semi-)synthetic data, because of the lack of a real publicly-available AIS dataset. Our work herein aims to help researchers by providing AIS data collected from a real environment during a 6 month long period. Additionally, we present the results of an analysis of this dataset, which reveal some surprising differences between the expected and the experienced features of the collected AIS data.

Our data collection involved deploying an AIS receiver near the shore in Tallinn, Estonia, with a receiver that supports —unlike many commercial receivers which do not indicate invalid packets— scientific research, enabling comprehensive data analysis.

We conducted statistical analysis to understand our dataset and to test the following hypotheses:

- The main characteristics of the received packets deviate from the standards, and they contain many anomalies.
- The quality of the received messages correlates with the maximal reception distance; the broader the coverage, the more inconsistent the received packets are.
- Natural phenomena can cause anomalies in the reception of AIS signals.
- Faulty transmitters or intentional jamming may cause anomalies in the received AIS packets.

Our dataset and findings substantiate a significant contribution to the AIS research domain. We present an authentic AIS dataset, echoing the sea of real-world ships, and its exploratory analysis. The results of our analysis, which prove our hypotheses, shed light on the differences between expectated AIS behaviour and realisitc AIS data; hence serving as an ideal testbed for developing AIS-related anomaly-detection systems.

II. Background

A. Automatic Identification System

The AIS is a short-range —typically 20-100NM at sea [6], [7]— tracking system. It was developed to provide identification and positioning information to vessels and shore stations. The AIS allows ships and shore stations to track, identify, or exchange vessel-traffic details. The International Maritime Organisation (IMO), through the Safety of Life at Sea (SOLAS) Convention, requires AIS transponders to be fitted aboard every ship with gross tonnage (GT) ≥ 500, every international voyaging ship with GT ≥ 300 and all passenger ships regardless of size, to improve the safety of life at sea and the efficiency of navigation [8].

There are two different classes of AIS transponders. Class A is intended for all SOLAS vessels, such as mentioned above, while Class B AIS is intended for non-SOLAS vessels, such as domestic commercial vessels and pleasure crafts. The AIS transponder regularly broadcasts the ship's status information,

such as static details, dynamic (*e.g.* vessel position, speed, navigational status) data, and voyage (*e.g.* destination port and the estimated time of arrival of the vessel) information [9]. The dynamic AIS data are automatically transmitted every 2 to 10 seconds, depending on the speed of the vessel as detailed in Table I. The static data is transmitted every 6 minutes regardless of the vessel's speed or status [10].

The AIS has a Data Link Service (DLS) sublayer, which is responsible for providing the AIS frame format. Each AIS frame consists of the preamble, followed by the start flag and subsequently the data field, the 16-bit cyclic redundancy check (CRC) [11] field to detect errors in AIS frames, and the stop flag. Finally, a 24-bit temporary buffer supplementing the frame can be used for various purposes, such as: bit stuffing, distance delay, repeater delay, and jitter effects [10].

AIS transponders mainly use two dedicated frequencies to transmit, namely 161.975MHz and 162.025MHz in the very-high frequency (VHF) band. Since the AIS signals have a limited horizontal range, the traffic information is only available around coastal zones or in ship-to-ship range [7]. When satellites are used to receive AIS transmission to forward them towards the Vessel Traffic Services, the term Satellite-AIS (S-AIS) is used [12].

Type of ship	Reporting interval
Ship at anchor	180 sec
Speed 0-14 knots	12 sec
Speed 0-14 knots and changing course	4 sec
Speed 14-23 knots	6 sec
Speed 14-23 knots and changing course	2 sec
Speed >23 knots	3 sec
Speed >23 knots and changing course	2 sec

Table I
DEFAULT TIMING OF AIS MESSAGES. [9]

B. Effects of Natural Phenomena on Radio Communications

Mendoza-Barcenas et al. explain that solar activity can affect radiofrequency communications [13]. For example, the radiation storm caused by solar energetic particles can disrupt VHF radio communication, including AIS. According to the Space Weather Prediction Centre of the National Oceanic and Atmospheric Administration (SWPC), the K-index is used to characterise the magnitude of geomagnetic storms and is an excellent indicator of disturbances in the Earth's magnetic field. SWPC provides access to historical values of the K-index, which we used for our analysis [14].

Other natural activities influence the propagation of VHF signals. Weather conditions have been known to generate turbulence, which in turn produces gravity waves that can propagate upwards to reach the low-altitude ionospheric layers. These waves interact with the atmospheric tidal winds and may result in a skywave propagation path (known as sporadic-E layer) that would lead long-range AIS observations [15]. In our research, among others, we include examination of the unusual AIS propagations in the context of weather conditions.

III. RELATED WORK

Rich literature investigates AIS-anomaly detection. In our survey, we examined the datasets used for validating the proposed approaches. Ristic et al. introduced the statistical analysis of vessel-motion patterns, in ports and waterways, using self-reported AIS data. The authors trained and tested their anomaly detector on simulated data first and then on datasets collected in Gulf St Vincent (Port Adelaide) and Port Jackson (Sydney Harbour); neither are publicly available [1].

Hadzig et al. introduced a probabilistic graphical model for representing and managing the uncertainty of AIS data. Their work studied the impact of imperfect information and availability, and the variability of contextual information, within a probabilistic graphical model. The paper does not mention whether the model was validated on real or simulated data [2].

Shahir et al. introduced an anomaly detection framework to analyse, detect and differentiate interaction patterns and anomalies of interest for marine vessels operating in relative proximity. Their method was validated on AIS data collected by the U.S. Coast Guard. In this dataset [16] the records are filtered to one minute, meaning its characteristics are slightly different from the original one. A ship's position should be transmitted several times a minute, but the given dataset samples the transmissions at 1-minute intervals. This solution reduces the size of the data and is perfect for trajectory analysis but hides some finer details [3].

Amro et al. presented a methodical framework for scrutinising navigational messages in the standadised format of NMEA (National Marine Electronics Association) sentences encompassing analysis of sensor-derived data, potential anomalies, malicious origins of such irregularities, and the corresponding detection algorithms. Their work was validated on simulated network data, and the anomalies were created with their developed tool, NMEA-Manipulator. Since the validation data is synthetic, it is likely that its features differ from data collected from real ships [4].

Iphar et al. proposed a rule-based method for data integrity assessment, with rules built from the system's technical specifications and by domain experts. Their work was validated on automatically and manually modified AIS messages received by a terrestrial station located in Brest Roadstead (France). Although the collected data originated from a real environment, the dataset is not publicly available [5].

There are publicly available data sources providing historical AIS data, like Marrinetraffic [17], Spire Global [18] or AISHub [19]. These sources are reliable, but they contain only a fraction of the content of the received messages. This is because these entities focus mainly on the ships' trajecory, position and movement, where only aggregated data is required [20]. Additionally, these datasets are not fine-grained enough to support detailed AIS-related research.

IV. METHOD

A. Data collection

In Section III we found that there is an urgent need for a realistic AIS dataset in the research community. To curate it,

we developed our collection setup, consisting of an antenna, an AIS receiver with a built-in computer, and data collection server. The schema of the data collector system can be seen in Figure 1.

1) Antenna: The setup uses an AV200 base station antenna with a ground plane designed for land and marine service, with a tunable frequency range of 135-175MHz. The antenna was tuned to 162MHz central frequency during the setup and deployed at N59.462N, E24.666 40m ASL.

2) Receiver: The AIS receiver is a unique radio that enables access to vessel information (speed, heading, course, vessel dimensions, and other particulars) when vessels are within range. It receives AIS signals, decodes them, checks their integrity and sends the decoded data towards the navigation device in NMEA0183 sentences [10].

For this research, a Comar Systems AIS receiver (R500Ni, Comar Sytems, United Kingdom) was deployed near the port of Tallinn, Estonia, with the coverage depicted in Figure 3. This device is more than a simple receiver, since it contains an AIS receiver interfaced to a Raspberry Pi 3 (RPi) computer [21]. We used this approach to ensure the realistic quality of the analysed data. Since this receiver was located onshore, the number of received records is higher than what would have been received during a voyage in the sea because of the higher density of ships in the port or at anchor near the shore. However, our solution limits the AIS data to the messages transmitted within the coverage of our receiver.

The AIS messages contain CRC in the DLS sublayer —as introduced in Section II-A.— to provide an integrity check, done by the receiver. If the check fails, most receivers drop the packet and do not emit any NMEA sentence to indicate the failed check and the dropped message. Unlike other AIS receivers, our receiver sends an empty NMEA sentence if a received AIS message did not meet the integrity check; for example, the CRC validation was invalid, or the received packet was incomplete. This feature helped analyse such *malformed packets*. Sometimes, packets pass the integrity check —the checksum matches the payload— but the bit length for the specified message type is incorrect. Since these packets have valid CRCs and pass the integrity check, the radio cannot indicate this error; only further analysis finds this content invalid. We refer to these packets as *error packets*.

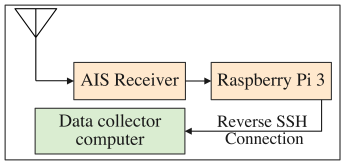


Figure 1. Data collector system's schema.

3) Data collector script: Since the radio unit of R500Ni sends the collected data to the computer unit over a serial protocol, a data collector script was written that collects all the decoded messages hourly into a file, and a scheduled task sends these files daily to the data collector server. This method provides safe storage for the collected data and ensures small file sizes for fast data loading.

4) Data collector server: During the data collection design, we estimated the limited storage of the RPi would be insufficient, so a storage server was established on the premises of the NATO Cooperative Cyber Defence Centre of Excellence. This server stores the data collected and regularly transferred from the receiver.

B. Data preparation

In the data preparation phase, the discrete one-hour-long recorded files were merged into one file, followed by the conversion of temporal annotations into UNIX time format; which measures time by the number of non-leap microseconds that have elapsed since 00:00:00 UTC on 1 January 1970. This temporal representation serves the purpose of enhancing dataset manageability. Subsequently, a comprehensive data cleansing process was executed, encompassing a spectrum of tasks and activities oriented towards identifying and rectifying errors introduced into the dataset during the data collection and acquisition phases.

During our investigation, it was observed that the receiver occasionally transmitted empty NMEA sentences in instances where a malformed message was received. A systematic examination of these messages was undertaken in response to this phenomenon. Subsequently, statistical analyses were conducted to elucidate patterns and characteristics within the dataset. These instances were treated as distinct cases, and segregated analyses were performed. All the methods mentioned above maintained consistency in treating data anomalies, ensuring a rigorous and comprehensive evaluation of the information received.

C. Outlier removal

Outlier detection pertains to identifying aberrant values within a dataset, constituting a quantitative task within error detection [22]. For the first statistical analysis, we did not remove the outliers, in order to have accurate values for the overall picture. Later, a parallel analytical approach was adopted to deal with error messages. Since these messages pass the CRC check despite their faulty content —inaccurate values within the error messages— they must be filtered out. Otherwise, they have the potential to introduce distortions into the subsequent analyses. The most eye-catching errors were the presence of random coordinates, seemingly placing the ship far beyond the reception coverage.

At first glance, we assumed latitude values below -90 or above 90 degrees or longitude values below -180 or above 180 degrees are error messages, since these values are clearly out of range and are considered outliers. However, we find special characteristics of these messages.

D. Data analysis

The computational tools employed in data analysis encompassed Python on the local computer and kaggle.com.

During this phase, the overall statistical parameters, such as the number of recorded, broken, and error messages and the daily and hourly distribution, were figured out. After the exclusion of the outliers, the positions of the "ships at anchor" and the "ships on the way using engine" were analysed. These primary results were evaluated further for anomaly detection.

E. Data degradation

Data degradation consists of all kinds of data modification that lower the level of data veracity [22]. During our anomaly analysis, controlled data degradation was performed to highlight the anomalies suppressed by regular messages. For example, to highlight the propagation anomalies, the median reception distance (MRD) was calculated every hour from each ships' positional data. This method amplified the presence of the ships from which only a few transmissions were received.

V. Results

A. Overall anaysis

The data collection period spanned 181 days from Sept. 8, 2022, 00:00, to Mar. 8, 2023, 00:00. Throughout this temporal interval, 71,251,552 AIS messages were acquired. Within this dataset, 1,058,784 messages were identified as malformed, and 1,145 records were not supported by our parser. These messages may occur because the checksum matches the payload, but the bit length for the specified message type is wrong, which we consider corrupted.

342,301 messages exhibited the presence of out-of-scope values. These messages can occur because of the previously mentioned reasons or they can be transmitted intentionally. We will provide detailed explanation of this in Section V-D.

We identified 3,779 unique MMSI numbers corresponding to the different ships.

B. Distance analysis

The computed mean of the receiver-transmitter distances was $D = 10.364$ NM, while the median was $M = 8.0$ NM. To highlight the special characteristic of the reception we grouped the unique MRDs hourly, and visualised it in Figure 4(a). This figure shows that the MRD was most often 7.5 NM, but there are slight peaks around 18, 26 and 29 NM. During these periods, the MRD increased or doubled, and in some cases, we can observe extraordinary distances. We classify these occurrences as propagation anomalies caused by solar and weather activities introduced in Section II-B.

The histogram of MRDs is represented in Figure 4(a) and their values over the time in Figure 4(b), wherein the MRDs are computed at hour-long intervals. In Figure 4(b), peaks were observed on 23/09/2022, and 7/03/2023. Our analysis indicates that these peaks are attributed to a single record stored during these hours, leading to a notable increase in the median value. So, we omitted these hours. The following maxima mean distances were documented: 20.6 NM between 14:00-15:00 14/02/2023, 20.3 NM between 01:00-02:00 12/09/2022, 20,3 NM between 01:00-02:00 02/11/2022, and 20,2 NM between 12:00-13:00 23/11/2022. During these days the MRD exhibits

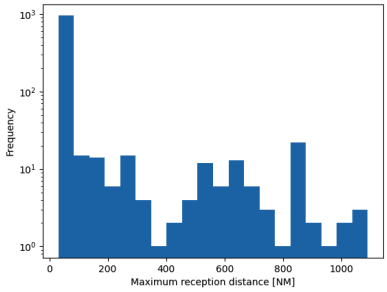


Figure 2. Histogram of the maximum reception distance.

a significant increase (Figure 3, green area), compared to the regular days (Figure 3, magenta area), but there was no reception from extremely far distances. During the same period there was no considerable solar activity. However, because of the concurrent weather condition the propagetion might have influenced by the sporadic E-layer. Figure 2 depicts the histogram of the hourly grouped maximum reception distance. It shows that, in most cases, the coverage was below 100 NM, but we experienced periods with coverage of 600, 900, 1200 NM. The analysis of the maximum distances is depicted in Figure 3. The coverage was extremely high on 08/10/2022: 1090.4 NM (red dots), on 10/12/20221210: 993.6 NM (blue dots), and on 29/11/2022: 861.1 NM (yellow dots). However, it is noteworthy that numerous signals were detected originating from distant sources, contributing to the observed phenomena. The difference between the characteristic of the propagation anomalies can also be observed in Figure 3.

C. Malformed packet analysis

We investigated the number of the received packets with incorrect checksums. According to our hypothesis, the number of these malformed packets correlates with the maximum reception distance, with the total number of the packets and with the avarage distance during a given period. To prove our hypothesis we aggregated the different values, such as number of broken or malformed packets, distances, etc. in four-hour-long periods and calculated the values. Table II summarises the results of the correlation analysis.

Table II
Correlation Analysis: Broken Packets, Maximum & Average Reception Distance, and Total Packets.

Values	Correlated Variables		
	Broken packets: Max. distance	Broken packets: Average distance	Broken packets: Total packets
t	6.216	-0.385	32.85
df	4343	4343	4343
p-value	5.569e-10	0.700	2.2e-16
correlation	0.094	-0.006	0.446
95% conf. interval	0.064	-0.036	0.422
	0.123	0.024	0.470

Regarding the correlation between the daily received broken packets and maximum reception distance, p = $5.569e^{-10}$,

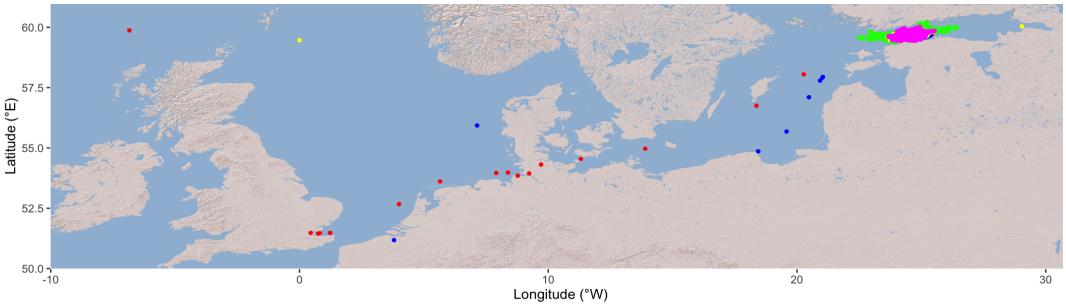
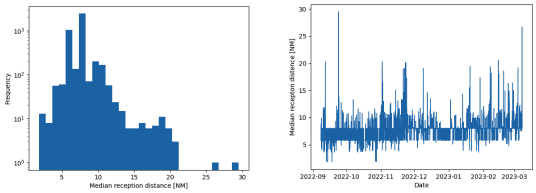


Figure 3. Propagation anomalies.



(a) Histogram of the mean reception distance.

(b) Mean reception distance.

Figure 4. Mean reception distance analysis.

which is less than the significance level $\alpha = 0.05$. From this we can conclude that these values are significantly correlated with a very weak correlation coefficient of 0.094.

The same applies to the correlation between the received malformed packets and the total number of received packets, where p = $2.2e-16$, which is less than the significance level $\alpha = 0.05$. We can conclude that these values correlate significantly with a strong correlation coefficient of 0.446.

In the case of the correlation between the received malformed packets and the MRD, we experienced a weak correlation with a correlation coefficient of -0.006 and p = 0.700, which is higher than $\alpha = 0.05$. Thus, the number of broken packets does not correlate with the MRD.

Since the receiver just indicates the existence of the broken packets but does not provide further information about their transmitter or why the integrity check has failed, we cannot investigate this further.

D. Error packet analysis

During our data collection period, we collected 342,301 error messages with correct CRC, whose values could not be valid; for example, the latitude was more than 180 degrees. This can happen if the packet changes, but the CRC remains correct, or the packet is intentionally sent. We analysed the number of these packets in Figure 5.

