# Fortifying Maritime Cyber Defence Through Secure Ship Zones and Network Safeguards

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Anjana Paul

Supervisors:
Petri Sainio (UTU)
Jouni Isoaho (UTU)
Petri Kolehmainen (Lead Cybersecurity Engineer, Meyer Turku)

June 2025

**Master of Science in Technology Thesis**
**Department of Computing, Faculty of Technology**
**University of Turku**

**Subject**: Cyber Security
**Programme:** Master's Degree Programme in Information and Communication Technology
**Author**: Anjana Paul
**Title**: Fortifying Maritime Cyber Defence Through Secure Ship Zones and Network Safeguards in Maritime Operations
**Number of pages**: 56 pages
**Date**: June 2025

This thesis explores the increasingly critical issue of cybersecurity in maritime operations with a focus on shipbuilding practices. Ships can face heightened exposure to cyber threats, resulting in compromised safety, operational efficiency, and data integrity as they become more reliant on interconnected digital technologies. The objective of this research is to plan security zones in ships, initiate network protection safeguards, and develop a ship cyber resilience test procedure that aims to assess the network's resilience in real-world scenarios so that it can withstand and recover from cyberattacks.

An elementary analysis of existing network architectures, the identification of critical systems, and the evolution of robust cybersecurity measures such as network segmentation, firewalls, intrusion detection/prevention systems, and encryption protocols is included in the research methodology of this thesis. A combination of qualitative and quantitative methods was used to evaluate the effectiveness of these measures. Testing and validation can be performed through simulated attacks and vulnerability assessments to identify weak points in the network.

The study demonstrates the necessity of implementing detailed network divisions, creating a proactive security policy, and conducting periodic cybersecurity training for ship personnel. Operational security and potential attack surface increased while overall security enhancement happened through these measures at Meyer Turku's network architecture. The necessary recommendations consist of permanent network surveillance along with scheduled system updates and detailed incident response preparation for future security risks.

Keywords: Maritime Cybersecurity, Network Segmentation, Ship Security Zones, Cyber Resilience, Intrusion Detection, Encryption

# List of Figures

# Table of contents

# 1 Introduction

## 1.1 Background Study

Maritime businesses are moving quickly towards digital solutions, as ships use digital technologies to automate their tasks, oversee operations and cargo, and improve essential communications. At the same time as improving efficiency and safety at sea, these new technologies have subjected the industry to more cyber dangers. Because IT and OT systems are now connected, vessels are at greater risk of being attacked in ways that can put safety, performance, and important records at risk. The latest data shows a dramatic rise in operational technology attacks on maritime ships, which calls for more attention to cybersecurity [1]. Modern ships now use digitalization, automation, and systems integration regularly. Since IT and OT systems are regularly linked to the Internet now, they become more vulnerable to being hacked, accessed without permission, or infected by malware. Consequently, vessel systems and the way they operate increase in risk, risking blocked navigation, less secure cargo storage, and unwanted harm to marine environments. With more advanced maritime networks and few skilled technicians aboard, new, simple solutions are needed to protect ship information systems [1]. International information sharing about cyber incidents constitutes an essential strategy to enhance resilience because cyber resilience represents an entity's capability to anticipate, monitor, stop, grow after, and recover from cyber events [2]. This thesis seeks to address the major problem of cybersecurity in maritime operations by developing a broad framework for ship cyber resilience. The key purpose is to plan well-guarded ship security zones, use firewalls, intrusion detection and prevention systems, encryption, and build a test procedure to check how robust ship networks are during simulation attacks. The research team looks at current network designs, highlights vital systems, and checks for strong cyber defences using approaches such as statistics, simulation, and the AHP [3]. It has significant value as it tries to solve urgent cybersecurity challenges in the maritime area. Operational disruptions, significant financial problems, harm to a company’s name, and environmental disasters can happen because of cyberattacks. Carrying out a successful cyberattack could stop navigation, put cargo safety at risk, and put the environment in peril. Because maritime networks are so complex these days, better cybersecurity is needed all the time, such as continuous surveillance, regular updates, and planning for incidents [4]. This work supports the ongoing discussion about maritime cybersecurity by reviewing the difficulties and hazards presented by new technologies in the sector. IT offers plans to help improve cybersecurity over time, with an emphasis on getting stronger, flexible, and following standards and regulations established around the world. Results are designed to enhance cyber defences for ships and offer guidelines for using the same methods across the maritime industry to keep shipping secure and sustainable as threats grow.

The goal of this research is to review network designs and suggest ways to strengthen maritime cyber defence, including designing resilient ship zones and network protections. The thesis was done together with Meyer Turku, which is one of the world's leading and modern cruise ship construction yards. Figure 1 below gives a quick look at the common automation systems found on modern and autonomous ships, according to sources [5]. It describes how navigation automation, engine control, managing cargo, and communication are carefully linked to support both efficiency and safety on a vessel. The figure explains the growing need for interconnected systems, which then leads to talks about the special cybersecurity risks that the maritime sectors face.

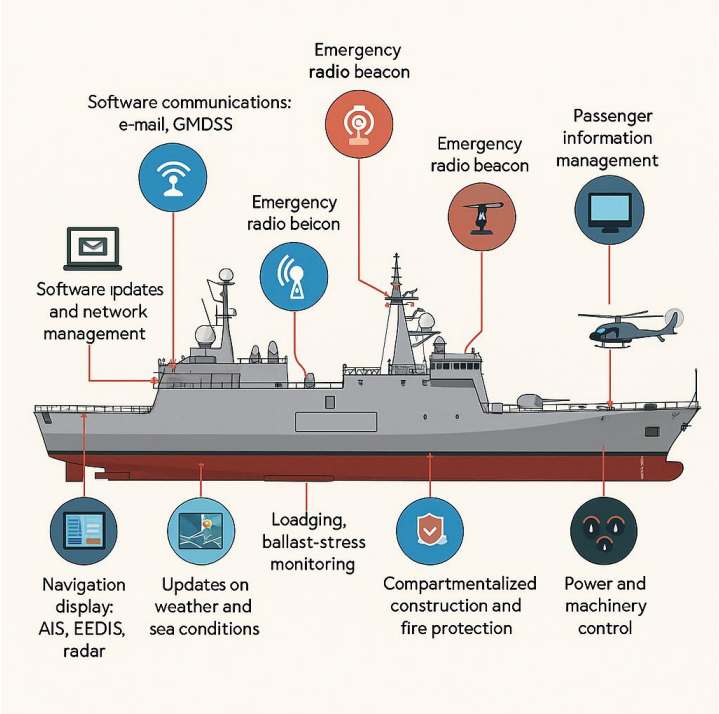


Figure 1: Automation systems for modern and autonomous ships [2].