Most packets (277,824 messages), indicated by the blue line in Figure 5 were transmitted by a crewed vessel with MMSI (Maritime Mobile Service Identity):277824 located at N59.64589° / E25.49998°. The transmitted message type was 17, used by a base station to broadcast differential corrections for GPS. This service was started on 13/10/2022-10 at 10:48:18.

Out of the remaining 64,477 packets 63,009 were transmitted by 120 different ships with lat=91°, lon=181° positions. One of the most significant transmissions was experienced on 03/11/2022, when a burst (32,770) of navigational information messages were transmitted by MMSI:276197000, EVA320 (High-Speed Craft); however, the ship —according to its AIS messages— was moored from 31/10/2022 11:53:41 in the port of Hundipea, Estonia (59°27'33.3"N 24°43'14.1"E), and suspended its AIS transmissions from 01/11/2022 17:07:19 to 05/11/2022 00:38:59. *These packets were transmitted either intentionally or by transmitter failure.*

The remaining 1,468 packets with message types 1, 3 or 18, used for navigational information reporting, contained random positions. These packets are most probably corrupted because of propagation anomalies.

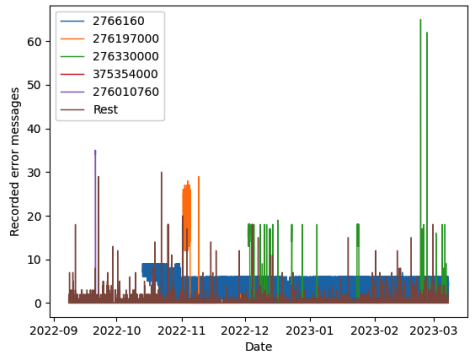
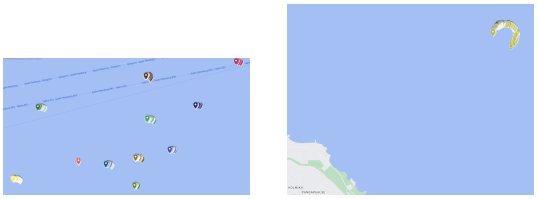


Figure 5. Number of recorded error messages.

E. Anchored ship position analysis

1) Position analysis: The position analysis of the ships at anchor is based on the type 3 messages in which the status of the ship was "at anchor". Theoretically, the ships' positions

should remain unchanged during the mooring, or the position of the closely anchoring ships should be changing similarly due to current/wind conditions. Our analysis produced different results. We identified ships which kept their position in Figure 6(a), while others moved significantly, as depicted in Figure 6(b). We identified the windy weather conditions as a possible reason. However, this pattern could have been caused by transmission of intentionally modified position.



(a) Ships without significant movement.

(b) Ship at anchor sways around on the radius of its anchor chain.

Figure 6. Ships' position at anchor.

2) Behaviour analysis: Androjna et al., among others, reported several AIS spoofing-related incidents in [23]; including the case when twelve ships reported their positions by AIS with significant error [24]. In our dataset, we observed several ships changing their position at anchor. We analysed the ship's latitude and longitude versus time to check the possible reason.

We visualised the ship's longitudinal and latitudinal coordinates over time to investigate the patterns of position changes. Our analysis revealed a discernible correlation between the shifts in position and environmental factors, particularly wind dynamics. The observed changes exhibited a smooth trajectory, indicative of natural influences rather than arbitrary or artificial manipulation. This pattern is depicted in Figure 7, where the coherent and continuous movements align with the expected behaviour influenced by wind patterns.

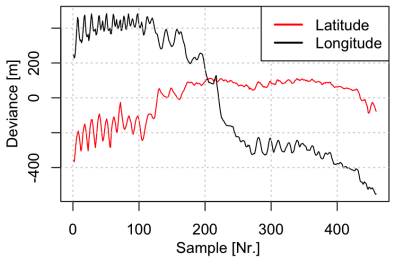


Figure 7. Ship's position deviation (S-N/W-E) from the average position.

VI. Discussion and Future Work

The accessibility of our research and the corresponding dataset stand to significantly help experts in the need for a dataset encompassing diverse anomalies. Even with the merits of our study, it is imperative to acknowledge its limitations, particularly concerning the spatial coverage of the receiver —S-AIS is outside the scope of this research— and the temporal constraints imposed by the data collection period. In our forthcoming research endeavours, we intend to conduct a comparative analysis spanning identical timeframes across different years, enhancing our investigations' temporal robustness and depth. Our dataset [25] is publicly avalilable at https://www.kaggle.com/datasets/gaborvisky/ais-dataset.

VII. Conclusion

This manuscript aims to introduce our acquired AIS dataset and its primary attributes. We employed detailed analyses to discern certain (pseudo) anomalies and explicated their underlying causative factors. While our investigation aligns with numerous studies expounded upon in Section III, our work's distinctive contribution lies in the dataset's public availability and its detailed analysis.

During a six-month-long period, we collected more than 71 million AIS messages transmitted by 3,779 unique ships. 1.5% of the messages were corrupted (failed the CRC check), which can be caused by propagation anomalies because of the long distance that degrades the packets' integrity. This proves our hypothesis: The quality of the received messages correlates with the maximum reception distance; the bigger the coverage, the more inconsistent the received packets.

0.48% of the received messages passed the CRC check but contained out-of-range values. A fraction of these packets (1,468) —since they were distributed randomly in time— were malformed because of propagation anomalies. A huge fraction of the packets were transmitted by a VTS station; still, the rest were transmitted intentionally or because of transmitter failure since we received these signals in short periods, from the same transmitter, based on the MMSI number. The identified anomaly proves this claim and our hypothesis since we found anomalies in the received packets because of faulty transmitters or intentional jamming.

We identified several propagation-related anomalies that occurred mainly during irregular weather conditions but were not directly related to solar activity. Since the weather conditions influenced our coverage over the propagation, our hypothesis that natural phenomena can cause anomalies in reception is partly proven.

We received packets at a 400 packets/minute rate, which is against the AIS message timing rules introduced in Table I, proving our hypothesis: the main characteristics of the received packets can deviate from the standards.

We find different behaviours when analysing the ships "at anchor" position. We identified the weather conditions as a possible reason. The ship's position changed smoothly on the radius of the anchor chain.

Acknowledgment

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

REFERENCES

[1] B. Ristic, B. La Scala, M. Morelande, and N. Gordon, "Statistical analysis of motion patterns in ais data: Anomaly detection and motion prediction," in *2008 11th International Conference on Information Fusion*, 2008, pp. 1–7.

[2] M. Hadzagic and A.-L. Jousselme, "Contextual anomalous destination detection for maritime surveillance," in *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.(July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy*, 2016, pp. 62–65.

[3] H. Y. Shahir, U. Glässer, N. Nalbandyan, and H. Wehn, "Maritime situation analysis: A multi-vessel interaction and anomaly detection framework," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 192–199.

[4] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104

[5] C. Iphar, C. Ray, and A. Napoli, "Data integrity assessment for maritime anomaly detection," *Expert Systems with Applications*, vol. 147, p. 113219, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417420300452

[6] T. Eriksen, G. Høye, B. Narheim, and B. Jensløkken Meland, "Maritime traffic monitoring using a space-based ais receiver," *Acta Astronautica*, vol. 58, no. 10, pp. 537–549, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0094576506000233

[7] Y. Chen, "Satellite-based ais and its comparison with lrit," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 8, no. 2, p. 183–187, 2014. [Online]. Available: http://dx.doi.org/10.12716/1001.08.02.02

[8] I. M. Organization, *Solas: Consolidated Text of the International Convention for the Safety of Life at Sea, 1974, and Its Protocol of 1988, Articles, Annexes and Certificates, Incorporating All Amendments in Effect from 1 January 2020*, ser. IMO publication. International Maritime Organization, 2020. [Online]. Available: https://books.google.hu/books?id=JKULzgEACAAJ

[9] IMO, "Resolution Resolution A.917(22) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," 2001.

[10] F. Cabrera, N. Molina, M. Tichavska, and V. Araña, "Automatic identification system modular receiver for academic purposes," *Radio Science*, vol. 51, no. 7, p. 1038–1047, Jul. 2016. [Online]. Available: http://dx.doi.org/10.1002/2015RS005895

[11] "Iso/iec 3309:1993 - information technology — telecommunications and information exchange between systems — high-level data link control (hdlc) procedures — frame structure," https://www.iso.org/standard/8561.html, (Accessed on 03/19/2024).

[12] "Satellite – automatic identification system (sat-ais) overview — esa csc," https://connectivity.esa.int/satellite-%E2%80%93-automatic-identification-system-satais-overview, (Accessed on 02/02/2024).

[13] M. A. Mendoza-Barcenas, G. M. Galvan-Tejada, O. Alvarez-Cardenas, M. Herraiz-Sarachaga, and A. Tamez-Rodriguez, "Preliminary study of space weather effects on the hf and vhf communications at low latitudes during an early stage of the solar cycle 25," in *2020 17th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*, 2020, pp. 1–6.

[14] "Planetary k-index — noaa / nws space weather prediction center," https://www.swpc.noaa.gov/products/planetary-k-index, (Accessed on 01/10/2024).

[15] A. T. Chartier, T. R. Hanley, and D. J. Emmons, "Long-distance propagation of 162 mhz shipping information links associated with sporadic e," *Atmospheric Measurement Techniques*, vol. 15, no. 21, p. 6387–6393, Nov. 2022. [Online]. Available: http://dx.doi.org/10.5194/amt-15-6387-2022

[16] "Marinecadastre.gov," https://www.marinecadastre.gov/, (Accessed on 03/18/2024).

[17] "Marinetraffic: Global ship tracking intelligence — ais marine traffic," https://www.marinetraffic.com/en/ais/home/centerx:25.7/centery:59.8/zoom:8, (Accessed on 01/14/2024).

[18] "Marine ais data - maritime ais vessel tracking solutions," https://spire.com/maritime/, (Accessed on 03/18/2024).

[19] "Free ais vessel tracking — ais data exchange — json/xml ship positions," https://www.aishub.net/, (Accessed on 01/14/2024).

[20] "Ais dispatcher free ais data sharing tool aishub," https://www.aishub.net/ais-dispatcher, 07 2017, (undefined 14/1/2024 17:34).

[21] "Comar Systems RECEIVER: R500Ni - MarineTraffic AIS Shop." [Online]. Available: https://shop.marinetraffic.com/comar-systems-r500ni.html

[22] I. F. Ilyas and X. Chu, *Data cleaning*. Morgan & Claypool, 2019.

[23] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "Ais data vulnerability indicated by a spoofing case-study," *Applied Sciences*, vol. 11, no. 11, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/11/5015

[24] "Ais mystery: 12 ships appear to cross continents and drive in circles," https://maritime-executive.com/editorials/mystery-12-ships-ais-positions-thousands-of-miles-off-and-circling, (Accessed on 03/20/2024).

[25] G. Visky, "Ais dataset," 2024. [Online]. Available: https://www.kaggle.com/ds/4703219

Appendix 10

Publication X
G. Visky, R. Vaarandi, S. Katsikas, and O. Maennel. Statistical analysis-based feature selection for anomaly detection in ais dataset. In *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 159–164, 2025

Statistical analysis-based feature selection for anomaly detection in AIS dataset

1st Gabor Visky
Dept. of Software Science
Tallinn University of Technology
Tallinn, Estonia
gabor.visky@taltech.ee

2nd Risto Vaarandi
Dept. of Software Science
Tallinn University of Technology
Tallinn, Estonia
risto.vaarandi@taltech.ee

3rd Sokratis Katsikas
Dept. of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, Norway
sokratis.katsikas@ntnu.no

4th Olaf Maennel
School of Computer & Mathematical Sciences
University of Adelaide
Adelaide, Australia
olaf.maennel@adelaide.edu.au

***Abstract*—A global trend in the progressive digitalisation of the world is affecting different industries, including the maritime transport sector. Electronic navigation and autonomous sailing heavily rely on sensor data, such as Global Navigation Satellite Systems (GNSS), Light Detection and Ranging (LIDAR), Radio Detection and Ranging (RADAR), or Automated Identification System (AIS) systems. Interference with these systems can endanger the situational awareness of the ship control system and influence navigation-related decisions. Our research focuses on AIS data and seeks possible features for anomaly detection based on transmission timing, reported and calculated speed analysis. We conducted a comprehensive statistical analysis of a 24-hour-long AIS dataset recorded in Tallinn to highlight the special characteristics of such data. Our findings suggest that the use of a single speed-based feature offers limited benefits, leading us to propose the combination of several speed-based features for anomaly detection. The results of this research have the potential to impact the cyber security of ship's navigation systems by the identified properties of AIS data.**

***Keywords*—Automatic Identification System, AIS, Maritime, Cyber Security, Anomaly Detection, Statistical Analysis**

I. Introduction

Modern society heavily depends on marine transportation, responsible for handling around 80% of global trade [1]. Over the past few decades, maritime systems have become more digitalised and interconnected to improve efficiency, leading to substantial cybersecurity challenges within the sector [2–5].

Electronic navigation equipment used onboard modern ships has undoubtedly decreased the ships' collision incidents over the years [6], but they suffer from a number of cyber security vulnerabilities [7], [8]. Melad et al. in [9] introduce 46 maritime-related cyber incidents, four of which targeted ships' operational technology (OT) systems.

A. Automatic Identification System

The Automatic Identification System (AIS) is crucial for ensuring situational awareness at sea [10], [11]. The International Maritime Organisation (IMO) requires a specified set of ships to be equipped with AIS to improve the safety of life at sea, the safety and efficiency of navigation, and the protection of the marine environment.

Ships equipped with AIS continuously broadcast their unique identifiers and other essential navigation details, such as position, speed, and course. It helps identify vessels, assist in target tracking, and simplify information exchange. Ships are sending their static and dynamic data *regularly* (Table I) over VHF of satellite link [12].

Table I. AIS Default Timing [12].

Type of ship	General reporting interval
Ship at anchor	180 sec
Ship 0-14 knots	12 sec
Ship 0-14 knots and changing course	4 sec
Ship 14-23 knots	6 sec
Ship 14-23 knots and changing course	2 sec
Ship >23 knots	3 sec
Ship >23 knots and changing course	2 sec

Since the system is not secured by design, malicious actors can spoof or jam the system [13], manipulate or falsify data, leading to the dissemination of incorrect vessel information [14–17]. Detecting anomalies in the transmitted data can promptly assist in identifying such attacks and initiating appropriate countermeasures.

This motivated the work in this paper, in which we study the transmission time between AIS messages and compare it against the standards' recommendations. Furthermore, we evaluate how efficiently the reported (by AIS) and the calculated speed of the vessel can be used for anomaly detection.

In this paper, we make the following contributions:

- We analyse a 24-hour long, real-life AIS dataset focusing on the time lapse between the messages.
- We introduce the *calculated speed* (V_{calc}) of the vessel, based on the haversine distance and the time lapse between two consecutive messages.

- We analyse the discrimination strength of the V_{calc} compared to the reported speed (V_{rep}) and the time between the messages.
- We introduce the *Speed Variance Ratio* (SVR), by leveraging the ratio of the variance of V_{calc} and V_{rep}, and we analyse its discrimination strength when used as an anomaly detection feature.

II. Related work

Extensive literature is available focusing on anomaly detection in AIS data, with approaches including statistical, rule-based, and neural network-based machine learning methods.

Amro et al. published an overview of navigation data anomaly analysis and detection. The paper targets the anomaly detection methods in NMEA messages created by malicious actors [18].

Iphar et al. [19] proposed a data quality-based integrity assessment of AIS messages and a rule-based detection approach.

Gamage et al. wrote a comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviour [20].

Ristic et al. analysed the statistics of the vessels' motion patterns in the ports and waterways based on the transmitted positions. They extracted motion patterns from historical data and constructed models using adaptive kernel density estimation to predict vessels' motion. The work focused on anomaly detection in the ship's trajectory [21].

Hadyagic and Jousselme in [22] introduced a situational analysis model for vessel tracking that can support the detecting vessel's deviation from its destination. Their Bayesian network-based probabilistic graphical model also supported the detection of anomalies in the ship's trajectory.

These papers delve deep into trajectory-related irregularities, providing a comprehensive understanding of this aspect of vessel tracking without introducing methods for the detection of anomalies in AIS transmissions or data.

Campbella et al. in [23] introduced machine learning techniques for invalid AIS message detection. The study identified several features to be evaluated by the applied methods, including the standard deviation and mean time between messages and the difference in distance calculations.

This publication motivated us to evaluate time-based and speed based features and validate they discriminating strength on real-life AIS dataset.

III. Method

A. AIS Dataset

There are publicly available AIS data feeds from Marinetraffic [24], Spire Global [25] or AISHub [26]. These sources make valuable contributions but focus mainly on the ships' trajectory, position and movement. As far as only aggregated data is available from these sources [27], these datasets are not suitable enough to support detailed AIS anomaly detection-related research. To ensure the trustworthiness of our proposed approach, we used a real-life dataset, collected with a dedicated receiver installed on the premises of the Estonian Maritime Academy, N59.462N, E24.666 40m ASL [28], [29] for testing its performance.

B. Data Preparation

Since this study analyses a fraction of the dataset, we executed a data preparation phase as Figure 1 shows. The original subset of the recorded data consisted of 425952 messages, including Class-A and B ones, from ship-on-way and on anchor, from navigational aids and vessel traffic services. Since this research focuses only on the Class-A messages transmitted by moving ships on-way, we selected only the relevant 43760 messages recorded between 08/09/2022 00:00 and 09/09/2022 00:00, providing a 24-hour long snapshot of vessel movements in the area.

During the preparation, the date and time information were converted to UNIX timestamps, which were added to all records. Based on these timestamps, the time differences for each pair of consecutive records were calculated, as well as the haversine distance between the reported positions, see equation 1.

$$V_{calc}(n) = \frac{hav(loc(n+1), loc(n))}{(unix(n+1) - unix(n))} \tag{1}$$

These values were used for the calculation of the V_{calc}, and of the variances of V_{calc} and V_{rep} for all records. This enhanced dataset was used during the analysis.

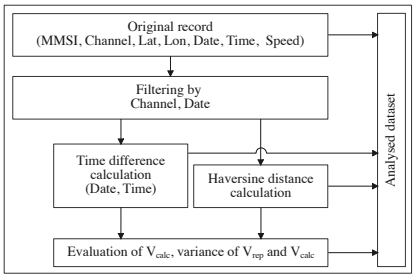


Figure 1. Flowchart of the data preparation.

C. Transmission Timing Analysis

To better understand the transmission timing, we analysed the transmission timing against the ship's speed, as presented in Table II. This comparison was necessary to explore whether variations in transmission timing could be correlated with the vessel's speed.

D. Calculated Speed Analysis

The analysed packets contain both the ship's positional data and its speed (V_{rep}). As introduced in Section III-B, we obtained the V_{calc}, representing the calculated speed based on the reported positions. With both the V_{rep} and V_{calc} in hand, we conducted a series of tests to evaluate the effectiveness of correlating these two data sets. Specifically, we focused on

measuring the correlation strength and calculating the average difference between the V_{rep} and V_{calc} across various time intervals and conditions.

Based on the variance of V_{rep} and V_{calc} we calculated the Speed Variance Ratio (SVR) (equation 2), that we also used as a feature.

$$SVR(V_c, V_r) = \begin{cases} var(V_{calc})/var(V_{rep}), & \text{if } V_{calc}) \geq V_{rep} \\ var(V_{rep})/var(V_{calc}) & \text{otherwise} \end{cases} \quad (2)$$

IV. Results

A. Results of the Transmission Timing Analysis

As it can be seen in Table I, the standard defines exact timing values for AIS transmission. Table II shows the calculated time differences between the received messages. The analysis revealed that the timing of transmissions did not adhere to the requirements set forth by the AIS communication standard, which mandates specific timing intervals based on vessel speed and other factors.

Table II. Results of AIS timing results.

Time [s]	Speed [kts]			Total
	<14	14-23	23<	
<1.5	70	15	0	85
1.5-2.5	0	0	0	0
2.5-3.5	3	2	2	7
3.5-5	321	1370	**2736**	4427
5-9	41	116	167	323
9-16	460	**10001**	48	10509
16-30	**21403**	1271	19	22693
30-45	3167	299	5	3471
45-70	767	195	4	966
70-	1080	189	9	1278
Total	27312	13458	2990	43760

The comparison of the standard-defined timing vs. calculated time differences of the real life dataset can be seen in Table III.

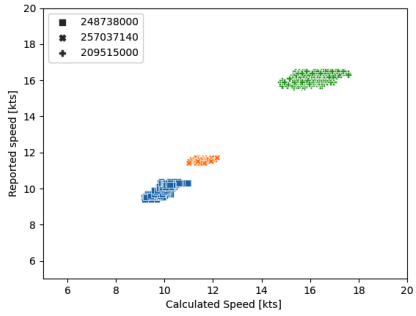
Table III. AIS Timing analysis.

Reported speed [kts]	0-14		14-23		>23	
Number of messages	27312		13458		2990	
Expected timing [s]	4.0	12.0	2.0	6.0	2.0	3.0
Measured timing [s]	3.5-5.0	9.0-16.0	1.5-2.5	5.0-9.0	1.5-2.5	2.5-3.5
Number of reports	321	460	0	116	0	2
Correct category [%]	1,17	1,68	0.0	0,86	0.0	0,001

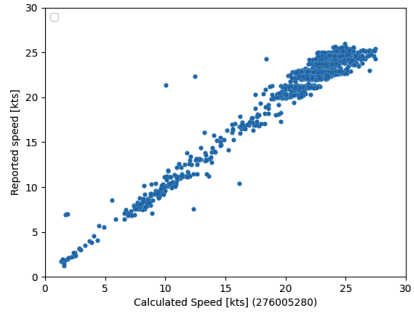
The results show that in most cases, the transmission intervals did not align with the expected timing based on the ship's speed, indicating the method's low reliance.

B. Overview of the Calculated and Reported Speed Analysis

We generated scatter plots to gain deeper insights into the differences between calculated and reported speeds. These visualisations help identify patterns and deviations that may take time to be apparent through raw data analysis alone. Figure 2 illustrates vessels exhibiting minimal deviations in their reported speeds. Specifically, in Figure 2a, we observe three ships maintaining a nearly constant speed over time, suggesting high accuracy and consistency in their AIS-transmitted speed data. This consistency indicates either routine maritime operations or reliable transmission of the ship's speed information. In contrast, the plot in Figure 2b shows a vessel with a more dynamic speed profile, where the ship's speed fluctuates over time. Such variations could be attributed to various operational factors, such as manoeuvring in congested waters, responding to environmental conditions, or engaging in different phases of its voyage, like accelerating or decelerating. These speed changes are captured effectively in the plot, allowing us to compare the reported data against the calculated speed values and observe any discrepancies.



(a) Ships with constant speed



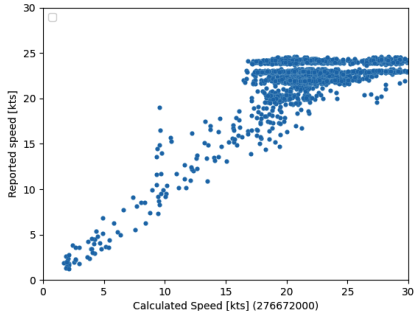
(b) Ship with changing speed

Figure 2. Ships with consistent speed data.

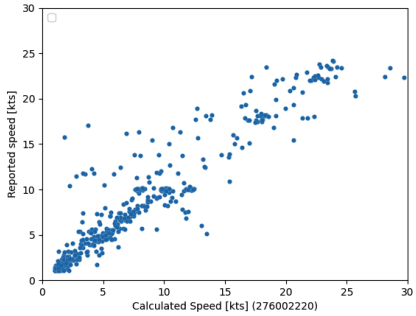
Figure 3 illustrates vessels that exhibit a higher degree of speed deviation, highlighting potential discrepancies between the calculated and reported speeds. Such deviations could be indicative of irregularities in the AIS data or other operational factors influencing the vessel's speed.

In particular, Figure 3a demonstrates that as the ship's speed increases, the calculated speed shows greater deviation from the reported values. This pattern suggests that higher speeds may amplify inaccuracies in the transmitted data, possibly due

to limitations in AIS reporting regularities. Figure 3b presents a ship where the deviation between the reported and the calculated speed is larger. This could suggest that the vessel's speed calculation more inaccurate.



(a) Ship with increasing speed.



(b) Ship executing complex operation.

Figure 3. Ships with deviating speed values.

These figures suggest that the correlation between V_{rep} and V_{calc} speed can indicate anomalies.

C. Speeds' Correlation as feature

Our analysis shows that the correlation between V_{rep} and V_{calc} does not necessarily correlate with anomalies. The values of the Pearson correlation coefficient between the V_{rep} and V_{calc} of the ships (MMSI: 248738000, 257037140, 209515000) depicted in Figure 2a vary, namely they are 0.843, 0.339, 0.412 respectively, while in the case of ships depicted in Figure 3a and 3b the correlation is high, despite the significant error in high speeds and the reporting error.

The low variance of the speed is the reason for the varying correlation in the case of ships with MMSI 248738000, 257037140, and 209515000, so this feature is reliable only if the speed variance is high.

D. Absolute Average Speed Difference (AASD) as a feature

The value of the average difference between the V_{calc} and V_{rep} can serve as a feature for detecting anomalies in the data. This difference can reveal discrepancies that may indicate irregular behaviour. A higher AASD suggests a greater likelihood of anomalous data, which may reflect unexpected deviations from typical or expected speed patterns. Therefore, monitoring the average difference between V_{calc} and V_{rep} is a good candidate for anomaly detection.

Table IV. Correlation and avarage speed differnce.

MMSI	Correlation between RS and CS	Calculated Speed's Variance	Reported Speed's Variance	Speed Variances Ratio	Avarage Speed Difference
248738000	0.843	0.147	0.104	1.413	0.167
257037140	0.339	0.049	0.007	7.00	0.159
209515000	0.412	0.273	0.054	5.056	0.383
276672000	0.727	18.788	10.078	1.864	2.310
276002220	0.937	42.440	41.195	1.030	1.311
256332000	0.072	2.995	0.008	374.375	1.021
636021907	0.050	8.564	0.046	186.17	1.582
636022144	0.335	1.613	0.192	8.401	1.052

While the AASD was initially considered a good candidate, our results indicate that it is not reliable. The high variance in V_{calc}, particularly at higher speeds, diminishes the effectiveness of this metric in identifying anomalies. As speeds increase, the natural fluctuation in V_{calc} becomes more pronounced, which can obscure meaningful deviations and lead to the potential for false positives or missed anomalies.

E. Speeds Variance Ratio as a feature

Naturally, V_{calc} and V_{rep} are expected to have similar values, similar behaviour. To represent the behaviour similarity we introduced SVR, calculated according to equation 2. The similarity is evident in the case of ships with MMSI 248738000, 257037140, 209515000, and 276002220, where the V_{calc} and V_{rep} closely align. However, this ratio tends to increase at higher speeds, indicating a growing discrepancy between V_{calc} and V_{rep}. As speed increases, the variation in V_{calc} becomes more pronounced, and the alignment with V_{rep} diminishes. Consequently, SVR has limited discrimination strength, especially at higher speeds, where the variance becomes too large to detect anomalies reliably. The increased SVR at high speeds reduces the utility of this feature for anomaly detection, as it fails to distinguish between normal and anomalous behaviour consistently.

F. Discrimination by multiple features

SVR and AASD did not provide us strong enough features, so we used them together, to achieve better results, since a high SVR, which reflects the growing discrepancy between the variance of V_{calc} and V_{rep}, coupled with a high AASD, signals a significant deviation from expected speed patterns. Together, these features provide a clearer distinction between normal and anomalous data, as depicted in Figure 4.

Based on these features, with K-Means clustering method, we identified ships demonstrating irregular behaviour, depicted in Figure 5.

At the same time we judged 276002220 and 276672000 depicted in Figures 3a and Figure 3b irregular as well; however these ships just executed complex operations.

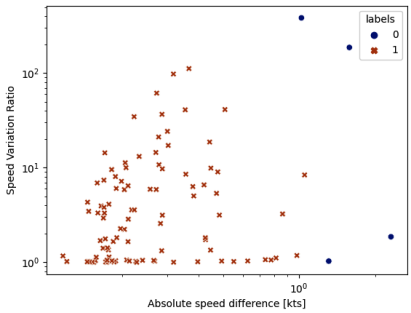


Figure 4. Plot of AVS vs. AASD

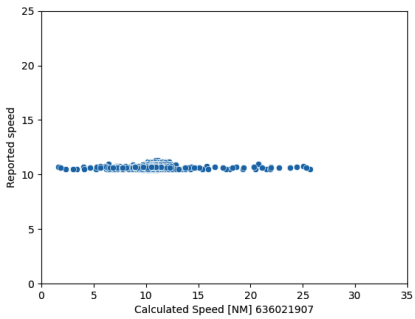


Figure 5. Ship with irregular behaviour.

V. Discussion and Conclusions

In conclusion, the anomaly detection approach based on transmission timing has yielded limited results. While this method can help identify irregularities in the timing of AIS transmissions, it appears insufficient for detecting more subtle or sophisticated forms of data manipulation or cyberattacks. The reliance on timing alone does not account for various external factors, such as communication delays or environmental influences, which may cause benign variations in transmission intervals.

As highlighted in Section IV-A, the measured timing values do not follow the standards. A possible reason lies in the transmission organisation of AIS. Since the AIS is based on self-organised time division multiple access (SOTDMA) and dynamic slot reservation (DSR) selection method under high data link load condition, multi-user conflicts may occur, which brings difficulties to the dynamic monitoring of the ships, because of the overlapping of candidate slots [30].

Although the AIS transmitter sends the packets with a certain regularity, the receiver side receives only 0.0-16.8% of the packets with correct timing, which leads to a doubled or tripled time interval.

According to [31] the transmitters must change their time slot regularly to maintain DSR. It can lead to shorter time difference if the transmitter allocates the new time slot closer to the old one. These characteristics reduces the time interval's discrimination strength.

Regarding the difference between V_{calc} and V_{rep} we can conclude that the higher speed the higher the difference. As Figure 6 shows, the reporting that we experience higher difference when the time delay between the reports is lower. According to the standards, it happens, when the ship changes its course, what explains the higher V_{calc} calculation error.

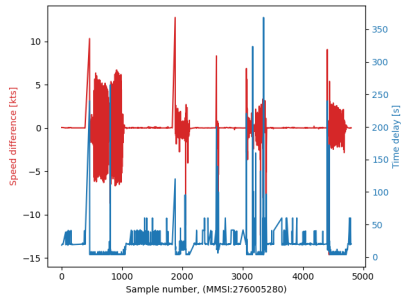


Figure 6. Plot of V_{calc} and V_{rep} difference, and reporting time.

Furthermore, we can conclude that the correlation between V_{calc} and V_{rep} and the individual features SVR and AASD can be valuable indicators for anomaly detection. However, these correlations come with certain limitations. Their performance is highly dependent on the ship's speed and trajectory, as higher speeds and complex manoeuvres introduce more significant variability, reducing the accuracy of these features when used in isolation.

To mitigate these challenges, we recommend using SVR and AASD together for anomaly detection. The complementary nature of these two metrics allows for a more robust detection of anomalies. By leveraging both features, the system can more effectively account for variations in speed and trajectory, providing a stronger basis for identifying anomalies.

Together with all the results, it is important to keep in mind that the identified anomalies are due to calculation error or potentially faulty AIS transmitter setups or malicious activity. While the combined features of SVR and AASD serve as effective tools for anomaly detection, the root cause of many detected irregularities is likely related to course or speed changes, AIS reception irregularities, or calculation error.

We can consider faulty AIS setups, that can lead to inconsistent or inaccurate transmission of speed and positional data, causing discrepancies between V_{calc} and V_{rep}, and thus triggering high SVR and AASD values. As such, while these features are valuable for detecting anomalies, it is crucial to

consider the possibility of AIS transmitter issues as a primary factor behind the observed data irregularities.

VI. Future work

In our future work, we plan to develop and train a better model capable of distinguishing between regular and anomalous cases more accurately and create a system that can automatically identify irregular behaviour while accounting for factors such as the ship's speed, trajectory, and potential external influences.

By leveraging the insights gained from features such as SVR and AASD, along with other relevant parameters, the model will aim to improve the detection of anomalies in maritime data. The goal is to create a system that can automatically identify irregular behaviour while accounting for factors such as the ship's speed, trajectory, and potential external influences.

Acknowledgment

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360).

References

[1] H. N. Psaraftis, *The Future of Maritime Transport*. Elsevier, 2021, p. 535–539. [Online]. Available: http://dx.doi.org/10.1016/b978-0-08-102671-7.10479-8

[2] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean &; Coastal Management*, vol. 236, p. 106493, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1016/j.ocecoaman.2023.106493

[3] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000166

[4] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection*, vol. 39, p. 100571, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000555

[5] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/22

[6] S.-B. Hong, "A study on the effects of e-navigation on reducing vessel accidents," 2015.

[7] B. Svilicic, 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, 2019. [Online]. Available: https://www.mdpi.com/2077-1312/7/10/364

[8] M. S. Lund, J. E. Gulland, O. S. Hareide, ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–5.

[9] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, no. 3, pp. 519–530, 2021. [Online]. Available: https://doi.org/10.12716/1001.15.03.04

[10] "AIS for Safety and Tracking: A Brief History - Global Fishing Watch," [Online]. Available from: https://globalfishingwatch.org/article/ais-brief-history/, (Accessed on 09/20/2024).

[11] "IALA GUIDELINE - An overview of AIS," [Online]. Available from: https://www.navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf, (Accessed on 09/20/2024).

[12] IMO, "Resolution Resolution A.917(22) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," 2001.

[13] D. McFadden, R. Lennon, and J. O'Raw, "AIS transmission data quality: Identification of attack vectors," in *2019 International Symposium ELMAR*. IEEE, Sep. 2019. [Online]. Available: https://doi.org/10.1109/elmar.2019.8918672

[14] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "AIS data vulnerability indicated by a spoofing case-study," *Applied Sciences*, vol. 11, no. 11, p. 5015, May 2021. [Online]. Available: http://dx.doi.org/10.3390/app11115015

[15] A. Androjna, I. Pavić, L. Gucma, P. Vidmar, and M. Perkovič, "AIS data manipulation in the illicit global oil trade," *Journal of Marine Science and Engineering*, vol. 12, no. 1, p. 6, Dec. 2023. [Online]. Available: http://dx.doi.org/10.3390/jmse12010006

[16] "Above us only stars - C4ADS," https://c4ads.org/reports/above-us-only-stars/, (Accessed on 09/20/2024).

[17] D. M. Valentine, "Now you see me, now you don't: Vanishing vessels along argentina's waters," Oceana, Tech. Rep., 2021. [Online]. Available: https://zenodo.org/record/4893397

[18] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104

[19] C. Iphar, C. Ray, and A. Napoli, "Data integrity assessment for maritime anomaly detection," *Expert Systems with Applications*, vol. 147, p. 113219, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417420300452

[20] C. Gamage, R. Dinalankarac, J. Samarabandu, and et al, "A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors," *WMU J Marit Affairs*, vol. 22, p. 447–477, 2023.

[21] B. Ristic, B. La Scala, M. Morelande, and N. Gordon, "Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction," in *2008 11th International Conference on Information Fusion*, 2008, pp. 1–7.

[22] M. Hadzagic and A.-L. Jousselme, "Contextual anomalous destination detection for maritime surveillance," in *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.(July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy*, 2016, pp. 62–65.

[23] J. N. Campbell, A. W. Isenor, and M. D. Ferreira, "Detection of invalid AIS messages using machine learning techniques," *Procedia Computer Science*, vol. 205, pp. 229–238, 2022, 2022 International Conference on Military Communication and Information Systems (ICMCIS). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050922008894

[24] "MarineTraffic: Global Ship Tracking Intelligence | AIS Marine Traffic," [Online]. Available from: https://www.marinetraffic.com/, (Accessed on 01/14/2024).

[25] "Marine AIS data - Maritime AIS vessel tracking solutions," [Online]. Available from: https://spire.com/maritime/, (Accessed on 03/18/2024).

[26] "Free ais vessel tracking | ais data exchange | json/xml ship positions," [Online]. Available from: https://www.aishub.net/, (Accessed on 01/14/2024).

[27] "AIS Dispatcher free AIS data sharing tool AISHub," [Online]. Available from: https://www.aishub.net/ais-dispatcher, 07 2017, (Accessed on: 14/1/2024 17:34).