## 1.2 Thesis Objectives

The primary objective of this research is to enhance the cybersecurity of maritime networks. Specific objectives include:

- Designing secure ship security zones that protect critical systems.
- Implementing network protection safeguards, including firewalls, encryption, and intrusion detection systems, to mitigate cyber threats.
- Developing a Ship Cyber Resilience Test Procedure to assess the robustness of ship networks under simulated attack scenarios.
- Proposing recommendations for the continuous improvement of cybersecurity measures in the maritime industry.

## 1.3 Importance of the study

Ship operations require cybersecurity in the maritime sector to achieve safety and operational security. Computer attacks have increased dramatically, causing businesses to face high costs of recovery while facing regulatory fines and both financial and reputational damage stemming from reduced trust with customers. Digital system implementations have caused operational technology breaches in maritime vessels to increase catastrophically by 900%, according to recent reports. Maritime cybersecurity research progresses, yet a thorough investigation of the subject remains absent. The paper [1] conducts a comprehensive examination of maritime sector cybersecurity domains, aiming to show security difficulties and operational challenges. Through vulnerability analysis, the study [1] examines maritime systems available for attack documentation, resulting in cases of system entry and their subsequent consequences [1]. The execution of a successful cyberattack can obstruct navigation while simultaneously damaging cargo security and potentially resulting in environmental hazards. The analysis [1] holds great importance because modern maritime networks need immediate protection from digital threats stemming from increasingly complicated systems onboard ships. The research [1] analysing ship operations brings tangible implications suitable for wider maritime industry application. The findings of this research will work to increase maritime vessel cyber resilience alongside meeting future standards for maritime cybersecurity regulations.

**Use of AI-Assisted Tools in my Research and Writing**

During the research and writing of this thesis, I used a variety of advanced AI tools to increase how well and efficiently I work. To assist with conceptual exploration, technical idea improvement, structure diagrams and summarize important points, tools such as ChatGPT (from OpenAI) were used. In addition, Perplexity.ai helped by directing me to fresh academic information, checking facts and summarizing insights from extensive resources.

I rewrote my text using QuillBot, a paraphrasing tool, so my sentences would be easy to read and understand yet keep the original point. These AI systems were not meant to replace important thinking or study, but were to enhance writing, help with citations, and maintain the standard of cybersecurity and maritime-related information. Every bit of AI-generated content has been probed, checked, and adapted to follow scholarly practices.

# 2 Literature Review

## 2.1 Maritime Network Security

The expansion of maritime operations toward digital technologies has led to an extensive increase in network security importance within the maritime sector. Modern vessels operate under integrated complex systems used for navigation while additionally managing their communication systems as well as propulsion systems, and cargo operation needs. Secure network systems maintain utmost importance to achieve vessel operational safety and efficiency. Pressing cybersecurity concerns emerged when maritime networks upgraded their connectivity and adopted networked systems because these developments exposed ships to rising cyber threats. This section details maritime network security development alongside the identification of barriers when protecting information technology (IT) and operational technology (OT) systems at sea. The combination of threat, vulnerability, and technology stands as the prime sub-criteria for maritime enterprises to cope with severe cyber threats since these three elements hold a total global importance weight of 0.102. The maritime cyber resilience is at level 4 (70.701%), according to expert projections, which indicate stability in 2023 while predicting a downward trend between 2024 and 2025 [5].

## 2.2 Maritime Cybersecurity Risks

Ships operating in isolated environments face specialized cybersecurity threats due to their unique combination of isolation and networking capabilities. The maritime sector confronts diverse cybersecurity risks, which include ransomware assaults, information thefts, and system break-in attempts, together with targeted operational interruptions. The maritime sector has three principal weak points: old software and insufficient encryption protocols, and unprotected data channels. Ships suffer from operational disruptions together with financial losses, and environmental disasters because of cyberattacks. Maritime-sector cyber threats are examined in this sub-section, among other cyberattacks that target Information Technology systems, such as navigation and communication, in addition to Operational Technology systems that involve engine control and ballast water management. During Shipping 4.0, digital transformation shipping companies implement expanded onboard system digitization that also brings higher vessel automation and autonomy levels. Operational safety and vessel navigation for modern and upcoming ships depends on Cyber Physical Systems created through Information Technology integration with Operation Technology systems. These highly connected systems make the digital infrastructure of vessels susceptible to cybersecurity risks, together with cyberattacks [4].

## 2.3 Network Segmentation

Information Technology (IT) and Operational Technology (OT) networks on ships serve distinct functions, yet they are increasingly interconnected, which introduces cybersecurity risks. IT systems handle data communication and administrative functions, while OT systems control physical processes such as propulsion and cargo handling. The segmentation of IT and OT networks is essential to prevent cyber threats from crossing over between the two domains. This section explores best practices for segmenting IT and OT networks on ships, discussing strategies like firewalls, virtual LANs (VLANs), and access controls that help minimize the risk of unauthorized access and system vulnerabilities. The strategic foundation of Cybersecurity includes network segmentation that divides networks into segments and manages traffic flows as a means of restricting cyber threats. Network segmentation plays an essential role in operational technology environments when organizations need to face severe consequences due to security breaches. Security increases together with performance along with management capabilities while maintaining regulatory compliance through these methods. The implementation process may generate problems, especially when taking place within limited resource environments that maintain legacy OT systems. Segmentation operates as a fundamental tool that the OT network engineer must use. The implementation of segmentation results in improved defensive capabilities as well as continuous operations for critical systems [6].

To have effective maritime cyber defence, we should choose network segmentation and monitoring tools that fit the requirements of shipboard systems. Here, the top solutions are compared, and a reason is given for settling on Nozomi Networks and Forescout for the framework.

**Table 1 Tool Comparison for Network Segmentation and Monitoring** [7], [8], [9].

| Purdue Layer | Nozomi Networks | Forescout | Claroty | Tenable |
|---|---|---|---|---|
| Enterprise (L5) | Limited focus | Strong (IT asset discovery) | Limited | Strong (vulnerability mgmt.) |
| DMZ (L4) | OT-focused monitoring | IT/OT asset visibility | OT/IT convergence | IT vulnerability scanning |
| Operations (L3) | Deep OT protocol analysis | Policy enforcement | OT threat detection | Limited |
| Control (L2) | PLC/RTU monitoring | Limited | PLC/SCADA focus | N/A |
| Field (L1) | Sensor/actuator visibility | Limited | Limited | N/A |

**What makes Nozomi Networks and Forescout important?**

Nozomi Networks is an expert in OT networks and makes it possible to clearly see the operations of legacy maritime control systems. Claroty does not have as much support for maritime-based OT protocols as other solutions offer [10].

Because of Forescout, it is easy to find assets on IT and OT networks and enforce policies for dividing shipboard crew Wi-Fi from the navigation network. Tenable nicely handles IT faults, but there is no intelligent segmentation for OT [8].

The table gives a quick overview of the top network monitoring and threat detection tools used in operational technology (OT) and the maritime sector. Every option, such as Nozomi Networks, Darktrace, Cisco Stealth watch, and Palo Alto, is judged on how much they support OT protocols, use anomaly detection methods, and whether they are suitable for use in the maritime area. It indicates what tools are designed for analysing protocols, for catching unusual patterns using AI, and what tools are simply used to monitor general or IT-related devices. This way of comparing tools reveals the reasons some tools better fit shipboard and industrial networks related to cybersecurity, highlighting each tool's advantages and disadvantages [11], [12].

**Table 2 Network Monitoring and Threat Detection Tool Comparison** [11], [12], [13], [14], [15].

| Criteria | Nozomi Networks | Darktrace | Cisco Stealth watch | Palo Alto |
|---|---|---|---|---|
| OT Protocol Support | Excellent (Modbus, IEC 60870) | Limited | Limited | Moderate |
| Anomaly Detection | Rule-based + ML | AI/ML-driven | Flow analysis | Signature-based |
| Maritime Use Cases | AIS spoofing, ECDIS attacks | Generic | Generic | Firewall integration |

Nozomi Networks detects maritime-specific threats like AIS spoofing and ECDIS ransomware through OT-aware rule sets. Darktrace's AI/ML approach lacks contextual understanding of shipboard OT systems, leading to false positives in isolated maritime environments [16].

The table below highlights and outlines different incident response and reporting options for IT/OT and maritime industries. Under these criteria, it looks at platforms like Forescout, Splunk, IBM QRadar, and Elastic Security to find out about their OT, regulatory, and maritime incident response support. The table says that some systems, like Forescout feature excellent asset tagging tools and have pre-defined workflows for maritime cases [17], while systems such as Splunk and QRadar need a lot of customization for ships [18], [19]. As the table brings together these features, it gives a clear reason for choosing the right tool according to how it fits, automates, and conforms with regulations in the maritime field.

**Table 3 Incident Response and Reporting Tool Comparison** [17], [18], [19], [20].

| Criteria | Forescout | Splunk | IBM QRadar | Elastic Security |
|---|---|---|---|---|
| OT Integration | High (IT/OT asset tagging) | Moderate | Low | Low |
| Regulatory Compliance | NIST CSF, IEC 62443 | Generic | Generic | GDPR-focused |
| Maritime Playbooks | Prebuilt for ship networks | Custom | Custom | Limited |

Choosing Nozomi Networks and Forescout is reasonable because of their focus on OT, applications in maritime industries, and a friendly approach with international maritime regulations and IEC standards. Even though Tenable and Darktrace are excellent in traditional IT systems, their expertise does not include shipboard OT networks. Research in the future should address the usefulness of Claroty and similar AI-based tools for hybrid systems, including IT and OT [17].

Digitalization, together with automation and integration systems, is now more frequently utilized aboard ships. A Cyber Threat Management Plan becomes necessary to enable such systems. The continuous technological evolution leads ships to merge information technology (IT) with operational technology (OT), so they become frequently connected to the Internet. Subsequent digital systems of ships experience greater exposure to hacking attempts and unauthorized entry that threaten their operational networks and systems' integrity. The introduction of malware through removable media (USB flash memory or hard disk) becomes a potential risk for onboard systems because of personnel who access those systems. Ships possess extremely advanced IT/OT systems, and the information systems dedicated to the shipping industry have faced multiple types of cyberattacks in recent years. A cyberattack poses the risk of compromising or making inaccessible the security features, along with the control capabilities of ship systems and their operational elements. Assuring the implementation of necessary cyber protection methods requires new ships, but making existing ships secure proves difficult because several additional measures become necessary. The worldwide decline in maritime crew and the shortage of onboard IT personnel specialized in maintaining ship information systems necessitate simple technical solutions for boosting ships' information system security Nozomi [21].

## 2.4 Critical Assets of Maritime Industry

For their cybersecurity, maritime organizations can use the Purdue Model [22] and rely on tools such as Nozomi Networks [21] and Forescout get complete and instant monitoring and control across all network levels. With the addition of AI-based detection or managed security offerings, security will be more elastic to new threats, and the business will keep meeting compliance and resilience standards worldwide [8].

Critical assets in maritime systems consist of essential components with infrastructure that presents a threat to ship operations and places the safety of vessels and their personnel, and cargo at risk. The maritime infrastructure consists of navigation systems as well as propulsion controls, communication systems, and multiple operational technology devices, including engine monitoring and control systems. The section establishes a list of essential assets while providing classification along with evidence showing the necessity to defend them against cyberattacks through strong security systems. Monitoring and resilience planning serve as keys to maintain asset security because they protect assets from modern security threats that appear during changing conditions.

Maritime cyber-physical systems form a complex network of IT (information technology) and OT (operational technology) systems linked through human element parameters. The illustration in Figure 1 illustrates how this integration system defines cyber-physical systems and manifests within most maritime vessel systems. Figure 2 presents a simplified representation showing the communication routes that connect shipboard and portside stakeholders to their IT/OT platforms to show IT and OT network interconnectivity. Vessel operations run by human users maintain a connection between processes and both IT systems and OT components. Naval vessels operate as platforms to connect various systems that include both IT and OT devices. The vessel's crew functions as the operator for ship components and processes, which they maintain for operational and performance quality through their responsibilities [23].

Shipping companies implement IT systems that provide technical assistance to naval ships at operational and technical levels. The human operator uses IT platforms as tools to complete both performance-based functions and financial tasks, which enhance maritime operations. Ports execute maritime commercial goods receipt and handling operations at shore-to-ship and ship-to-shore operational levels when they receive maritime cargo from or load the goods into naval vessels. This offloading and loading operation requires the integration of IT and operational technology platforms for successful execution by port control systems. IT and OT platforms operate together for maritime asset support in technical and operational capacities, including configuration and operational control of cargo management systems and cranes, and utilities support systems. People serve the role of operator and configurator as well as moderator across all cyber-physical systems. System and device maintenance operations for OT can occur through physical device access or at a distance. Most vessel system performance indicators are configured and monitored by remote procedures. Throughout every situation, the human operator stands as the vital operational leadership element [23].

## 2.5 DNV Regulations in Maritime Cybersecurity

DNV (Det Norske Veritas) offers maritime cybersecurity guidelines that tie together standards and plans for ship operations with regulations such as IEC 62443. DNV’s Cyber Secure class notations call for carrying out risk assessments, dividing the network, and monitoring everything continuously over the

whole lifetime of a vessel. These rules require maritime companies to fix risks in both IT/OT areas while still obeying IMO and IACS guidelines. Such as DNV standards, focus on ensuring proper security for old control systems and third-party devices involved in marine system management [24], [25]. The authors point out in their discussion of maritime cybersecurity that DNV aligns with the NIST CSF and uses its lifecycle approach to eliminate gaps between standard IT security and maritime needs [24].