[28] G. Visky, "Ais dataset," 2024. [Online]. Available: https://www.kaggle.com/ds/4703219

[29] G. Visky, A. Rohl, S. Katsikas, and O. Maennel, "Ais data analysis: Reality in the sea of echos," in *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, 2024, pp. 1–7.

[30] L. Liping and M. Shexiang, "Analysis and simulation of slot collision and reception performance of ais," in *Advances in Electric and Electronics*, W. Hu, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 661–669.

[31] *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*, ITU-R Radiocommunication Sector of ITU, 2014, recommendation ITU-R M.1371-5.

Appendix 11

Publication XI
A. S. Benterki, G. Visky, J. Vain, and L. Tsiopoulos. Using Incremental Inductive Logic Programming for learning spoofing attacks on maritime automatic identification system data. In S. Bauk, editor, *Maritime Cybersecurity*, pages 123–141. Springer Nature Switzerland, Cham, 2025

Using Incremental Inductive Logic Programming for Learning Spoofing Attacks on Maritime Automatic Identification System Data

Aboubaker Seddiq Benterki, Gabor Visky, Jüri Vain, and Leonidas Tsiopoulos

Abstract The Automatic Identification System (AIS) is a tracking system used in vessels and vessel traffic control services to identify and locate vessels and is being regarded as the main tool for complementing the navigator's direct visual/audible information augmented with RADAR data to prevent collisions at sea. Despite its criticality, AIS in its general use, with the corresponding message broadcasting protocol, is not secured from cyberattacks. Its security vulnerabilities have been extensively discussed in the literature and several real incidents have been reported. To address this issue several research papers have been published proposing anomaly/attack detection systems based either on machine learning (ML) approaches requiring large datasets or on logic-based rule systems built with the help of maritime experts. In this chapter we propose an alternative ML approach to develop an attack detection system using Inductive Logic Programming (ILP), a symbolic AI method, to incrementally learn rules that help detect anomalies in AIS data that potentially could indicate spoofing attacks. As a main result, we demonstrate that ILP frameworks that combine relational logic and numerical reasoning stand out for the ability to generalise from a small set of

Aboubaker Seddiq Benterki
Department of Software Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: aboubaker.benterki@taltech.ee

Gabor Visky
Department of Software Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: gabor.visky@taltech.ee

Jüri Vain
Department of Software Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: juri.vain@taltech.ee

Leonidas Tsiopoulos
Department of Software Science, Tallinn University of Technology, Ehitajate tee 5, 19086, Tallinn, Estonia e-mail: leonidas.tsiopoulos@taltech.ee

examples and provide explainable evidence of anomaly occurrence, making it suitable for operational use in maritime environments

Key words: anomaly detection, inductive logic programming, automatic identification system, maritime, cyber, security, AIS, ILP

1 Introduction

Maritime transport has significant role in the global economy [1]; however, it is vulnerable to disruptions impacting severely whole global chains of trade [2]. Therefore, academia, industry, and public sector have recognised the need to improve the sector's resilience equalising its importance with other critical aspects in the maritime domain [3–7].

In 2017 and 2022, the IMO released guidelines with high-level recommendations on maritime cyber risk management to promote effective cyber risk management and protect the shipping industry from cyber threats and vulnerabilities [8, 9].

International Ship and Port Facility Security (ISPS) Code established by the IMO partly regulates the cybersecurity risk assessment [10]. These regulations do not specify particular characteristics of cybersecurity solutions on a ship.

In June 2017, the Maritime Safety Committee also adopted the resolution for Maritime Cyber Risk Management in Safety Management Systems to encourage administrations to appropriately address cyber risks in existing safety management systems [11].

One of the key components to assure situation awareness at sea is the Automatic Identification System (AIS) [12, 13]. Vessels outfitted with AIS continuously transmit their unique identification along with other vital navigation data. Despite the criticality of AIS, its communication protocol is not secured from cyberattacks. This, in turn, makes AIS a desirable target of cyber crime by altering or falsifying data and allowing the spread of inaccurate information about vessels [14–17]. Timely detection of anomalies in the transmitted data can help the identification of such attacks and trigger adequate countermeasures.

Current research literature increases rapidly in the number of approaches focusing on anomaly detection in AIS data, with approaches ranging from statistical and rule-based [18–22], to exploiting neural network (NN) based machine learning (ML) methods [23, 24]. However, there is an alternative ML methods group, based on inductive logic programming (ILP), introduced by Muggleton [25], that surprisingly has not got any attention in existing works, though ILP has demonstrated a series of advantages over other ML methods. The advantages include the ability to generalise from small numbers

of training examples, natural support to lifelong and transfer learning, ability to learn complex relational theories, and explainability of learning results [26].

To our best knowledge, in this chapter, ILP is applied first time for anomaly detection in real-life AIS data. According to our experimental results on real AIS data collected at the harbour of Tallinn, we demonstrate that ILP extended with the support for learning also numerical relations can efficiently learn various AIS attack signatures and generalize them in the form of compact set of attack detection rules.

The rest of the chapter is organised as follows. In Section 2 we present preliminaries of AIS, ILP and an extension of ILP that we use in this chapter to learn logic programs combining relational logic and numerical reasoning. In Section 3 we discuss the related works. In Section 4 we present our method and in Section 5 we evaluate it on a real-life dataset. In Section 6 we conclude this chapter and discuss the future work.

2 Preliminaries

2.1 Automatic Identification System (AIS)

The AIS is a coastal tracking system designed for short-range monitoring, typically effective up to a distance of 20-100 nautical miles (NM) at sea, depending on the setup [27, 28]. It was created to offer identification and positioning data to vessels and coastal stations, enabling them to monitor, identify, and share information about marine traffic. The International Maritime Organization (IMO), under the Safety of Life at Sea (SOLAS) Convention, mandates that AIS transponders be installed on international voyaging ships with a gross tonnage (GT) of 300 or more, all ships with a GT of 500 or above, and on all passenger ships irrespective of size. This requirement aims to enhance safety and navigation efficiency at sea [29].

AIS transponders are available in two different classes. Class A transponders are required for all SOLAS-compliant vessels, as previously mentioned. Class B transponders, on the other hand, are designed for non-SOLAS vessels, including domestic commercial vessels and pleasure crafts.

The installed AIS transponder regularly broadcasts information on the ship's status, such as static details, dynamic (e.g., vessel position, speed, navigational status) data, and voyage (destination port and the estimated time of arrival of the vessel) information [30]. The dynamic AIS data are automatically transmitted every 2 to 10 seconds, depending on the vessel's speed, as detailed in Table 1. The static data is transmitted every 6 minutes regardless of the vessel's movement speed or status [31].

Type of ship	Reporting interval
Ship at anchor	180 sec
Speed 0-14 knots	12 sec
Speed 0-14 knots and changing course	4 sec
Speed 14-23 knots	6 sec
Speed 14-23 knots and changing course	2 sec
Speed >23 knots	3 sec
Speed >23 knots and changing course	2 sec

Table 1 Default timing of AIS messages [30].

2.2 Inductive Logic Programming

ILP studies learning from examples, within the framework provided by clausal logic. The examples and background knowledge are given as clauses, and the theory that is to be induced from these, also consist of clauses. ILP uses logic programming as a uniform clausal representation for examples, background knowledge and hypotheses learned. Given an encoding of the known background knowledge and a set of examples represented as a logical database of facts, an ILP system derives a hypothesised logic program which entails all the positive and none of the negative examples. Formally,

- given a finite set of clauses B (background knowledge), and sets of clauses $E+$ and $E-$ (positive and negative examples, respectively),
- find a theory Σ, such that $\Sigma \cup B$ is correct with respect to $E+$ and $E-$.

By the correctness of theory Σ we mean that $\Sigma \cup B \models e+, \forall e+ \in E+$ (*completeness*), and $\Sigma \cup B \not\models e-, \forall e- \in E-$ (*consistency*). The two basic steps in the search for a correct theory are *specialisation* and *generalisation*. If the current theory together with the background knowledge entails some of the negative examples, it is too strong and needs weakening, i.e., specialisation, such that the new theory and the background knowledge are consistent with respect to the negative examples. If the current theory together with the background knowledge does not imply all positive examples, it needs to be strengthened (generalised) by finding a more general theory such that all positive examples are implied.

In ILP setting we now formulate the learning task as the task of learning rules that generalise correct AIS data exchange and, thus, by monitoring AIS data and checking them against learned rules (in terms of ILP theory) it allows distinguishing anomalies from normal AIS data. This, in turn, could indicate the possibility of cyber incidence, e.g., spoofing attacks. As a case study, the positive examples are based on a small (but sufficient) subset of real AIS data collected at the harbour of Tallinn and the negative examples are based on extracted samples from the same subset of data which violate the accuracy constraint for the reported consecutive vessel positions. Addi-

tionally, we injected fake vessels into this dataset to simulate spoofing attacks (see subsection 4.2.3).

2.3 Relational Program Synthesis with Numerical Reasoning(NUMSYNTH)

NUMSYNTH [32] is an ILP framework designed to learn programs that combine relational logic and numerical reasoning. While many ILP frameworks primarily focus on learning Prolog programs with symbolic reasoning, NUMSYNTH extends this by learning programs with numerical values, crucial for tasks involving continuous domains like real numbers or discrete domains of integers. NUMSYNTH ensures that for each positive example, a learned hypothesis includes numerical constraints that cover the positive examples. In contrast, for each negative example, the hypothesis excludes the values that would entail it. NUMSYNTH incorporates this form of reasoning by using two stages: program search and numerical search. In the first stage, partial programs are generated with numerical variables. In the second stage, satisfiability modulo theories (SMT) solvers are employed to search for appropriate numerical values that fit the training data. This two-stage process allows NUMSYNTH to handle infinite numerical domains and derive numerical thresholds, constraints, or inequalities from multiple examples. The system's ability to reason over examples jointly, rather than individually, distinguishes it from other ILP systems that struggle with complex numerical relationships.

3 Related work

Since the AIS system is not designed to be resistant against cyberattacks, it brings severe vulnerability into the Vessel Traffic Service systems. Balduzzi et al. [33, 34] introduced the security consideration related to this system. Due to this, a lot of research has been conducted to identify anomalies in AIS data, including anomalies possibly caused by cyberattacks.

Several research works focused on the identification of anomalies in ship trajectories by applying different methods. Ristic et al. [35] used statistical analysis of the position of the ships for anomaly detection in trajectory, with promising results, however their method generated high false positive alerts.

Kowalska and Peel [36] used data-driven, non-parametric Bayesian model with active learning for anomaly detection in ships' trajectory. Vespe et al. [37] applied unsupervised learning for anomaly detection in maritime traffic patterns, using real-time and historical AIS data. The method successfully identified ships violating the traffic separating zones and prohibited areas.

Katsilieris et al. [38] studied the trustworthiness of AIS data with the help of radar measurements and information from the tracking system. The applied log-likelihood ratio test delivered good results, especially if the data from the AIS and RADAR system deviated enough.

Coleman in his thesis applied and analysed several different ML-based anomaly detection methods on the heatmap of ships' location based on data [39].

Kontopoulos et al. [40] studied the detection of data spoofing and falsification attacks in real-time environment. Their method determines the average speed needed to travel along the shortest route between two consecutive locations reported via AIS. If the computed speed falls within a realistic range, the next message is accepted as the new last valid position for that vessel. If not, the message is marked as potentially spoofed. With this approach they achieved moderate results.

Kullberg et al. [41] developed a method that recursively learned a model of the nominal vessel routes from AIS data and simultaneously estimated the current state of the vessels. The method also distinguished anomalies and measurement outliers. Statistical testing relative to a current motion model was applied and the method was evaluated against historical AIS data showing that previously unseen motions could be detected.

d'Afflisio et al. [42] proposed an anomaly detection strategy based on a multiple hypothesis testing framework using two approaches. The first approach was based on the generalised likelihood ratio testing and the second approach was based on the model-order selection methodology applying an appropriate penalty term to the maximised log-likelihood based on the statistical model for the vessel kinematic. Anomaly detection rules were then derived and the effectiveness of the approach was demonstrated against simulated data.

All the approaches discussed above brought good results, however they did not consider any further characteristics of the AIS transmissions, like transmission periodicity, etc.

Lane et al. [43], besides the trajectory-related anomalies, considered the unexpected AIS activity as anomalous behaviour focusing on the *existence* of the transmissions. The priory used approach generated false positives, if a signal was received from a priory not covered area, so the authors improved this method by building a receiver coverage map. This approach works with land-based receivers, but on the sea its usefulness is questionable. To determine the probability of a higher-level threat, a general Bayesian network-based method was used.

Iphar et al. [22] proposed a rule-based method for AIS data integrity assessment, with rules derived manually from the system's technical specifications and with help by domain experts. The study focused on the different characteristics of the transmitted data, like consistency, next position violation, (dis)appearing of a transmitter, etc. Correctness checking of the 935 descrip-

tion logic-based rules was not discussed. 666 of these rules were implemented in Python as part of an AIS data anomaly detection component.

Blauwkamp et al. analysed 334 million AIS messages. They conducted statistical analysis, supervised classification and unsupervised clustering for feature selection and proposed the implementation of a behaviour-based anomaly detection system based on leveraging deep neural networks, historical AIS data, and logic rules [44]. Their method uses message types, location, velocity and other attributes with known behaviour for training the model to identify deviations in message patterns. Another indicator of aberrant activity is a deviated or unknown response sequence to a base station's interrogation.

Louart et al. [45] developed a method for detection of AIS messages falsifications and spoofing by checking messages compliance with the time-division multiple access (TDMA) communication protocol, which is the protocol employed for AIS data broadcasts. The authors applied a Kalman filter to track every vessel and to assess the consistency of their velocity data sent because the vessel velocity can affect the TDMA protocol. The proposed method was validated on real data and showed promising results, being at the same time computationally cheap for real-time application. Importantly, the authors provided open-access to the source codes to foster research activities from both industry and academia in this field.

Louart et al. [46] also developed an approach that detects AIS identity spoofing combining the tracking of the vessel position and AIS transceiver's carrier frequency offset caused by the carrier frequencies mismatch between emitter and receiver and Doppler effect. This offset is used as a radiometric signature to identify every transceiver independently of its transmitted identity. The offset can drift over time and, thus, it is tracked by a Kalman filter. Vessel position is also considered to reduce the miss probability of spoofing detection. The method was tested on real AIS data and the results demonstrated very low false alarm (1%) and miss probabilities (1.7%). The algorithm and AIS data used are open access.

Similarly to the work by Coleman [39] that compared different ML techniques for trajectory anomaly detection, Campbell et al. [23] compared several different ML techniques to identify the most suitable ones for the detection of AIS spoofing, motivated by a real event in the North Atlantic in April 2020 where more than 200 fake vessels appeared suddenly. The AIS data fields considered were the MMSI, date, time, SOG, COG, latitude, and longitude. Data cleaning involved removal of duplicate messages and of records that contained physically invalid entries. The final dataset covered April 1 - 30, 2020 and contained 19,029 data entries. The dataset had 17,853 entries that belonged to the valid vessel class and 1176 entries as part of the invalid vessel class. The data set was divided into a training, validation, and test set with a 60% / 20% / 20% split, respectively. The ML techniques investigated were K-means clustering, Decision Tree (DT), Random Forest (RF), Feed-Forward Neural Networks (FNN), Support Vector Machines (SVM), and One-Class

Support Vector Machines (One-SVM). The results showed that DT, RF, and FNN best identified the fabricated AIS messages with F1 scores greater than 93 percent on the test data.

For an additional comprehensive review on supervised and unsupervised ML techniques to detect abnormal activities, behaviours, and intents in AIS data, the reader is referred to the review paper by Gamage et al. [24].

Based on our review of existing literature, various methods have been employed for anomaly detection in identifying attacks against AIS, each yielding different strengths and weaknesses. Compared to the ML and rule-based approaches described above, our method requires much less AIS data to automatically learn logically correct-by-construction anomaly detection rules and it does not require a complex mathematical model of the vessel kinematics nor extensive expert involvement to guide the feature extraction and efficient rule formation. Further more, our method contributes to Explainable AI with human understandable "if-then" type rules.

4 Learning Method for AIS Attack Detection

General flowchart describing the main steps of applying ILP for learning rules of AIS attack detection is depicted in Figure 1. In the following sections, each of the steps is described in detail.

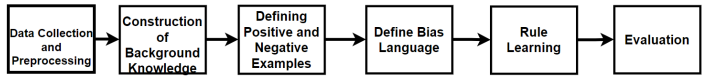


Fig. 1 Flowchart of learning AIS attack signatures using ILP.

4.1 Data Collection and Preprocessing

There are publicly available AIS data from Marrinetraffic [47], Spire Global [48] or AISHub [49]. These sources make valuable contributions but focus mainly on the ships' trajectory, position and movement. As far as only aggregated data is available from these sources [50], these datasets are not fine-grained enough to support detailed AIS anomaly detection-related research. To assure the trustworthiness of our solution, we used for training and testing it on a real-life MarCyb dataset, collected with a dedicated receiver installed

on the premises of Estonian Maritime Academy, N59.462N, E24.666 40m ASL [51, 52].

The AIS data used in this study was recorded in the Baltic Sea. For this experiment, we extracted a portion of the data from **19/06/2022** at **2:00:00** to **20/06/2022** at **2:00:00**, providing a 24-hour snapshot of vessels movements in the area.

Vessels, passed the edge of the AIS receiver's coverage, appeared only a few times in the dataset. During the training set's preprocessing, we excluded these vessels' data if only one or two messages within a normal reporting interval (less than 3 minutes) were received from them. These vessels were removed as outliers causing unnecessary noise in the dataset since they prevent accurate behaviour analysis and rule derivation. The remaining vessels' data were used for the learning.

In the data cleaning phase, and in order to answer the reliability question, messages including data fields with default values (such as speed value of 102.3 knots) were excluded due to being uninformative. We also excluded messages with fields inserted by the crew and fields such as RAIM and accuracy, which were found to be inconsistent with AIS specifications. The cleaned dataset was the basis for constructing background knowledge and positive examples for the ILP system to learn general rules describing correct AIS data.

4.2 Learning Rules of Correct AIS Data

4.2.1 Setup of the NUMSYNTH Environment

In ILP, learning is structured around constructing three key components: *background knowledge*, *examples*, and *bias language*. This approach applies to NUMSYNTH to derive meaningful rules from data, and we followed this when learning rules describing normal vessel behaviour from AIS data.