## 2.6 NIST Cybersecurity Framework

NIST CSF gives maritime organizations a flexible approach to manage risks from cyberattacks on both IT and OT systems. By using the functions Identify, Protect, Detect, Respond, and Recover, operators learn how to organize company assets and create appropriate protections and responses. Maritime environments find the framework very useful as it is adaptable to the unique issues of using legacy systems and combined IT/OT systems [24], [25]. The paper [24] conducted an examination of the maritime sector, which found that organizations applying NIST CSF v2.0 detect more threats and meet the regulations set by the International Maritime Organization. The research reveals weaknesses in monitoring and risk management for supply chains, which Nozomi Networks and Forescout offer key help [24].

# 3 Network Architecture Analysis

## 3.1 Analysis of Network Architecture

Real-world network analysis entails focusing on how the components of a maritime network communicate in cooperative work. This approach makes it possible to evaluate possible security threats at the same time while it evaluates the current defences and points out potential areas for improvement. An assessment establishes the strength of a network against cyber threats and the protection of such systems. Network architecture assessment is the procedure of critically examining the design, layout, and interactions of the structures and workings of the network within a working environment. In the case of ships, it involves looking at IT and OT, because there must be free and effective communication between the two technologies for efficient and secure operations.

The key purpose of such an analysis is to achieve a level of understanding of how the network elements are configured, how the data moves through and around the vessel, and the mechanisms used for the protection of all boundaries. This will involve evaluating hardware such as routers, switches, and firewalls; software programs, including those used in business; communication protocols in place or being used in the business; and integration of IT with OT systems such as propulsion control, engine monitoring, and navigational aids. The diagram below illustrates the usual layout of IT and OT systems on a vessel in the maritime sector. It makes it clear that the paths of data and control in monitoring, steering, movement power, communication, and business must all be considered because they are complex and depend on each other in modern ships.

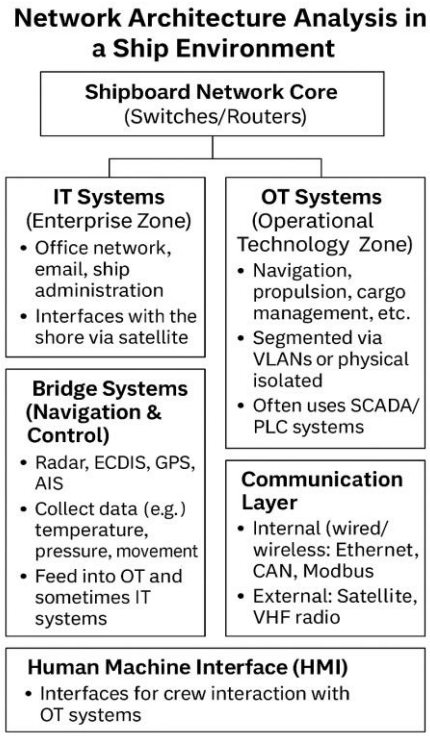


Figure 2: Network Architecture in Maritime Operations.

Figure 2 illustrates the typical layout of IT and OT systems on a vessel in the maritime sector. It makes it clear that the paths of data and control in monitoring, steering, movement power, communication, and business must all be considered, as they are complex and interdependent in modern ships.

### 3.1.1 Existing Network Components Overview

Maritime networks are composed of several interconnected components, including IT systems for communication, navigation, and data processing, and OT systems controlling engines, propulsion, and cargo handling. These networks often rely on multiple devices, such as routers, switches, firewalls, and sensors, all integrated into the ship's digital infrastructure. The complexity of this system increases the risk of cyberattacks, particularly in areas where IT and OT components overlap.

The maritime cyber environment consists of networked information technology (IT) systems and cyber-physical systems (operational technology, or OT). It comprises communication networks, allowing information to move from a ship's IT systems to OT systems. This is realized through different sensors and programmable logic controllers (PLCs), thus controlling complex navigational instruments such as Global Positioning Systems (GPS). With a widening scope of potential threats, more vulnerabilities and entry points discovered in maritime systems, the integration of IT and OT in the maritime sector poses more cyber threats because of the connections between the isolated OT systems and IT networks. Cyberattacks from both internal and external sources are now a possibility for vessels. As connectivity increases, maritime cybersecurity reaches beyond ships and is defined by intricate relationships between stakeholders and elements, including ports and shippers. The potential consequence of a cyberattack on a major vessel might upset global supply lines and cause billions of dollars in economic damage, in contrast to the automotive industry, where the effects of cyberattacks are often more confined, affecting single vehicles or restricted regions. Furthermore, the danger is not limited to a single ship; a cyberattack that targets shared infrastructure, such as a VSAT service provider, may cause a fleetwide or cross-fleet incident, increasing the harm to numerous ships and shipping businesses at once [26].

Figure 3 shows how marine IT and OT bring together different hardware and software. According to the source Maritime Cybersecurity: A Comprehensive Review [26], it illustrates the major devices involved, including servers, computers, control systems, sensors, and the software used, and explains their roles in supporting all processes on ships.

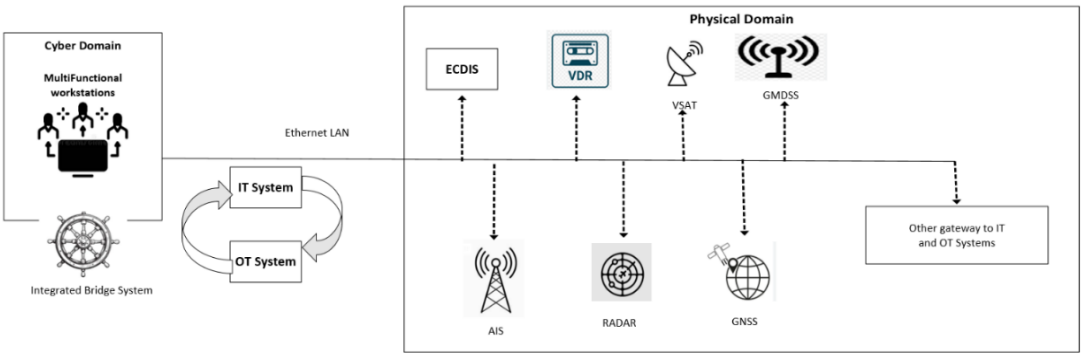


Figure 3: Typical Maritime IT and OT systems combined with hardware and software systems [27].

### 3.1.2 Strategy of Network Zones and Segmentation

Network segmentation is one of the most effective ways to enhance maritime cybersecurity. By dividing the network into distinct zones (such as IT and OT), segmentation minimizes the attack surface and prevents a single breach from spreading across the entire system. In maritime contexts, IT and OT systems should be segmented using virtual LANs (VLANs) or physical separation to ensure maximum security. IT zones handle communication and data transfer (e.g., email and Internet access). OT zones manage operational systems (e.g., engine controls, navigation). Demilitarized Zone (DMZ) separates the ship's internal systems from external communications, such as satellite connections.

Figure 4 shows how to separate a ship's network into different, well-defined security zones. It reveals that separate firewalls and restrictions on access keep the bridge, engine, business, crew, and passenger networks from being connected. The plan is put in place to isolate cyber threats and stop them from reaching important assets without permission.

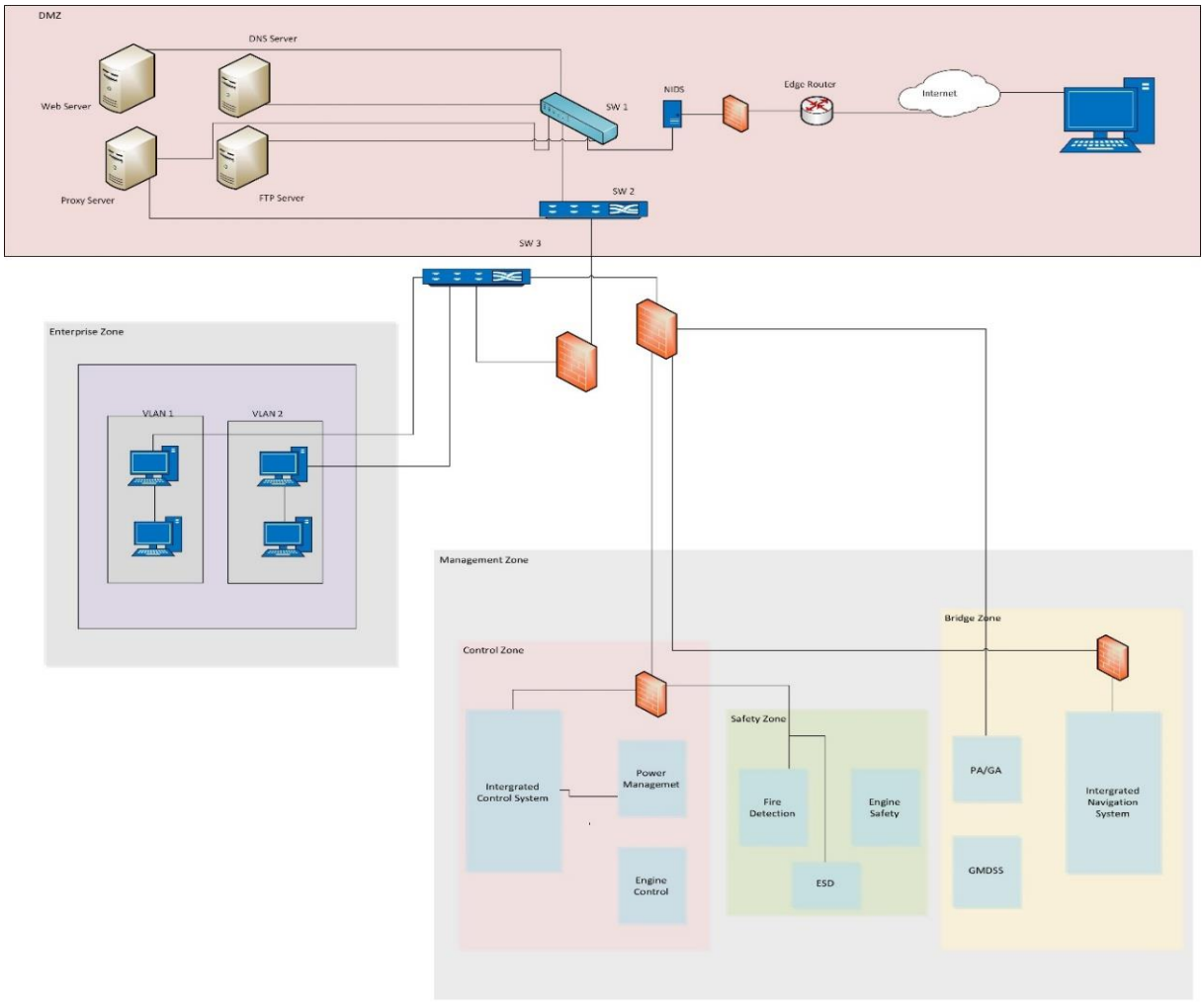


Figure 4: Zone-wise network segmentation plan.

### 3.1.3 Ship Security Zones & Network Segmentation

As a rule, ships use both IT (Information Technology) and OT (Operational Technology) networks; they have their own security requirements. The modern ship's function uses both Information Technology (IT) and Operational Technology (OT) systems. Following the specificities of their purpose and risks, the separation of the networks must be performed using smart segmentation. The method of segmentation suggested here should assist in enhancing cyber resilience and operational continuity even in the case that one of the areas is lost. The division strategy suggested in this research consists of the following:

**Bridge & Navigation Systems (High-Security Zone):** This zone is to be isolated from any other ship networks with the help of a hardware firewall and VLAN separation. The role of the high-security zone is to perform navigation, radar, and planning for a voyage. The security mechanisms include physical and logical isolation by firewalls (hardware), VLANs (Virtual LANs), which limit the data traffic flow, and there is no direct internet or public network access.

**Engine & Propulsion Control (Restricted Zone):** On the other hand, the restricted zone will be firewalled and connected only to authorized control systems with multi-factor authentication. The function of the restricted zone is to oversee the main engine, power distribution, and propulsion. Security measures include access only via authorized control terminals, multi-factor authentication (MFA) is required, and enforced internal firewall rules.

**Crew & Passenger Network (Public Zone):** The public zone must be quarantined through a DMZ to eliminate unauthorized access to the critical OT systems. This zone can operate with the help of offering Internet access and communication tools to onboard personnel and guests. Measures taken for security purposes are separation in DMZ (Demilitarized Zone), fully separated from OT networks, and constant monitoring of unusual activity.

This strategy ensures that a cyber-breach in one zone does not affect critical ship operations. By isolating networks, any potential compromise in the public or administrative IT systems will not propagate to the critical OT infrastructure controlling the ship. Figure 5 goes beyond the segmentation strategy by showing how to set up cybersecurity protections for each part of the network. The diagram points out where monitoring points, intrusion detection systems, and security gateways are put, all to ensure the vessel has increased defences against cyber threats.