4.2.2 Constructing Background Knowledge

In ILP, background knowledge plays a key role in guiding the system during the learning process. It consists of facts and known information that the ILP system uses to derive rules. For this experiment, the background knowledge is derived from the AIS message type 1 data, containing the ground truth for each recorded vessel. The key components of background knowledge include:

- *The number of messages* encoded as Prolog fact `(msg_nbr/2)` representing the total number of AIS messages reported by a vessel.

- *Duration* encoded in the fact `(duration/2)` that specifies the time interval (measured in seconds) when the vessel's AIS have been received.

- *Maximum and minimum speed* `(max_speed/2, min_speed/2)`, the highest and lowest speeds reported by the vessel.
- *Mean and standard deviation of position error*, calculated based on two factors: according to AIS specifications, the coordinate accuracy is within 10 meters if the accuracy field is set to true. To account for this, we calculate the difference between the distance derived from longitude and latitude between two coordinates reported in consecutive messages and the distance computed using the reported time and speed. From now on we call this distance difference *delta distance*. Since we are dealing with two points, the accuracy of calculated distance can be assumed to be less than 20 meters. Given that each vessel has multiple reported messages, we calculate the ground truth of the positional error by determining the mean and standard deviation in two ways. The first method includes only the points where the delta distance, as described above, is 20 meters or less. The second method includes all data points, regardless of whether the delta distance is greater or less than 20 meters. We encode the mean and standard deviation for the points with a delta distance of 20 meters or less as `(mean/2)` and `(standard_deviation/2)`, and for the second case, we use `(mean1/2)` and `(standard_deviation1/2)`.
  Our analysis shows that, whether the accuracy field is set to true or false, most of the data points still meet the accuracy threshold expected.
- Predicate `(negative/2)` is used to count the number of messages that exceeded the delta distance constraint.
- Predicate `(status/2)` indicates whether the vessel is moving or stopped based on its reported speed. A vessel is considered to be in a stopped state if its maximum speed was less than or equal to 0.4 knots.
- Predicate`(trajectory/2)` determines whether a vessel follows a straight or non-straight trajectory.

The background knowledge is expressed as a set of Prolog facts where a fact describes a specific characteristic of the vessel. An example of background knowledge for a given vessel (sh_276636222) is as follows:

```
msg_nbr(sh_276636222, 66).
duration(sh_276636222, 1241.23).
max_speed(sh_276636222, 17.5).
min_speed(sh_276636222, 17.1).
mean(sh_276636222, -10000000.0).
standard_deviation(sh_276636222, -10000000.0).
negative(sh_276636222, 66).
mean1(sh_276636222, 148.77).
standard_deviation1(sh_276636222, 2.13).
status(sh_276636222, moving).
```

```
trajectory(sh_276636222, straight).
```

This background knowledge, combined with the examples and bias declarations, allows NUMSYNTH to explore the space of possible hypotheses and derive rules that explain normal vessel behaviour.

4.2.3 Defining Positive and Negative Examples

Defining positive and negative examples (sets E+ and E-, respectively) is a critical step for getting correct learning hypothesis. We defined **negative examples** as vessels that have sent data violating the accuracy constraint (i.e., a delta distance larger than 20 meters between positions reported in consecutive messages). The violations were caused by one or more of the following issues:

- Reporting position outside the zone where the data was collected
- Significant speed jumps reflected in consecutive messages
- Long time gaps between consecutive message transmissions

Any vessel with one or more of these violations was labelled as a negative example. On the other hand, positive examples were the vessels data that did not violate any of these constraints. These vessels adhered to the expected behaviour, maintaining a consistent position and speed, and thus represent normal behaviour in the dataset. In addition to the naturally occurring negative examples, we additionally generated *fake vessels* to imitate spoofing attacks. These synthetic data about the vessels were designed with two types of trajectories: one with a straight trajectory and another with a circular trajectory, to simulate suspicious or abnormal behaviour. To make these synthetic examples more realistic, we:

- Deleted certain data points to simulate missing transmissions
- Extracted segments from real vessel data (such as speed) to mimic normal conditions, while modifying the time and trajectory information to introduce anomalies.

4.2.4 Language Bias and Search Space

The NUMSYNTH *bias language* is a declarations file that informs the system which predicates from the background knowledge can be used during the learning process. This file defines the structure of the rules that NUMSYNTH can generate, specifying which predicates are allowed in the head and which ones in the body of the resulting rules, as well as the types and directions (input, output) of the variables involved. It also provides information to limit the search space, such as the type of variables and the direction (input or output) for each predicate used in rule generation, and how many numerical

variables must be bounded for a valid rule. An example of the bias file used in this study is as follows:

```
head_pred(vessel_id,1).
body_pred(min_speed,2).
type(min_speed,(string,float)).
direction(min_speed,(in,out)).
```

- `head_pred/2`: Declares the head of the resulting rule, which, in this case, is the predicate `fact/1`. The number 1 indicates that the predicate has arity 1.
- `body_pred/2`: Declares a predicate that can appear in the body of the learned rule. For example, `min_speed/2` is a predicate with an arity 2, which can be used to describe the minimum speed of a vessel.
- `type/2`: Specifies the types of the variables involved in the predicate. For the `min_speed/2` predicate, the first variable is of type string (representing the vessel identifier), and the second variable is of type float (representing the minimum speed).
- `direction/2`: Indicates the direction of the variables. `in` means the variable is an input (e.g., the vessel identifier), while `out` means the variable is an output (e.g., the minimum speed value calculated by the system).

This bias file plays a crucial role in guiding the ILP system by:

- Defining the *structure* of the rules that can be generated, ensuring that only meaningful rules are created based on the available data.
- Restricting the *search space* by limiting the predicates and their types, which improves computational efficiency.
- Indicating how variables flow through the rule: input variables (in) are provided from the data, while output variables (out) are inferred by the system.

NUMSYNTH uses so called *generate, test, and constrain* approach [53], where it generates rules based on these declarations, tests them against the examples, and constrains the search space iteratively. The system begins with rules of size 1 and increases the size of the rule incrementally while respecting the variable constraints. The search process continues until a valid rule is found or the maximum size limit is reached, ensuring that the system efficiently explores possible hypotheses without getting stuck in an exhaustive search.

4.2.5 NUMSYNTH Derived Rules

Inductive Logic Programming (ILP) aims to discover minimal, non-disjunctive rules that accurately classify all positive examples while excluding all negative ones. Using NUMSYNTH, we applied a systematic refinement approach to

optimise the generated rules over three learning epochs. Each epoch produced increasingly concise and accurate rules to classify vessel behaviour based on AIS data, culminating in perfect classification.

4.3 Summary of Results

The performance metrics across the three learning epochs are summarised in the Table 2:

Epoch	Precision	Recall	TP	FN	TN	FP	Rule Size
Epoch 1	1.00	0.61	27	17	34	0	16
Epoch 2	1.00	1.00	44	0	34	0	9
Epoch 3	1.00	1.00	44	0	34	0	6

Table 2 Summary of Learning Epochs: Precision, Recall, and Rule Size

Through these iterations, the rules were refined to achieve both precision and recall scores of 1.00, with the final phase producing the most concise and effective rule set. These rules provide a reliable classification of vessel behaviour, leveraging key features such as trajectory, status, and numerical values like mean value and standard deviation of speed.

4.4 Learning Epochs in Detail

4.4.1 Epoch 1

In the initial iteration, the system was configured with a maximum of seven variables and one numerical variable. Despite an early system crash due to inconsistencies between positive and negative examples, we deactivated conflicting predicates to resolve these issues. This led to the following rules being generated:

```
vessel_id(A) :- standard_deviation1(A, C),geq(C,
                0.254), standard_deviation(A, C).
vessel_id(A) :- standard_deviation(A, C),
                trajectory(A, straight), geq(C, 3.089).
vessel_id(A) :- status(A, stop), mean(A, B), geq(B,
                0.274).
vessel_id(A) :- standard_deviation(A, D), leq(D,
                0.439), status(A, stop).
```

Although *precision* reached 1.00, the recall was only 0.61, indicating that 17 positive examples were missed, and the rule size was relatively large (16 literals).

4.4.2 Epoch 2

In the Epoch 2, we increased the number of numerical variables to two, enabling the system to explore more complex relationships. This adjustment improved recall to 1.00, achieving perfect classification with the following rules:

```
vessel_id(A) :-standard_deviation1(A,B),
                leq(B,17.564),standard_deviation(A,C),
                geq(C, 0.222).
vessel_id(A) :- standard_deviation1(A, C),status(A,
                 stop), standard_deviation(A, C).
```

The system successfully classified all examples with a smaller rule size (9 literals), demonstrating the advantage of incorporating additional numerical variables.

4.4.3 Epoch 3

In the Epoch 3, we further increased the number of numerical variables to three, yielding a more concise and effective rule set. The rules produced in this phase were:

```
vessel_id(A) :- standard_deviation1(A, E),mean(A,
                D),geq(D, 0.012),geq(E, 0.084),
                leq(E,17.564).
```

This epoch resulted in both *precision* and *recall* scores of 1.00, while reducing the rule size to 6 literals. The system successfully generated a rule that can distinguish between normal and abnormal vessel behaviour based on the bounded values of the parameters in predicates `mean` and `standard_deviation1`.

4.4.4 Learning Runtime

The learning process of Epoch 3 (with three numerical variables) took the longest time, approximately **15** seconds, running on an Intel Core i5 processor. This demonstrates the feasibility of NUMSYNTH in handling complex numerical reasoning tasks, even with multiple variables and large datasets, and the scalability of our approach for real-time and data intensive applications.

4.4.5 Saturation of the learning process

When the number of numerical variables was increased beyond 3, the solution remained the same as with 3 variables. This indicates that three numerical variables were sufficient to capture the complexity of the dataset required to distinguish between normal and abnormal vessel behaviour based on AIS data. Further increases did not contribute to further optimisation of the rule set.

5 Evaluation of the method

In this section, we evaluate the method by studying the results of learned rules based on three criteria: (1) validity of the rules, (2) explainability, and (3) the limitations of using only AIS Message Type 1 to detect spoofing attacks.

5.1 Validity of the Rules

The generated rules were tested using independent from training dataset snapshot of recorded AIS data. The learned rules were valid in correctly classifying both normal and abnormal vessel behaviour. This validation was based on real-world AIS data collected over a 24-hour period from the Baltic Sea, specifically in the Tallinn Bay area. The rules demonstrated perfect classification performance within the dataset, achieving 100% in both precision and recall.

However, one has to admit that our current validation dataset is somewhat limited. Though Tallinn Bay is one of the most intensive traffic zones in Baltic sea, the dataset does not capture the full range of global maritime conditions, such as varying traffic density, environmental conditions, or regional navigation patterns. Testing the learned rules with additional datasets from different regions would allow us to confirm the method feasibility in a broader context. By using data from other maritime regions, we can determine whether the rules are robust enough to handle different vessel behaviours and operational patterns across the world.

In addition to expanding the dataset, future work will focus on determining the perfect time interval for testing the rules. The perfect time interval refers to the interval that best captures the vessel's position during different scenarios, such as when it is moving or stopping. This is important because the behaviour of a vessel may vary significantly depending on its status. Furthermore, we must consider the coverage area, as vessels may still appear in the dataset after reaching their intended destination and starting a new trip,

thus creating a new scenario that requires different analysis. Better selection of data collecting time intervals will help improve the accuracy and consistency of the rule extraction and application across various vessel operations.

5.2 Explainability

A significant advantage of using ILP is the explainability of the learned rules. The rules generated are interpretable and can be effortlessly understood by domain experts. For instance, rules based on vessel trajectory, speed, and positional accuracy are intuitively connected to maritime operations and can be reviewed and explained easily. This explainability makes the system more transparent and trustworthy, as users can inspect the specific conditions under which a vessel is flagged as behaving abnormally.

In comparison to black-box ML models, the ability to review and explain the rules ensures that the system can be used confidently in operational settings. It also allows for continuous improvement and adaptation, as new data and insights from maritime experts can be integrated during the rule refinement process, thus carrying out life-long learning approach.

5.3 Limitations of Using Only AIS Message Type 1

While the rules based on AIS Message Type 1 data effectively distinguish between normal and abnormal vessel behaviour, they still are limited in their ability to definitively detect spoofing attacks. AIS Message Type 1 contains dynamic information such as vessel position, speed, and course, which is helpful for identifying deviations from expected behaviour. However, without additional data sources (e.g., AIS Message Types 5 or 24, radar data), it is impossible to determine with full certainty whether abnormal behaviour is caused by a spoofing attack or by other factors, such as technical malfunctions or human error.

In summary, the current system can detect when a vessel is behaving abnormally, but it cannot guarantee that the abnormality is due to a cyberattack like spoofing. To accurately identify spoofing, the system would need to incorporate other AIS message types or external verification systems (e.g., radar or satellite data). However, current approach still helps narrowing down the number of suspicious cases that require further analysis. Developing a more comprehensive detection system is part of our future work.

6 Conclusion and Future Work

This study demonstrates promising results of applying inductive logic programming method for learning anomalies in AIS data that could indicate potential spoofing attacks. The method has been successfully applied to real-life data monitored from the Baltic Sea area and used to learn human interpretable rules that distinguish normal and abnormal vessel behaviours. The key advantage of this approach is its ability to generalise from a small set of examples and provide explainable evidence of anomaly occurrence, making it suitable for operational use in maritime environments.

The learned rules achieved perfect precision and recall in classifying vessel behaviour to correct and anomalous based on real AIS data. However, the dataset used for validation of the learned rules is limited in this study to the Tallinn Bay area, which presents somewhat limited range of global maritime conditions.

Future work will involve testing the relevance of the demonstrated method on a broader range of datasets and environments to ensure its robustness and range of applicability. As concluded from this study, improving the detection capability, specifically for reliable detection of spoofing attacks, may require extension of the training set with other AIS message types and with radar or satellite data. Nevertheless, this study opens new possibilities for future work in applying ILP methods for maritime cybersecurity, offering a step towards a more resilient and secure AIS system.

Acknowledgment

Research for this publication was funded by the EU Horizon 2020 project 952360-MariCybERA.

References

1. H. N. Psaraftis, *The Future of Maritime Transport.* Elsevier, 2021, p. 535–539. [Online]. Available: http://dx.doi.org/10.1016/b978-0-08-102671-7.10479-8
2. M. A. Belokas, "Maersk Line: Surviving from a cyber attack," [Online]. Available from: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/, 5 2018, (Accessed on: 7/4/2024 13:20).
3. "Maritime cyber security," [Online]. Available from: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/, 06 2022, (Accessed on: 7/4/2024 13:20).
4. "Introduction cooperation on maritime cybersecurity Atlantic Council," [Online]. Available from: https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/, 10 2021, (Accessed on: 7/4/2024 13:22).

5. "Maritime Cyber Resilience Prosjektbanken," [Online]. Available from: https://prosjektbanken.forskningsradet.no/project/FORISS/295077, (Accessed on: 7/4/2024 13:29).
6. "MariCybERA," [Online]. Available from: https://maricybera.taltech.ee/, 04 2021, (Accessed on: 7/4/2024 13:30).
7. "Maritime Cyber Threats research group University of Plymouth," [Online]. Available from: https://www.plymouth.ac.uk/research/maritime-cyber-threats-research-group, 08 2016, (Accessed on: 7/4/2024 13:32).
8. International Maritime Organization, "MSC-FAL.1-Circ.3 - Guidelines on maritime cyber risk management," 7 2017, [Accessed: 15-11-2020].
9. ——, "MSC-FAL.1/Circ.3/Rev.2 - Guidelines on maritime cyber risk management," 6 2022, [Accessed: 11/04/2024].
10. B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *Journal of Navigation*, vol. 72, no. 5, p. 1108–1120, Feb. 2019. [Online]. Available: http://dx.doi.org/10.1017/S0373463318001157
11. International Maritime Organization, "Resolution MSC.428(98) - Maritime cyber risk management in safety management systems," 7 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.
12. "AIS for Safety and Tracking: A Brief History - Global Fishing Watch," [Online]. Available from: https://globalfishingwatch.org/article/ais-brief-history/, (Accessed on 09/20/2024).
13. "IALA GUIDELINE - An overview of AIS," [Online]. Available from: https://www.navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf, (Accessed on 09/20/2024).
14. A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "AIS data vulnerability indicated by a spoofing case-study," *Applied Sciences*, vol. 11, no. 11, p. 5015, May 2021. [Online]. Available: http://dx.doi.org/10.3390/app11115015
15. A. Androjna, I. Pavić, L. Gucma, P. Vidmar, and M. Perkovič, "AIS data manipulation in the illicit global oil trade," *Journal of Marine Science and Engineering*, vol. 12, no. 1, p. 6, Dec. 2023. [Online]. Available: http://dx.doi.org/10.3390/jmse12010006
16. "Above us only stars - C4ADS," https://c4ads.org/reports/above-us-only-stars/, (Accessed on 09/20/2024).
17. D. M. Valentine, "Now you see me, now you don't: Vanishing vessels along argentina's waters," Tech. Rep., 2021. [Online]. Available: https://zenodo.org/record/4893397
18. B. Ristic, B. La Scala, M. Morelande, and N. Gordon, "Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction," in *2008 11th International Conference on Information Fusion*, 2008, pp. 1–7.
19. M. Hadzagic and A.-L. Jousselme, "Contextual anomalous destination detection for maritime surveillance," in *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.(July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy*, 2016, pp. 62–65.
20. H. Y. Shahir, U. Glässer, N. Nalbandyan, and H. Wehn, "Maritime situation analysis: A multi-vessel interaction and anomaly detection framework," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 192–199.
21. A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13030104
22. C. Iphar, C. Ray, and A. Napoli, "Data integrity assessment for maritime anomaly detection," *Expert Systems with Applications*, vol. 147, p. 113219, 2020.