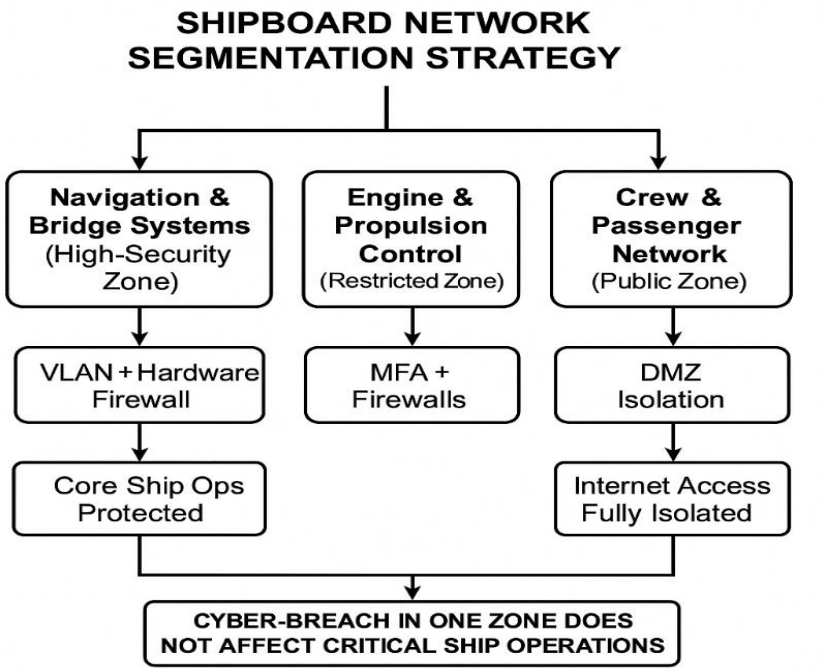


Figure 5: Shipboard Network Segmentation for Maritime Cybersecurity.

### 3.1.4 Core Vulnerabilities in Modern Ship Operations

As digital systems become increasingly embedded in maritime operations, the risk of cyber threats grows across multiple domains. Modern ships rely on complex, interconnected technologies that can expose vulnerabilities if not properly secured. These challenges span across the vessel itself, the port infrastructure, human behaviour, regulatory systems, and the broader supply chain.

**1. Shipboard Systems**

The ship is the heart of the maritime ecosystem, and its onboard systems, like navigation, propulsion, and communication, are cyberattack vectors. The interconnected nature of onboard technology allows a breach within one system to cascade into others. Therefore, it is important to carry out strict security protocols and isolate critical systems. The basis of maritime cybersecurity is vessel security, which operates in conjunction with and impacts other important aspects of the marine network. Ship security is also regulated by the web of international laws, conventions, and industry standards that require ships and ports to comply with security requirements and report piracy incidents to governmental agencies. Even though most marine incidents were caused by the failure to comply with international regulations concerning maritime safety, the adherence to these regulatory frameworks should be considered the minimal criterion, rather than the final objective of security efforts.

**2. Human Factors**

Crew members play a vital role in cybersecurity. Inadequate training, fatigue, or failure to follow procedures can unintentionally open the door to cyber threats. Human errors continue to be a leading cause of security incidents. Strengthening cybersecurity awareness and cultivating a safety culture are critical to reducing these risks. Crew members also have the distinction of being the first ones to notice and rectify security problems, as well as being the people who are at the forefront of implementing security practices. A vessel's security posture can be greatly enhanced by having crews that are knowledgeable in matters of security and possible threats [27]. Based on empirical findings, human-related events and activities have been identified as the major contributory factor to marine incidents in 65.8%-80% [28]. There are some very important parts within this comprehensive area, some of them are: 1) individual cognitive aspects, such as mental workload, situation awareness, decision-making strategies; 2) physiological factors such as fatigue, stress, and abnormalities in circadian rhythm. 3) interpersonal factors, like poor communication, coordination, and team dynamics; 4) human-machine interaction, particularly given the increasing automation and technological complexity of maritime operations; 5) organizational factors, like safety culture, management practices, and production pressure [29], [30].

**3. Regulatory Limitations**

Maritime cybersecurity regulations are still evolving. While international codes like the ISPS and IACS provide guidelines, they may not always keep pace with emerging cyber threats. Many standards are interpreted differently by operators, and some lack detailed technical guidance, which can result in inconsistent implementation across the industry. IACS Unified Requirements E26 [31] and E27 [32] are total cybersecurity regulatory requirements for the maritime industry. E26 deals with ship-level cyber resilience, while E27 covers cyber resilience at the onboard systems and equipment levels. They encompass the whole spectrum of a vessel's lifecycle from design, construction, operation, to maintenance, and review critical topics such as network segmentation, access controls, malware protection, and incident response. They assist ship owners, system integrators, and manufacturers in establishing effective cybersecurity, thus lowering the risk of cyber incidents. The International Ship and Port Facility Security (ISPS) Code [33] stipulates an international approach to spotting security threats and proactive measures against security incidents impacting ships or port facilities being utilized in trade. It creates a role and responsibility for governments, local administration, the ship and port industry at the national and international level.

**4. Port Vulnerabilities**

Ports are key points at which ships connect to onshore systems. Growing automation and digitalization in port management systems, such as cargo handling and vessel traffic management, build new attack surfaces. Ports need to adopt physical and cybersecurity measures to secure the infrastructure and ensure the operations are not disrupted. To counter the rising portend danger of coordinated cyber-physical attacks in ports, there is likely to be the future of port security to focus on the integration of cybersecurity with physical security approaches [34]. Its complex nature reveals how intertwined it is and that a combination of technological, procedural, and physical shields is required to create a solid wall against both traditional and evolving threats. There are many studies dealing with port infrastructure risk on an itemized basis [34], [35], [36]. Port security management is important in mitigating a vast diversity of perils and perils existing in a maritime setting. This approach involves a set of important aspects to secure the maritime operations and infrastructure, such as emergency response plans, surveillance, monitoring, perimeter security, an access control system, and cargo screening [37].

**5. Supply Chain Weaknesses**

The maritime supply chain comprises many stakeholders, systems, and geographical regions. Cyberattacks on suppliers, logistics platforms, or software providers may disrupt global shipping services. Besides, counterfeited hardware or malicious code installed in supplying components can clandestinely undermine the security of vessels. The process of moving commodities by sea, involving shipping, port operations, and frequently interior transportation, is referred to as a maritime supply chain. This intricate system connects numerous ports spread over several nations and continents and

encompasses a wide spectrum of stakeholders, including freight forwarders, shippers, carriers, and customs officials. The maritime supply chain is faced with several difficulties that could seriously jeopardize operational effectiveness and security. Among the many potential reasons for port interruptions, these include worker strikes, natural disasters, equipment malfunctions, and cyberattacks [38]. Examples of physical security threats to the marine supply chains include piracy (in the high-risk maritime zones), cargo theft, and illegal commodities smuggling [39]. These are issues that are still to be satisfactorily addressed. Since climate continues to change and the level of water in the seas continues to increase, port infrastructure and port routes are increasingly exposed to disastrous weather conditions [40]. In addition, operational risks, including equipment breakdown, delay in handling of cargoes, and human error in logistics planning, have significant effects on the efficiency of supply chains. Given that more than 80% of the global trade is conducted using ships [41]. Any disruption to the circulation of products in the world would be disastrous.

**6. Ineffective Risk Assessment**

Risk management frameworks that are employed to identify and combat cyber threats tend to differ in terms of qualitative and quantitative orientation. Failure to standardize and comprehensively evaluate some of the critical vulnerabilities may remain unnoticed. As well, many operators do not possess the Cyber risk analysis skills of evaluating the Cyber risk in depth, especially in remote and high-pressure settings. The absence of a globally established standard in terms of maritime cyber risk assessment techniques may become its cause. the source of any discrepancies. Some of the recent efforts have focused on setting a whole framework for risk analysis in maritime systems. For example, IACS Unified Requirement E22, [42] defines a systematic method of performing the estimation of the consequences of failures, which is essential for risk management. IACS Recommendation 166 [43], [44] is a recommendation for systematic risk assessments that take into consideration the occurrence and possible consequences of the hazards. These IACS initiatives are highly pronounced steps towards standardization, but the maritime systems are complicated, and the diversity of the operating realm remains an issue. Most importantly, there could be a lack of competence in cybersecurity and a maritime background to conduct comprehensive risk assessments [44]. Each component adds to the broader landscape of vulnerabilities, which, if left unchecked, increases the likelihood of cyberattacks.

In Figure 6, the flowchart illustrates each stage needed to evaluate cybersecurity risks in maritime operations. Steps include finding out what is important, examining potential threats, taking stock of weaknesses, assessing risk, and determining which actions help. It helps users manage and lower cyber risks on ships in an orderly way.

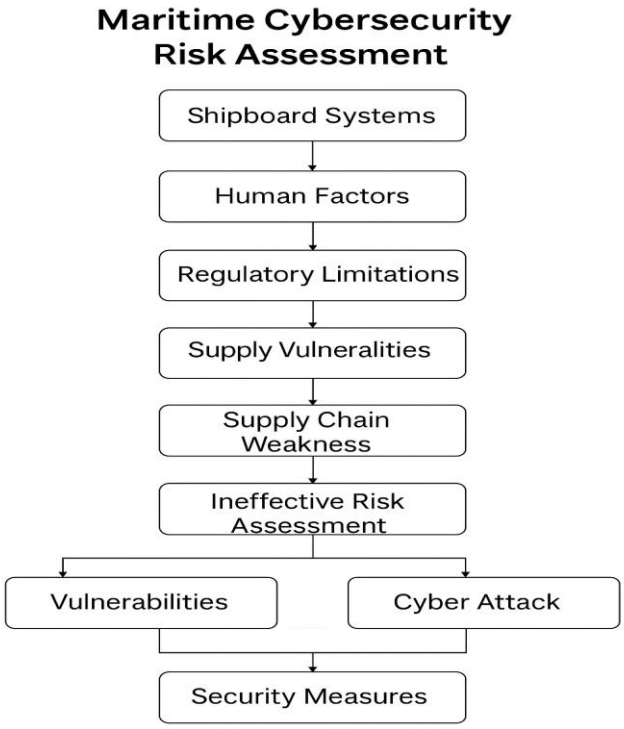


Figure 6: Flowchart for Maritime Cybersecurity Risk Assessment.

### 3.1.5 Chronological Overview of Major Maritime Cyber Incidents (2015-2024)

Ports, ships, shipping companies, and maritime authorities have become targets of cyberattacks in the last few years. Now, the industry is at greater risk of more complex cyberattacks, so recently observed issues should be looked at carefully. For this reason, this section considers only cyberattacks that have occurred since 2016, all the way up to 2024. A detailed analysis has been done on the twenty selected maritime events (refer to Table 1 and Figure 7 for more details).

**Table 4 Timeline of Major Maritime Cybersecurity Incidents (2015-2024).**

| Year | Incident | Description |
|---|---|---|
| 2015 | Targeted Phishing Attack in Cyprus | A shipping company suffered financial losses after a targeted phishing campaign where attackers impersonated a supplier, leading to misdirected payments. |
| 2016 | GPS Jamming Attacks in South Korea | Maritime navigation systems were disrupted by GPS jamming attacks, suspected to be conducted by a hostile state actor, impacting vessel operations. |
| 2016 | Software Vulnerabilities in U.S. Port Systems | A critical SQL injection vulnerability in a major port logistics system was disclosed, exposing ports worldwide to potential exploitation. |

| | | |
|---|---|---|
| 2017 | Navigation System Hijacking of German Vessel | Hackers took control of a vessel's navigation systems, preventing the captain from maneuvering the ship for hours, suspected to be linked to piracy attempts. |
| 2017 | GPS Spoofing in the Black Sea | Numerous vessels experienced GPS spoofing attacks, showing false locations inland, severely affecting situational awareness and navigation. |
| 2018 | Cyberattack on Port of Barcelona | A cyberattack on the Port of Barcelona's IT systems caused delays in cargo handling and reduced overall port operational efficiency. |
| 2018 | Data Breach at Australian Shipbuilder Austal | Hackers exploited stolen employee credentials to access sensitive company data, followed by ransom demands. |
| 2019 | GNSS Spoofing at Port of Shanghai | GNSS spoofing incidents disrupted vessel navigation in the Port of Shanghai, suspected to conceal sensitive areas or evade surveillance. |
| 2019 | Cyber Intrusion at James Fisher and Sons (JFS) | Unauthorized access to the company's systems resulted in operational disruptions and a decline in share value. |
| 2020 | AIS Spoofing Incident in Polish Waters | AIS location data of a U.S. naval vessel was spoofed to misrepresent its position near Russian territories, potentially escalating geopolitical tensions. |
| 2021 | Death Kitty Ransomware Attack on South African Port Operator | Ransomware attacks halted port operations, disrupting logistics and supply chains across the region. |
| 2022 | Port of Lisbon Ransomware Attack | The Port of Lisbon experienced a ransomware attack by the LockBit group, leading to operational disruptions and data breaches. |
| 2023 | DP World Australia Cyberattack | DP World, managing 40% of Australia's maritime freight, suspended operations at major ports due to a cybersecurity breach, affecting approximately 30,000 containers. |
| 2024 | Ransomware Attack on Singapore Freight Firm | A freight company in Singapore faced severe operational disruptions after a ransomware attack encrypted critical IT systems, causing delays and data loss. |

**2015 - Targeted Phishing Attack in Cyprus**

A company based in Cyprus was hit by a well-planned phishing scam. Attackers appeared to be trusted suppliers by replicating the way they regularly email and communicate with the victims. Because of this, money designated for the company was taken and used on fraudulent accounts. It was only when the genuine supplier reached out about unpaid bills that the deception became clear, leading to big financial losses for the company [45].

**2016 - GPS Jamming Attacks in South Korea**

In 2016, there were reports of GPS jamming around South Korea, disrupting the systems used for navigation and tracking vessels. Such attacks on GPS signals were believed to be carried out by adversarial groups, leading to widespread problems for businesses and regular citizens. Because of the issue with GPS, over 70 fishing boats were brought back to port by the coastguard, AFP reported. We have not heard of any disruptions to flights so far [46].