[Online]. Available: https://www.sciencedirect.com/science/article/pii/S09574174203004522

23. J. N. Campbell, A. W. Isenor, and M. D. Ferreira, "Detection of invalid AIS messages using machine learning techniques," *Procedia Computer Science*, vol. 205, pp. 229–238, 2022, 2022 International Conference on Military Communication and Information Systems (ICMCIS). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050922008894
24. C. Gamage, R. Dinalankarac, J. Samarabandu, and et al, "A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors," *WMU J Marit Affairs*, vol. 22, p. 447–477, 2023.
25. S. Muggleton, "Inductive Logic Programming," *New generation computing*, vol. 8, pp. 295–318, 1991.
26. A. Cropper, S. Dumančić, R. Evans, and S. H. Muggleton, "Inductive Logic Programming at 30," *Machine Learning*, vol. 111, no. 1, pp. 147–172, 2022.
27. T. Eriksen, G. Høye, B. Narheim, and B. Jensløkken Meland, "Maritime traffic monitoring using a space-based AIS receiver," *Acta Astronautica*, vol. 58, no. 10, pp. 537–549, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0094576506000233
28. Y. Chen, "Satellite-based AIS and its comparison with LRIT," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 8, no. 2, p. 183–187, 2014. [Online]. Available: http://dx.doi.org/10.12716/1001.08.02.02
29. International Maritime Organization, *Solas: Consolidated Text of the International Convention for the Safety of Life at Sea, 1974, and Its Protocol of 1988, Articles, Annexes and Certificates, Incorporating All Amendments in Effect from 1 January 2020*, ser. IMO publication, 2020. [Online]. Available: https://books.google.hu/books?id=JKULzgEACAAJ
30. ——, "Resolution A.917(22) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," 2001.
31. F. Cabrera, N. Molina, M. Tichavska, and V. Araña, "Automatic Identification System modular receiver for academic purposes," *Radio Science*, vol. 51, no. 7, p. 1038–1047, Jul. 2016. [Online]. Available: http://dx.doi.org/10.1002/2015RS005895
32. C. Hocquette and A. Cropper, "Relational program synthesis with numerical reasoning," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 5, pp. 6425–6433, Jun. 2023. [Online]. Available: https://ojs.aaai.org/index.php/AAAI/article/view/25790
33. M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 436–445. [Online]. Available: https://doi.org/10.1145/2664243.2664257
34. M. Balduzzi, "AIS exposed understanding vulnerabilities & attacks 2.0," 2014.
35. B. Ristic, B. La Scala, M. Morelande, and N. Gordon, "Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction," in *2008 11th International Conference on Information Fusion*, 2008, pp. 1–7.
36. K. Kowalska and L. Peel, "Maritime anomaly detection using Gaussian Process active learning," in *2012 15th International Conference on Information Fusion*, 2012, pp. 1164–1171.
37. M. Vespe, I. Visentini, K. Bryan, and P. Braca, "Unsupervised learning of maritime traffic patterns for anomaly detection," in *9th IET Data Fusion & Target Tracking Conference (DF&TT 2012): Algorithms & Applications*, 2012, pp. 1–5.
38. F. Katsilieris, P. Braca, and S. Coraluppi, "Detection of malicious AIS position spoofing by exploiting radar information," 07 2013.

39. J. Coleman, "Behavioral model anomaly detection in Automatic Identification System (AIS)," in *Master thesis.* Chattanooga, Tennessee, USA: The University of Tennessee at Chattanooga, 2020.
40. I. Kontopoulos, G. Spiliopoulos, D. Zissis, K. Chatzikokolakis, and A. Artikis, "Countering Real-Time Stream Poisoning: An Architecture for Detecting Vessel Spoofing in Streams of AIS Data," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*. IEEE, aug 2018. [Online]. Available: http://dx.doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00139
41. A. Kullberg, I. Skog, and G. Hendeby, "Learning motion patterns in AIS data and detecting anomalous vessel behavior," in *2021 IEEE 24th International Conference on Information Fusion (FUSION)*, 2021, pp. 1–8.
42. E. d'Afflisio, P. Braca, and P. Willett, "Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2093–2108, 2021.
43. R. O. Lane, D. A. Nevell, S. D. Hayward, and T. W. Beaney, "Maritime anomaly detection and threat assessment," in *2010 13th International Conference on Information Fusion*, 2010, pp. 1–8.
44. D. Blauwkamp, T. Nguyen, and G. Xie, "Toward a deep learning approach to behavior-based AIS traffic anomaly detection." San Juan, Puerto Rico, USA: ACM, 12 2018.
45. M. Louart, J.-J. Szkolnik, A.-O. Boudraa, J.-C. Le Lann, and F. Le Roy, "Detection of AIS messages falsifications and spoofing by checking messages compliance with TDMA protocol," *Digital Signal Processing*, vol. 136, p. 103983, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1051200423000787
46. ——, "An approach to detect identity spoofing in AIS messages," *Expert Systems with Applications*, vol. 252, p. 124257, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417424011230
47. "MarineTraffic: Global Ship Tracking Intelligence — AIS Marine Traffic," [Online]. Available from: https://www.marinetraffic.com/, month = , year = , note = (Accessed on 01/14/2024).
48. "Marine AIS data - Maritime AIS vessel tracking solutions," https://spire.com/maritime/, (Accessed on 03/18/2024).
49. "Free ais vessel tracking — ais data exchange — json/xml ship positions," [Online]. Available from: https://www.aishub.net/, (Accessed on 01/14/2024).
50. "AIS Dispatcher free AIS data sharing tool AISHub," [Online]. Available from: https://www.aishub.net/ais-dispatcher, 07 2017, (Accessed on: 14/1/2024 17:34).
51. G. Visky, A. Šiganov, U. R. Muaan, R. Varandi, H. Bahsi, and L. Tsiopoulos, "MarCyb dataset," 2024. [Online]. Available: https://data.taltech.ee/doi/10.48726/00fa9-5xv20
52. G. Visky, A. Rohl, S. Katsikas, and O. Maennel, "AIS Data Analysis: Reality in the Sea of Echos," in *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, 2024, pp. 1–7.
53. A. Cropper and R. Morel, "Learning programs by learning from failures," vol. 110, no. 4, pp. 801–856. [Online]. Available: https://link.springer.com/10.1007/s10994-020-05934-z

Appendix 12

Publication XII
M. E. Orye, G. Visky, A. Rohl, and O. Maennel. Enhancing the cyber resilience of sea drones. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, pages 83–102, 2024

CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)

Enhancing the Cyber Resilience of Sea Drones

Erwin Orye, Maj.
Centre for Digital Forensics
and Cyber Security
Tallinn University of Technology
Tallinn, Estonia
erwin@orye.eu

Gabor Visky
Centre for Digital Forensics
and Cyber Security
Tallinn University of Technology
Tallinn, Estonia
gabor.visky@taltech.ee

Alexander Rohl
School of Computer
and Mathematical Sciences
Faculty of Sciences, Engineering and
Technology
University of Adelaide
Adelaide, Australia
alexander.rohl@adelaide.edu.au

Olaf Maennel
School of Computer
and Mathematical Sciences
Faculty of Sciences, Engineering and
Technology
University of Adelaide
Adelaide, Australia
olaf.maennel@adelaide.edu.au

Abstract: Sea drones are unmanned vessels that operate on or below the water's surface. During the military conflict between the Russian Federation and Ukraine, the latter has demonstrated how to use sea drones to attack Russian targets efficiently. However, as Russia's defences against drone attacks are continuously increasing, the cyber resilience of sea drones is becoming increasingly important. Technological developments in shipping have brought new cybersecurity challenges. This paper contributes to the knowledge on augmenting the cyber robustness of maritime autonomous surface-floating and subaqueous drones. Firstly, we aim to support manufacturers in building affordable sea drones that reduce the cyberattack surface of commercial drones. Secondly, we offer guidance for tactical military commanders on the potential cyber weaknesses in a sea drone's specific operational environments and its reliance on particular technologies. We propose eight distinctive threat categories for cyberattacks against autonomous vessels: attacks to disrupt radio frequency signals; attacks to deceive or degrade sensors; attacks to intercept or modify communications; attacks on operational technology systems; attacks on information technology systems; attacks on artificial intelligence (AI) used for autonomous operations; attacks through supply chains; and attacks through physical access. We use the STRIDE (spoofing,

tampering, repudiation, denial of service, elevation of privilege) [1] methodology in the context of each threat scenario, formulate mitigation measures to reduce the risk for each category, and link methods of cyberattack to each category.

Keywords: *cybersecurity, autonomous, threat modelling, unmanned, vessels, sea drones*

1. INTRODUCTION

Automation, and consequently limited human interaction, has created new vectors for cyberattacks. Cybersecurity is a critical issue for ships with some level of autonomy because of their increased dependence on information and communication technologies (ICT) for ship control, their advanced integration of control systems, their increased connectivity with shore control centres, and their accessibility to (and *from*) the Internet [2].

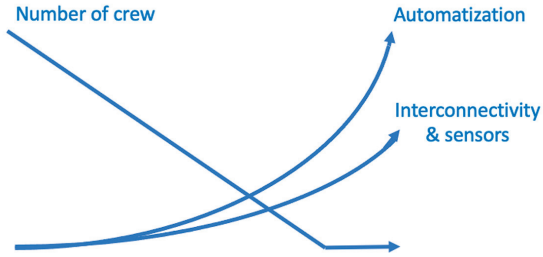
The coexistence of crewed and autonomous vessels (sea *drones*) necessitates the shared use of maritime, canal, and riverine domains. Ensuring the harmonious integration of these two naval transportation modes is vital to the sustainable and effective functioning of waterborne transportation systems.

Industry and academia have conducted extensive research and development in the field of autonomous vessels, such as Wärtsilä's IntelliTug [3], YARA Birkeland [4], L3Harris maritime autonomous systems [5], and Japan's fully autonomous ship program MEGURI2040 [6]. Research projects conducted in academia include, among many others, the University of Plymouth's Cetus Project [7], the Norwegian University of Science and Technology's Autoferry Project [8], and Heli by Tallinn University of Technology and the University of Tartu [9].

Sea drones rely entirely on digital systems with no physical crew to override them. Hence, the consequences of those digital systems being compromised can be more severe than would otherwise be the case.

Figure 1 depicts the evolution of growing automation. In particular, it shows how further automation is possible even when a vessel is already crewless, driven by the need for onshore supervision to become less involved.

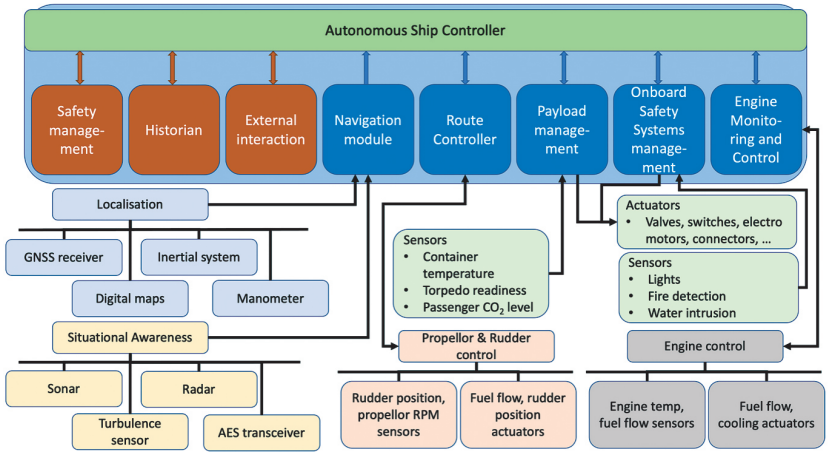
FIGURE 1: NUMBER OF CREW VERSUS THE LEVEL OF AUTONOMY AND RELIANCE ON AN INCREASED NUMBER OF INTERCONNECTED SENSORS



Sea drones come in many different configurations: surface and submarine, commercial and military, large and small, remote-controlled and auto-navigating, and many more [10]. Each configuration is suitable for a specific mission. Vessels can operate for days, weeks, and even longer without human intervention. For example, Saildrone's newest robotic ocean explorer sea drone draws its power from wind and can spend up to 12 months at a stretch out at sea [11]. The US Navy has recently received a prototype ship that can operate autonomously at sea for up to 30 days [12]. And, in 2022, the Nippon Yusen Kabushiki Kaisha (NYK Line) Designing the Future of Full Autonomous Ships (DFFAS) project achieved a 40-hour long autonomous trip across 790 kilometres (491 miles) at sea without human intervention for 99% of the journey [13].

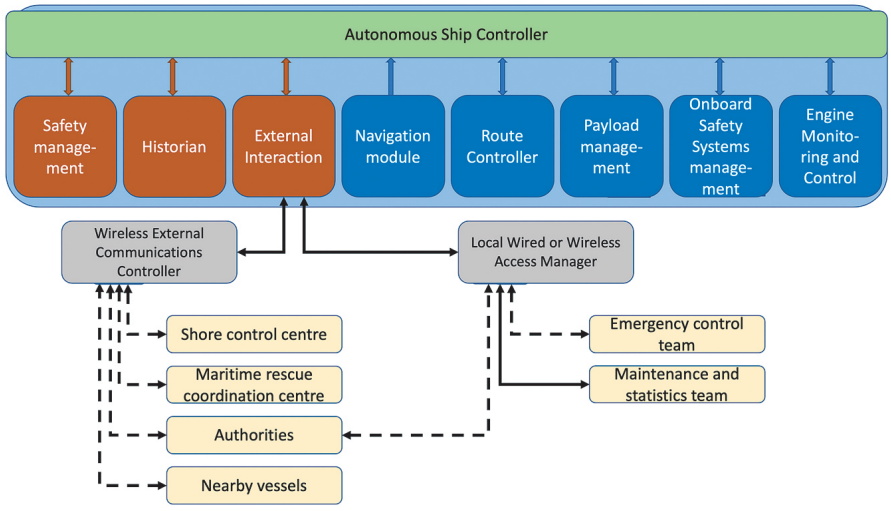
Although the configurations of sea drones might differ, their logical architecture often has the same functionalities. Figure 2 gives an overview of standard sea-drone functionalities.

FIGURE 2: SCHEMATIC OVERVIEW OF THE LOGICAL FUNCTIONS OF AN AUTONOMOUS SEA DRONE



Autonomous sea drones do, at some points, interact with humans, even if rarely or with only a minor impact on their functioning. Figure 3 shows the potential ways in which humans can interact with sea drones. Autonomous vessels have a command-and-control (C&C) channel to execute remote control commands, report sensor statuses, and receive mission instructions from the home base. This C&C channel is not necessarily always active, and the autonomous vessel might have to operate for long periods without supervision, potentially at a considerable physical distance from the control centre. As such, a sea drone needs to be equipped to operate in various uncontrolled environments and for different durations.

FIGURE 3: HUMAN INTERACTION WITH A SEA DRONE AND THE C&C LINKS FOR COMMUNICATIONS



2. RELATED WORK

To our knowledge, a combined study that jointly models the cyber threats, attacks, and defence methods regarding sea drones is not available in the literature (Section 2.B). It is this gap that motivated our research, in which we apply the STRIDE methodology (described in Section 2.A) to real scenarios to identify the adverse effects of cyber threats and the potential methods to defend against them.

A. Literature Review

Silverajan et al. [14] identify seven main attack surfaces through which attackers can gain access to or disrupt operations on uncrewed ships: positioning systems, sensors, firmware, voyage data recorders, intra-vessel networks, vessel-to-land communication,

and remote operations systems. They also define six attack methods: code injection, tampering/modification, positional data spoofing, Automated Identification System (AIS) data spoofing, signal jamming, and link disruption/eavesdropping. However, their work does not cover contextual attack scenarios, possible consequences, or the mitigations required for defence.

Along similar lines, Agamy [15] proposes that the following three threats can affect the cybersecurity of autonomous ships: malicious components added to control systems during building or maintenance sessions, compromised communication links, and position data spoofing. Agamy also discusses a number of examples and regulatory frameworks, such as the International Safety Management Code (ISM), the International Ship and Port Facility Security Code (ISPS), the EU's General Data Protection Regulation (GDPR), and the Australian Cyber Security Center's Final Security Strategy. However, these frameworks do not offer any technical defence measures.

As for the cybersecurity risk assessment of autonomous ships, Tam and Jones [16] model risks relating to the systems and components of autonomous vessels – for example, AIS, Global Navigation Satellite Systems (GNSS), automated mooring systems, cargo management systems, radar, sensors, and voyage data recorders (VDR) – from the perspectives of theft, damage, denial of service, obfuscation, and misdirection. Their model-based framework for maritime cyber-risk assessment (MaCRA) risk model provides a comprehensive method for assessing risk, but the paper does not cover mitigation for the risks or defensive methods against them.

Kavallieratos et al. [17] analyse an autonomous ship into 14 systems: Engine Automation, Bridge Automation, Shore Control Centre, Autonomous Engine Monitoring and Control, Engine Efficiency, Maintenance Interaction, Navigation, Autonomous Ship Controller, Human-Machine Interface, Remote Manoeuvring Support, Emergency Handling, AIS, ECDIS, and Global Maritime Distress and Safety. They then identify threat scenarios for each system using the STRIDE framework. In subsequent research, Kavallieratos and Katskas [18] extend this approach by considering further components of the ship's systems, such as collision avoidance, RADAR, closed circuit television (CCTV), advanced sensor modules, and autopilot systems. These papers give an overview of the risk assessment of autonomous ships. However, they do not detail attack scenarios and defensive measures.

Sungbaek et al. [19] identify cyber threats against autonomous ships, but they do not structure this content into a framework.

B. Threat Model

Threat modelling identifies and enumerates potential security threats and categorizes countermeasures by priority so as to reduce security risks to an acceptable level for the system owner. It includes several safety-focused risk management methodologies for Industrial Control Systems [20]. The CIA-triad (confidentiality, integrity and availability) has been used as a conceptual model in computer security for several decades [21]. The STRIDE methodology, as defined by Shostack [22], categorizes threats corresponding to cybersecurity goals by incorporating three more elements: authentication, non-repudiation, and authorization. The STRIDE threat categories are as follows [23]:

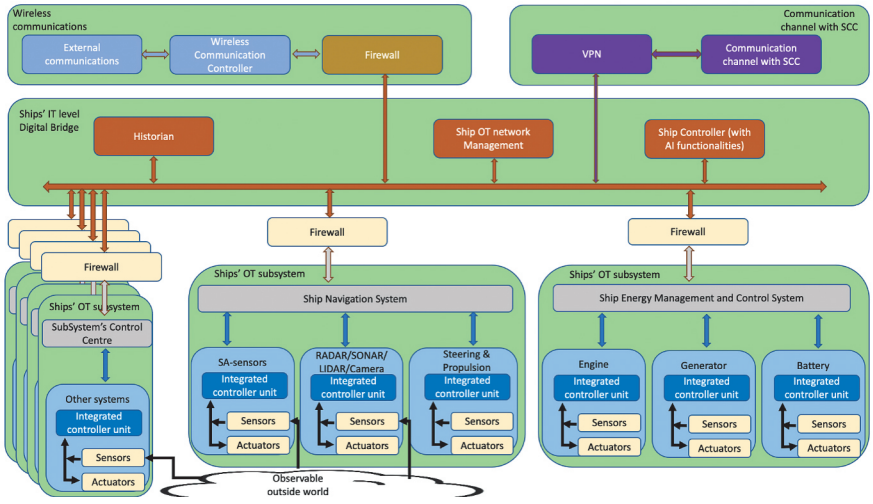
1) Spoofing is the ability of an adversary to masquerade as someone or something else.
2) Tampering refers to modifying or disrupting a system's disk, network, or memory.
3) Repudiation relates to threats where someone denies having taken specific actions that impact the system's operation or disclaims responsibility for the resulting outcomes.
4) Information disclosure involves exposing confidential information to unauthorized individuals.
5) Denial of service refers to compromises to the system's availability that work by consuming the necessary resources for its proper operation.
6) Elevation of privilege refers to situations in which an adversary can execute unauthorized actions.

According to Kim et al., the STRIDE methodology can be used for threat modelling against a distributed control system (DCS) [24]. Since our research focuses on sea drones, and since these are considered a system of DCSs [25], we adopt and use the STRIDE methodology. In that light, our research examines the different possible attacks so as to address the potential threats posed by malicious actors. Instead of focusing on a specific technology used in a particular ship, this paper employs general but transferrable abstractions. Thus, we offer a future-proof approach that can accommodate the broad functionalities of sea drones and cyberattack vectors.

3. RESULTS

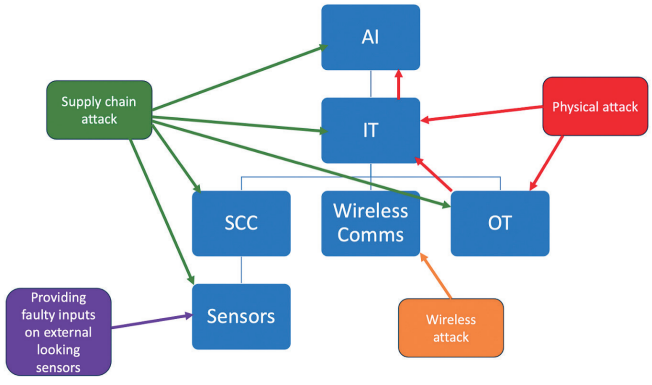
This section introduces the selected attack scenarios and their STRIDE analyses. To help motivate these scenarios, we must first consider the necessary functions of sea drones and their related subsystems. Figure 4 shows an abstract schematic overview, focusing only on the different types of equipment and how they relate to each other within an autonomous vessel.

FIGURE 4: SCHEMATIC OVERVIEW OF SUBSYSTEMS IN AN AUTONOMOUS VESSEL



To understand the attack surface of these subsystems, we must examine the lines for information flow. Figure 5 gives an overview of each sea-drone subsystem's possible attack vectors.

FIGURE 5: THE POSSIBLE ATTACKS ON A SEA DRONE'S SUBSYSTEMS



Taking these attacks and the interaction of the different subsystems as our starting point, we defined eight areas that we examine in more detail through the STRIDE methodology:

1) Attacks to intercept, modify or disrupt wireless communications
2) Attacks to deceive or degrade sensors
3) Attacks on operational technology (OT) systems
4) Attacks on information technology (IT) systems
5) Attacks on artificial intelligence (AI) for autonomous operations
6) Supply chain attacks (SCA)
7) Physical attacks to launch cybersecurity attacks and
8) Attacks against the shore control centre (SCC)

A. Attacks to Intercept, Modify, or Disrupt Wireless Communications

Description: RF signals serve various purposes in relation to wireless communication, radar systems, and other wireless technologies. Disrupting RF signals involves actions taken to interfere with or disturb these signals. This can be accomplished through various means – for instance, jamming, interference, or deliberate manipulation of the signals – that degrade or turn off communication between devices or systems that rely on these signals.

Possible scenario: A design weakness, implementation, or design flaw in authentication or encryption can lead to signal manipulation.

S: Communication protocols such as AIS are easy to spoof in the maritime sector [26].
T: An attacker on the wireless C&C channel between the control station and the autonomous vessel could take over complete control of the ship.
R: There is often at lack of robust resilience against data modification within existing RF protocols. The absence of features to facilitate repudiation becomes apparent.
I: Autonomous vessels have sensors onboard. Some vessels provide some information on the fly through wireless channels to the home base. Access by third parties to sensitive information can lead to the disclosure of information.
D: Disruption of the C&C channel can lead to the vessel being made idle or execute fully automated actions, such as return to base. In any case, it is likely to lead to a denial of service for the operation of the vessel.
E: Accessing the C&C channel can allow deeper access to the system and overruling immutable parameters from a distance.

Possible mitigations:

- Using inertial systems or recognizing the environment with sensors and correlation with databases can mitigate incorrect GNSS input data or the unavailability of GNSS input data.
- There are multiple mitigations to protect against jamming, such as channel hopping, spectrum spreading, MIMO (multiple-input and multiple-output) based mitigation, channel coding, rate adaptation, and power control [27].
- A VPN solution or similar can potentially protect the C&C channels themselves and add additional authentication and integrity checks such as counters on messages, structure of messages, digital signatures, and so on.
- Communications that rely on interoperability – for instance, a communication channel between harbour and vessel, AIS, weather forecast broadcast, GNSS, or GDMSS – are vulnerable to attacks by design. However, there are possible countermeasures. For example, the autonomous vessel could try to filter out fake AIS messages by looking at the physical layer of the message and correlating this with previous messages to compensate. On the other hand, ignoring AIS messages too readily might decrease the vessel's situational awareness, which can increase the danger of collisions. Securing those channels would be the next level of security for autonomous ships.

B. Attacks to Deceive or Degrade Sensors

Description: The sensors that capture information outside an autonomous ship offer a high-privilege way for attackers to influence the ship's operation because the attacker does not need physical access to the vessel to compromise these. In this regard, the location or proximity of the vessel is a condition to consider.

Another attack would be fooling internal sensors such as fire detection, engine failure, stability sensors, and so on. However, this would require first gaining physical access and initiating attacks on the sensors from there.

Possible scenario: A ship's sensors are prone to jamming and the injection of false echoes. The same applies to sensors designed for very short-distance situational awareness, such as cameras and illuminating LEDs on optical sensors.

S: An attack that changes the vessel's surroundings so that the sensors pick up a modified input. If an attacker knows a sensor's behaviour, they can modify the input so as not to trigger attention from the digital bridge.
T: Sensors need calibration before use. An attacker tampering with calibration (e.g., for a depth sensor) might cause severe havoc.

R: Most attacks that fool the sensors and provide erroneous information are challenging to repudiate.
I: Knowing how many sensors and what characteristics they have might indicate what type of vessel it is and how to attack it.
D: Ensuring that sensors cannot provide measurements in their everyday working range would constitute a denial of service for those sensors.
E: Attacks against sensors do not necessarily provide a means for privilege escalation.

Possible mitigations:

- The autonomous ship should have sufficient sensors based on entirely different technologies, compare the inputs from those sensors, and make decisions based on as complete information as possible. The greater the range of different technologies installed, the more difficult it becomes for the attacker to successfully provide all of the wrong inputs simultaneously. For example, using lidar, radar, and AIS systems to determine if the vessel is on a collision course with another ship is more reliable than using only AIS or only one radar sensor. In the former situation, hackers might need to intervene in close proximity to the targeted ship to influence its behaviour. Good situational awareness of the vessel's surroundings, above and under the sea level, is vital to detecting any signs of an intruder. The correlation of inputs from different sensors and specific sensors over time can reveal threats.
- Log files and histograms might help the digital bridge determine if any sensors are producing incorrect input data and take action to mitigate the problem. Such action can equally help with faulty sensors when there is no intervention from a malicious actor.

C. Attacks on Operational Technology Systems

Description: Most of the digital components of an autonomous ship are operational technology (OT) systems. Traditionally, protocols used in OT systems are vulnerable to various cyberattacks since there is no standard encryption mechanism implemented in most communication protocols, and the authentication happens at the hardware level or not at all. For example, all major fieldbus protocols – such as Modbus, DNP3, Profinet and EtherCAT – lack authentication or encryption. Thus, if they manage to get access to the network, attackers can disrupt network operations or manipulate I/O messages to cause a failure in the control process [28].

Possible scenario: Different attacks are possible in this context, such as first hacking the C&C link and, with privilege escalation, getting into the core networks. Gaining

physical access to the system, such as through maintenance ports or even the physical wires, is another option.

S: It is straightforward to spoof an endpoint in an OT network since there is no authentication, and, therefore, it is easy to spoof an existing hardware address.
T: OT systems are prone to supply chain attacks and insider threats. For example, maintenance personnel could constitute an insider threat. An example of the former would be if a manufacturer or another actor in the supply chain of the OT endpoint or core element were to reveal undocumented functionalities that an attacker could use to launch an attack.
R: There are often no logfiles for OT networks since the total number of messages is substantial, even though each individual message might be small in size.
I: An attacker can read all the information passing on the bus. Depending on the size and type of endpoints, they can map the topology of the network and the functionalities of each endpoint.
D: By flooding the bus with messages, the denial of service of an endpoint becomes straightforward. If the endpoint is only sending information, this information is not reaching any destination. If the endpoint reads information from the bus, it will not receive any helpful input data.
E: The OT systems are often at the heart of the autonomous vessel. Protection focuses on threats from the outside. An attacker might try to go from the OT network (or bus) to get to a central controller and from there to the digital bridge.

Possible mitigations:

- By segregating networks, the amount of helpful information available on any one segment can be limited. Gateways, firewalls, and other security measures are essential to reduce the risk of an attacker gaining access to more segments, controllers, or even the digital bridge.
- Considerations should be made for implementing enhanced security for control systems, encrypting all volatile and non-volatile memory, securing bus protocols between different devices, and segregating/segmenting the networks with controls. Implementing these measures is challenging because of the number of OT devices on board and the need for common relevant standards.
- Another possible line of defence is to analyse all traffic in real time with anomaly-detector machine-learning algorithms that can identify abnormal behaviour.

D. Attacks on Information Technology Systems

Description: Attacks on information technology (IT) systems modify the firmware of various components and devices on autonomous ships, operating systems, and software running on higher-level machines.

Possible scenario: With an attack on the IT systems, an attacker gains access to the digital bridge. Depending on the elevation of privilege on the IT system(s), this might allow them to gain complete control over the vessel.

S: Without firmware integrity verification and authorization for firmware updates, an attacker could perform an unauthorized firmware update. If the operator activates this option, the attacker could execute this via maintenance interfaces and over-the-air updates.
T: Malicious firmware updates can tamper with the functionalities of the autonomous vessel.
R: Without signed versions of software updates, it is nearly impossible to attribute an attack digitally.
I: Once an attacker is in the IT systems, they might have access to databases, (sensor) data, localization, the health status of the vessel, and other critical information.
D: When the central IT system is not responding as designed, the autonomous vessel is no longer executing its mission.
E: One of the most effective paths for an attacker of an IT system is an escalation of privilege. To gain complete control over the autonomous vessel, the attacker needs access to many functionalities in the IT system.

Possible mitigations:

- The first question that an operator of an autonomous vessel should decide upon is whether software or firmware updates are allowed over the air. Depending on the situation, one option will be better than the other. If operators at the SCC do not have access to the ship when they discover a significant software flaw, one option is to implement a patch immediately over the air. Still, enabling this access increases the attack surface for attackers. It is essential to know the status of the software and hardware and, therefore, use signed versions of firmware from trusted companies, define policies on who, when, and how to update the system, and, last but not least, test the software for functionality and security before installing it.
- Preferential redundancy is critical for making autonomous decisions. Use equipment and software from different vendors that provide the same functionality to install multiple independent calculation chains and, ultimately, use a voting system that decides what action to take.

E. Attacks on AI for Autonomous Operations

Description: Machine learning code provides functions that can replace the human factor. This kind of software is, therefore, interesting from an attacker's point of view since it is directly engaged with the decision-making process. Attacks on machine learning software aim to cause misjudgement or malfunction.

Possible scenario: Typical attacks on machine learning include evasion attacks (to fool a machine learning model by corrupting the query), model poisoning, and data pointing.

S: An attack on specific sensors might change the input for the AI coming from that sensor and fool the algorithms into changing the outcomes of decisions.
T: Modifying the behaviour of the AI software can result in different responses to sensor inputs. If the attacker has enough knowledge about the vessel, they might use this to execute actions on the ship.
R: Without digital signatures to allow changes in the AI software, other traces are required to achieve repudiation, which can be challenging.
I: Tampering with the AI system might lead to the full disclosure of all data available or generated on the vessel.
D: When altering the AI system, it is possible to achieve a complete denial of service of the autonomous vessel by spoofing input values to the AI that take unusually long to process.
E: Given that this attack targets the data of the AI system, it is important to note that it does not facilitate privilege escalation.

Possible mitigations:

- Select training datasets that focus on how to work effectively under sensor degradation or actuator failures. It is also crucial to consider what happens if the opponent knows the algorithms or the learning datasets and can create special conditions by fooling some sensors. Machine learning could help discover weaknesses in other machine learning software.
- Figure 6 shows all the attacks against deployed machine-learning systems according to the ATLAS framework.
- Extensive testing in extreme conditions should be conducted. The datasets for learning the system should include ways of responding to cyberattacks.

FIGURE 6: MITRE'S ADVERSARIAL THREAT LANDSCAPE FOR ARTIFICIAL INTELLIGENCE SYSTEMS [29]

F. Supply Chain Attacks

Description: Attacks on the supply chain – which can have various sources, including third-party vendors, internal employees, and others – include disruption of operations, compromise of sensitive information, financial losses, reputational damage, legal and regulatory implications, and so on [30].

Possible scenario: A hacker steals a certificate used to vouch for the legitimacy or safety of a company's product, or a hacker leverages the tools for building software applications to introduce security weaknesses in the development process. Similarly, preinstalled malware can represent a valid threat scenario – for instance, if there is a malicious component in the firmware.

S: Implement faulty MAC addresses, ID numbers, or other mechanisms to receive information from the internal bus or networks.
T: Malicious code or components can be injected into the product through targeted attacks that initialize, for example, communication to a C&C server, thus creating a tampering backdoor into the system.
R: It is always difficult to tell which actor implemented a backdoor, a spy module, a modified firmware, and so on. Was it the chip manufacturer, the print board, the integrator, the shipping company, or other stakeholders?
I: When malicious actors trick individuals, a phishing attack can lead to information disclosure or compromised security, sometimes providing access with elevated rights.
D: A compromised component can cause a denial of service on an autonomous ship.
E: Malicious code running in a software component with elevated privileges can offer access to the IT systems with elevated rights.

Possible mitigations:

- Considering the multiple forms they can take, defending against SCA requires a range of different techniques, including auditing the IT (shadow) infrastructure, a highly secure build and update infrastructure, up-to-date software assets, application of client-side protection solutions, and so on [31].
- It is necessary to precisely follow up on all modifications made to a product, from designing to manufacturing integration to decommissioning.

G. Physical Attacks to Launch Cybersecurity Attacks

Description: If an autonomous ship operates in the open sea, physical protection for the vessels can easily be weaker than otherwise.

Possible scenario: Various maintenance interfaces on autonomous ships, such as USB, Serial, JTAG and RJ45, could be exploited as initial attack vectors. Even if there are physical locks to prevent unauthorized physical access to these interfaces, there is a possibility that an attacker could compromise the locks and make unauthorized connections through these interfaces as the autonomous ship navigates in the open sea for an extended period of time.

S: With physical access to the vessel, an attacker gains an entry point to the digital systems without facing the difficulties of accessing interface points with the outside world. It makes sense that those interface points are the way in with the least privilege and the most extensive logging. Otherwise, determining the ease of spoofing the system depends on the exact location of the entry point.
T: There are many possible tampering actions, from swapping disks to plugging USB sticks with malware into maintenance. Different attacks are possible depending on the time available, size, computational power, design, and complexity.
R: Physical attacks are complicated to attribute digitally. Forensics might find some artefacts if, for example, malware leaves some digital traces.
I: Information disclosure is a risk for all internal communication that is not encrypted and where the attacker with physical access can extract the data. The same goes for databases that contain unencrypted data.
D: All physical destruction – for instance, unplugging a cable or flooding a data bus – will lead to denial of service of parts or the whole of the autonomous vessel.
E: An attacker still has to achieve elevation of privilege unless they can physically replace the IT system with their own.

Possible mitigations:

- There are many options to reduce the risk of physical access and the impact of such an attack: segregation and segmentation of the networks, cable fault sensors that detect anomalies, sensors that raise the alarm on intrusion, external sensors such as drones or satellites that surveil the neighbourhood of the vessel, physical protection measures such as locks to reduce the chances of obtaining physical access, firewalls between segments, time scheduled maintenance slots, and so on.
- Cost, the attacker's benefit, the vessel's value, available space, allowed weight, power consumption, and so on will probably determine the number and type of countermeasures that can and need to be put in place.

H. Attacks Against the Shore Control Centre to Launch a Cyberattack on a Sea Drone

Attack description: Most autonomous ships have a C&C channel to receive input from the home base. This communication can be sporadic when tasking a mission to remote control with some automatic functions. The shore control centre (SCC) has a privileged entry point to the vessel from the outside. Access to the SCC might compromise one or more ships.

Possible scenario: Inappropriate segregation between the C&C network and the office network at the SCC or inappropriate control over removable media/mobile devices might compromise the C&C network, which can result in the transmission of unauthorized commands to autonomous ships or disruption of the C&C communication channel itself.

S: When instructions come from a hacker that spoofs the SCC – if the attacker has the encryption key for the VPN tunnel to the vessel, for example – the vessel will be unable to differentiate between legitimate and spoofed instructions.
T: The attacker can install malware through the C&C channel or modify the vessel's behaviour if remote updates are allowed.
R: If the attacker leaves traces in the SCC, it is possible to attribute an attack, but the traces of the login on the vessel will not help identify an attacker if the messages are well crafted.
I: The hacker will have access to all the data the SCC has access to. For example, if a vessel sends observations from its sensors directly to the SCC, the attacker will receive the same information.
D: An attack against the SCC does not necessarily lead to a denial of service for an autonomous vehicle. However, because of the level of automation, it still poses a danger.

E: Once the attacker can take over the C&C control channel, they might still need an elevation of privilege for the functionalities the SCC cannot execute from a distance. The SCC retains a large number of permissions to intervene when unexpected situations occur.

Possible mitigations:

- The SCC is a typical IT infrastructure with specific software to create instructions for the vessel and communicate this in a particular way. Therefore, the protection of the SCC is most similar to protection measures implemented by banks or for critical infrastructure. ISO27K series, National Institute of Standards and Technology (NIST), or similar guides the management of cybersecurity risks in this field.

4. DISCUSSION

Cybersecurity relates to risk assessment. Criminals attacking cargo vessels do not have the same profile as state actors who also show interest in specialized military, research, and governmental-operated vessels. Configurations of such specialized vessels can differ extensively in terms of the type and number of sensors, redundancy of subsystems, processing power, machine learning algorithms, and many other features. Thus, not all the subsystems previously mentioned need to be present, and the size and number of existing subsystems can differ significantly.

What actions a system owner takes to reduce the impact of cybersecurity attacks depends on the threat scenario, the residual risk an operator wants to assume, the threat level, the importance of the mission, their finances, and the time they have available to operationalize a vessel. Improving cybersecurity boils down to securing the complete software and hardware supply chain. Early levels of indicators of compromise (IOCs) and intelligence about advanced persistent threats (APTs) are a significant help when it comes to being informed about the threat scenario and level.

Complete autonomous ship operations have a larger cybersecurity attack surface. Still, depending on the setting, this can be acceptable since such ships have the advantage that there will be no loss of life and no way to demand ransoms when something happens to the vessel and non-existent crew.

Verification at different levels is essential to reducing the risk of the vessel being compromised:

1) Identification and authentication control: Who is allowed to access the system, and can you verify that this person is who they claim to be?
2) User control: Who is allowed to execute which commands?
3) Integrity control: Are you sure that the instructions have not been tampered with?
4) Data confidentiality control: Are you sure that adversaries cannot intercept information?
5) Restricted: Ensure everyone has access to information only on a need-to-know basis. This concept is very crucial with regard to insider threat issues.

Following our STRIDE analysis of the eight subsystems, a sea drone owner or manufacturer should take the relevant steps to improve the cyber resilience of their sea drone:

1) Analyse the system into its logical components according to Figure 4.
2) Define all the data fluxes between each system component and the external world.
3) Identify threats for each system component and function based on the operational use of the sea drone and the corresponding attackers' profiles.
4) Once the threats for each system component are identified, the STRIDE model indicates where vulnerabilities might arise. Software exists to support the technical process of finding specific vulnerabilities. For example, the Microsoft Threat Modelling Tool (MTMT) [32] implements the STRIDE framework at the software level. Open-source software, such as the open software templates building tool, inserts STRIDE threats in the generated template by searching common vulnerabilities and exposures (CVE) databases [33].
5) Take mitigation measures such as controlling information flows, adapting policies and installing control mechanisms. Implement effective mitigation strategies based on the specific discovered vulnerabilities.

5. CONCLUSIONS AND FUTURE WORK

Our research identified potential threats against autonomous maritime vehicles and provided a framework for their mitigation. Following that, we used the STRIDE attack model to highlight the cybersecurity aspects of sea drones and considerations

relevant to those, thus providing a solid background for manufacturers and end users willing to improve their sea drones.

We provided a framework and inventory of cyber risks for the engineers who develop sea drones and the users of sea drones. While we did not focus on the different components or parts of the sea drones, we grouped these into general but applicable subsystems to provide a foundational path towards developing detailed solutions for a specific sea drone. In our judgement, this approach fits the field best since each sea drone is a system of systems with its own individual specialized configuration.

Our research was limited to autonomous sea drones and crewed ships, depending on the level of automation. Although we focused only on technology-related measures, training people and improving processes are similarly crucial to cyber defence.

Many sea drones will soon serve as military [34] and merchant ships [35]. Our research aims to help industry and policymakers create a global ecosystem for safe and secure autonomous shipping.

REFERENCES

[1] L. Kohnfelder and P. Garg, 'The threats to our products', Microsoft Security Development Blog, 1999. [Online]. Available: https://www.microsof t.com/security/blog/2009/08/27/the-threats-to-our-products/0Ahttps://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

[2] S. K. Katsikas, 'Cyber security of the autonomous ship', in *CPSS 2017 – Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2017*, pp. 55–56, 2017.

[3] 'Initial sea trials successfully completed by Wärtsilä & PSA Marine's ground-breaking "IntelliTug" project'. Wärtsilä. Accessed: Jan. 3, 2024. [Online]. Available: https://www.wartsila.com/media/news/13-03-2020-initial-sea-trials-successfully-completed-by-wartsila-psa-marine-s-ground-breaking-intellitug-project-3290931

[4] 'Yara Birkeland'. Yara. Accessed: Jan. 3, 2024. [Online]. Available: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/

[5] 'Autonomous systems'. L3Harris. Accessed: Jan. 3, 2024. [Online]. Available: https://www.l3harris.com/all-capabilities/autonomous-systems

[6] 'The Nippon Foundation Meguri2040 fully autonomous ship program'. Nippon Foundation. Accessed: Jan. 3, 2024. [Online]. Available: https://www.nippon-foundation.or.jp/en/what/projects/meguri2040

[7] 'Uncrewed surface vessel (USV) Cetus'. University of Plymouth. Accessed: Jan. 3, 2024. [Online]. Available: https://www.plymouth.ac.uk/research/esif-funded-projects/usv-cetus

[8] 'Autoferry'. NTNU. Accessed: Jan. 3, 2024. [Online]. Available: https://www.ntnu.edu/autoferry

[9] 'Scientists launch Estonia's first autonomous maritime research vessel'. ERR. Accessed: Jan. 3, 2024. [Online]. Available: https://news.err.ee/1609117841/scientists-launch-estonia-s-first-autonomous-maritime-research-vessel

[10] N. Klein, D. Guilfoyle, M. S. Karim, and R. McLaughlin, 'Maritime autonomous vehicles: New frontiers in the law of the sea', *International and Comparative Law Quarterly*, vol. 69, no. 3, pp. 719–734, 2020.

[11] 'Saildrone launches a 72-foot autonomous seabed-mapping boat'. TechCrunch. Accessed: Jan. 11, 2024. [Online]. Available: https://techcrunch.com/2021/01/11/saildrone-launches-a-72-foot-autonomous-seabed-mapping-boat/?guccounter=2

[12] 'The navy's new autonomous ship can run by itself for 30 days'. Accessed: Jan. 11, 2024. [Online]. Available: https://www.popularmechanics.com/military/navy-ships/a43033206/navy-ship-can-operate-autonomously-for-30-days/

[13] 'Autonomous cargo ship completes 500 mile voyage, avoiding hundreds of collisions'. Electrek. Accessed: Jan. 10, 2024. [Online]. Available: https://electrek.co/2022/05/13/autonomous-cargo-ship-completes-500-mile-voyage-avoiding-hundreds-of-collisions/
[14] B. Silverajan, M. Ocak, and B. Nagel, 'Cybersecurity attacks and defences for un-manned smart ships', in *Proceedings – IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 15–20, 2018.
[15] K. S. M. Agamy, 'The impact of cybersecurity on the future of autonomous ships', *International Journal of Recent Research in Interdisciplinary Sciences*, vol. 6, no. 2, pp. 10–15, 2019.
[16] K. Tam and K. Jones, 'Cyber-risk assessment for autonomous ships', in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*.
[17] G. Kavallieratos, S. Katsikas, and V. Gkioulos, 'Cyber-attacks against the autonomous ship', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11387, pp. 20–36, 2019.
[18] G. Kavallieratos and S. Katsikas, 'Managing cyber security risks of the cyber-enabled ship', *Journal of Marine Science and Engineering*, vol. 8, no. 10, pp. 1–19, 2020.
[19] S. Cho, E. Orye, G. Visky, and V. Prates, *Cybersecurity Considerations in Autonomous Ships*. Tallinn: CCDCOE, 2022.
[20] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, 'A safety/security risk analysis approach of industrial control systems: A cyber bowtie—combining new version of attack tree with bowtie analysis', *Computers & Security*, vol. 72, pp. 175–195, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817301931
[21] M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA: Cengage Learning, 2021. [Online]. Available: https://books.google.ee/books?id =Hwk1EAAAQBAJ
[22] A. Shostack, *Threat Modeling*. Nashville, TN: John Wiley & Sons, 2014.
[23] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamilla, and A. Murukan, *Improving Web Application Security*. Microsoft Corporation, 2003. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330
[24] K. H. Kim, K. Kim, and H. K. Kim, 'STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery', *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, Nov. 2022, doi: 10.4218/etrij.2021-0181.
[25] K. Tam, K. Forshaw, and K. Jones, 'Cyber-SHIP: Developing next generation maritime cyber research capabilities', in *Conference Proceedings of ICMET Oman*, Muscat, Oman, Nov. 2019, doi: 10.24868/icmet.oman.2019.005.
[26] 'Spoofed warship locations—automatic identification system (AIS)'. Popular Mechanics. Accessed: Jan. 7, 2024. [Online]. Available: https://www.popularmechanics.com/military/navy-ships/a37261561/ais-ship-location-data-spoofed/
[27] H. Pirayesh and H. Zeng, 'Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey', *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.
[28] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Waltham, MA: Syngress, 2015.
[29] 'ATLAS'. MITRE. 2021. [Online]. Available: https://atlas.mitre.org
[30] H. S. Berry, 'The importance of cybersecurity in supply chain', in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, May 2023, doi: 10.1109/ISDFS58141.2023.10131834.
[31] 'What are supply chain attacks? Examples and countermeasures'. Fortinet. Accessed: Jan. 7, 2024. [Online]. Available: https: //www.fortinet.com/resources/cyberglossary/supply-chain-attacks
[32] 'Microsoft threat modeling tool'. Microsoft. Accessed: Jan. 3, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
[33] M. Da Silva, M. Puys, P. H. Thevenon, S. Mocanu, and N. Nkawa, *Automated ICS template for STRIDE Microsoft Threat Modeling Tool* (ACM International Conference Proceeding Series), 2023.
[34] 'US Navy aims to field manned-unmanned fleet within 10 years'. Defense News. Accessed: Jan. 3, 2024. [Online]. Available: https://www.defensenews.com/naval/2023/04/12/us-navy-aims-to-field-manned-unmanned-fleet-within-10-years/
[35] Z. H. Munim and H. Haralambides, 'Advances in maritime autonomous surface ships (MASS) in merchant shipping', *Maritime Economics and Logistics*, vol. 24, no. 2, pp. 181–188, 2022, doi: 10.1057/s41278-022-00232-y.

Curriculum Vitae

1. Personal data

Name	Gábor Visky
Date and place of birth	8 December 1975 Budapest, Hungary
Nationality	Hungarian

2. Contact information

Address	Tallinn University of Technology, School of Information Technologies, Department of Software Science, Ehitajate tee 5, 19086 Tallinn, Estonia
Phone	+36 30 9844496
Email	gabor.visky@taltech.ee

3. Education

2021–	Tallinn University of Technology, School of Information Technologies, PhD Studies Program
2000–2004	University of Miskolc, Information Engineering, MSc
1994–1998	Bolyai János Military and Technology College, Telecommunication, BSc

4. Language competence

Hungarian	native
English	fluent
Russian	beginner

5. Professional employment

2022 –	Ministry of Defence, Head of Department
2017 – 2022	NATO Cooperative Cyber Defence Centre of Excellence, Technology Researcher
2016 – 2017	Assistant of Defense Attaché, Kiev
2012 – 2016	Ministry of Defence, Deputy Head of Department
2005 – 2011	Military Office, Head of Subdivision
2004 – 2005	Assistant of Defense Attaché, Warsaw
1998 – 2003	Ministry of Defence, Desk officer

6. Voluntary work

-

7. Computer skills

- Operating systems: Linux, Windows User
- Document preparation: MS Office
- Programming languages: Python, C#

8. Honours and awards

- 2024, Officers' Service Sign 1nd Class (30 years)
- 2014, Officers' Service Sign 2nd Class (20 years)
- 2012, Merit of Service Medal, Silver Grade
- 2005, Merit of Service Medal, Bronze Grade
- 2003, Officers' Service Sign 3rd Class (10 years)

9. Defended theses

- 1998 Morse Code Decoder Implementation With Microcontroller
- 2004 Design of a Controller Unit for Spectrum Analyser

10. Field of research

- Cybersecurity

11. Scientific work
Papers

1. A. Lavrenovs, G. Visky, and O. Maennel. Status detector for fuzzing-based vulnerability mining of IEC 61850 protocol. In *Proceedings of the European Conference on Information Warfare and Security*, ECCWS 2021. Academic Conferences International Ltd, 2021

2. G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam. Multi-purpose cyber environment for maritime sector. *Proceedings of the International Conference on Information Warfare and Security*, pages 349–357, Mar. 2022

3. E. Orye, G. Visky, and O. Maennel. Analysing the actual use of Controller–Pilot Data Link Communications. In *OpenSky 2022*, OpenSky 2022, page 18. MDPI, Jan. 2023

4. G. Visky, S. Katsikas, and O. Maennel. Lightweight Testbed for IEC61162-450-Related Cyber Security Research. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 638–643, 2024

5. G. Visky, A. Šiganov, M. u. Rehman, R. Vaarandi, H. Bahşi, H. Bahsi, and L. Tsiopoulos. Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 644–651, 2024

6. G. Visky, A. Rohl, R. Vaarandi, S. Katsikas, and O. M. Maennel. Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

7. G. Visky, D. Khisteva, R. Vaarandi, and O. M. Maennel. Towards an open-source intrusion detection system integration into marine vehicles. In *2024 International Symposium ELMAR*, pages 263–268, 2024

8. G. Visky, A. Rohl, S. Katsikas, and O. Maennel. AIS data analysis: Reality in the sea of echoes. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, pages 1–7, 2024

9. M. E. Orye, G. Visky, A. Rohl, and O. Maennel. Enhancing the cyber resilience of sea drones. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, pages 83–102, 2024

10. G. Visky, R. Vaarandi, S. Katsikas, and O. Maennel. Statistical analysis-based feature selection for anomaly detection in ais dataset. In *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 159–164, 2025

11. R. Vaarandi, L. Tsiopoulos, G. Visky, M. U. Rehman, and H. Bahşi. A systematic literature review of cyber security monitoring in maritime. *IEEE Access*, 13:85307–85329, 2025

12. G. Visky, D. Khisteva, and O. Maennel. *Technical Considerations for Open-Source Intrusion Detection System Integration in Marine Vehicles*, pages 143–160. Springer Nature Switzerland, Cham, 2025

13. A. S. Benterki, G. Visky, J. Vain, and L. Tsiopoulos. Using Incremental Inductive Logic Programming for learning spoofing attacks on maritime automatic identification system data. In S. Bauk, editor, *Maritime Cybersecurity*, pages 123–141. Springer Nature Switzerland, Cham, 2025

14. A. Lavrenovs and G. Visky. Exploring features of http responses for the classification of devices on the internet. In *2019 27th Telecommunications Forum (TELFOR)*, pages 1–4, 2019

15. A. Lavrenovs and G. Visky. Investigating HTTP response headers for the classification of devices on the internet. In *2019 IEEE 7th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pages 1–6, 2019

Conference presentations

1. Visky, Gábor (2019). Cyber-Physical Battlefield for Cyber Exercises. Proceedings of the 5th Interdisciplinary Cyber Research Conference 2019, [ICR]: 29th of June 2019, Tallinn University of Technology. Ed. Osula, Anna-Maria; Maennel, Olaf. Tallinn: Tallinn University of Technology, Department of Software Sciences, 10-12.

Elulookirjeldus

1. Isikuandmed

Nimi	Gábor Visky
Sünniaeg ja -koht	08.12.1975, Budapest, Ungari
Kodakondsus	Ungari

2. Kontaktandmed

Aadress	Tallinna Tehnikaülikool, Infotehnoogia teaduskond, Tarkvarateaduse instituut, Ehitajate tee 5, 19086 Tallinn, Eesti
Telefon	+36 30 9844496
E-post	gabor.visky@taltech.ee

3. Haridus

2021–…	Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Küberkaitse, doktoriõpe
2000–2004	Miskolci Ülikool, infotehnoloogia, MSc
1994–1998	János Bolyai Militaar- ja Tehnoloogiakolledž, telekommunikatsioon, BSc

4. Keelteoskus

ungari keel	emakeel
inglise keel	kõrgtase
vene keel	algtase

5. Teenistuskäik

2022– …	Ungari Kaitseministeerium, osakonnajuhataja
2017–2022	NATO Küberkaitse Kompetentsikeskus, tehnoloogiaosakonna teadur
2016 - 2017	Ungari saatkond Kiievis, kaitseatašee abi
2012 - 2016	Ungari Kaitseministeerium, osakonnajuhataja asetäitja
2005 - 2011	Ungari Kaitseministeerium, alamosakonna juhataja
2004 - 2005	Ungari saatkond Varssavis, kaitseatašee abi
1998 - 2003	Ungari Kaitseministeerium, lauaametnik

6. Vabatahtlik töö

-

7. Arvutioskused

- Operatsioonisüsteemid: Linux, Windows
- Kontoritarkvara: MS Office
- Programmeerimiskeeled: Python, C#

8. Autasud

- 2024, Ohvitseri 1. klassi teenistusmärk (30 aastat teenistust)
- 2014, Ohvitseri 2. klassi teenistusmärk (20 aastat teenistust)

- 2012, Teenetemedal (hõbe)
- 2005, Teenetemedal (pronks)
- 2003, Ohvitseri 3. klassi teenistusmärk (10 aastat teenistust)

9. Kaitstud lõputööd

- 1998 Morse Code Decoder Implementation With Microcontroller
- 2004 Design of a Controller Unit for Spectrum Analyser

10. Teadustöö põhisuunad

- Küberturve

11. Teadustegevus
Teadusartiklite, konverentsiteeside ja konverentsiettekannete loetelu on toodud ingliskeelse elulookirjelduse juures.

ISSN 2585-6901 (PDF)
ISBN 978-9916-80-382-0 (PDF)