**2016 - Software Vulnerabilities in U.S. Port Systems**

Port logistics software that is used by many companies contains a significant security gap that allows users to access data in real time. Because of this vulnerability, attackers could try SQL injection to execute pesky codes, which could threaten both the security and accessibility of port systems. The problem was made public by an ethical hacker, thus attracting attention but also opening users to threats before the patch was applied. According to ICS-CERT, the vendor has already reached out to all the customers, and everyone in the United States has already installed the fixes to protect their systems. However, the agency noted that the security issue has already been used to attack several US companies, causing some important data to get lost [47].

**2017 - Navigation System Hijacking of German Vessel**

In the early part of 2017, a German container ship was controlled by hackers for many hours. The ship's handling was blocked during this cyberattack, putting many safety issues at risk. Experts from the company were called in to take over again. Some sources in the industry stated that the attack could be due to pirates trying to take control of the ship to board it illegally and ask for a ransom [48].

**2017 - GPS Spoofing in the Black Sea**

Several vessels in the Black Sea noted in 2017 that their GPS was giving them false information about where they were, for example, reporting they were at airports located inland. This act was discovered to be a deliberate spoofing of GPS, affecting where ships were on the map and their awareness of the situation around them. The fact that GPS signals were consistently changed over a large region pointed toward a single attempt to lead tracking systems astray [49].

**2018 - Cyberattack on Port of Barcelona**

The Port of Barcelona was hit by a cyberattack on its information technology system in 2018. Because of the incident, there were major delays in shipping and sorting merchandise at the port. As a result of the attack, trade activities were held up and efficiency was lowered, causing issues for those who use port services and affecting the economy [50].

**2018 - Data Breach at Australian Shipbuilder Austal**

In the middle of 2018, a data breach took place at Austal, a major Australian defence and shipbuilding business. Attackers were able to break into the system after buying stolen employee login details from the dark web. The company's sensitive data was made public, and the attackers asked for a ransom to return the same to the company [51].

**2019 - GNSS Spoofing at Port of Shanghai**

There were reports of GNSS (Global Navigation Satellite System) spoofing off China's coast in Shanghai and close regions in 2019. As a result, the navigation signals were altered, which might have prevented the ships from being located correctly and from talking to each other. The acts of spoofing were rumoured to be organized by the state to defend important facilities and avoid being spotted by warships [52].

**2019 - Cyber Intrusion at James Fisher and Sons (JFS)**

James Fisher and Son, a marine service company based in the UK, was hit by a cyberattack that put their systems at risk. Because of the incident, there were challenges in operations, and confidence from shareholders fell, as seen by the company's falling stock price [53].

**2020 - AIS Spoofing Incident in Polish Waters**

In late 2020, information from a U.S. naval ship was changed in a way that made it look like the vessel was somewhere it wasn't, close to the Polish coast. Spoofers changed the ship's location to make people think it was close to Russian waters, which could make people think differently about what was really happening between the two countries [54].

**2021 - Death Kitty Ransomware Attack on South African Port Operator**

Widespread disruption in operations hit a South African transportation company after the Death Kitty ransomware targeted it in 2021. Because of the encryption, port operations were disrupted, and the company faced serious pressure to deal with the cyber incident [55].

**2022 – Port of Lisbon Ransomware Attack**

The third-largest port in Portugal, the Port of Lisbon Administration, was hit by a LockBit ransomware group attack on Christmas Day. Being situated near the heart of Lisbon, the Port of Lisbon is essential to the city's infrastructure, since it attracts many ships from the continent and the rest of Europe [56].

**2023 – DP World Australia Cyberattack**

On 10 November, the technology team working for DP World Australia noticed that someone had gained unapproved access to the organisation's Australian corporate systems. To isolate the incident, the DP World Australia team took the step to remove the network from the Internet. Though it delayed work at the port, it was able to stop the incident from spreading. Since the first detection, DP World Australia and its advisers have put in a lot of effort to recover operations and find out the effects of the incident. From Monday, 13 November, DP World Australia was able to resume work at the port, and since then it has been cooperating closely with all the relevant people to get back to normal speed as soon as possible [57].

**2024 - Ransomware Attack on Singapore Freight Firm**

In 2024, a world-leading freight and logistics company based in Singapore suffered from a highly targeted ransomware attack. As a result of malware, the company's essential technology was made unreadable, which halted many tasks and delayed the delivery of orders. It revealed that ransomware is a constant danger to the shipping industry and is challenging the security of sensitive infrastructure more and more. As of Apr 7, 2024, DBS said it has found through preliminary investigations that about 8,200 customers may have had their letters or statements compromised. BOC says that about 3,000 of its customers whose letters were printed and mailed by the vendor were affected. Customer names and addresses were part of the data disclosed, and in a few situations, the loan account numbers were released as well [58].

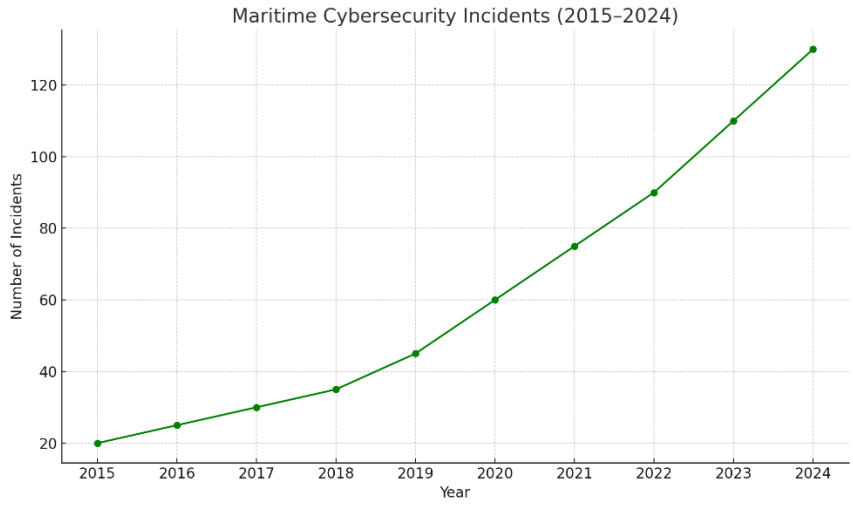


Figure 7: Rising Maritime Cyber Threats: 2015–2024 with Key Incidents.

Maritime cybersecurity incidents have risen steadily from 2015 to 2024, as reflected in the graph shown. At first, the number of reported incidents was low. Meanwhile, these types of incidents have grown more frequent and severe during the last 10 years. Such an increase in incidents may be due to the maritime industry's increasing reliance on digital technologies for seamless operations. Several major cyberattacks have pushed the trend of increasing incidents higher. A major ransomware attack in 2017 on Maersk disrupted many operations within the international shipping industry. Several notable attacks found in recent years allowed criminals to refine their tactics and focus their efforts on maritime assets. In the years leading up to 2024, maritime security experts began worrying about threats to critical infrastructure, demonstrated by the suspected attack on undersea telecommunication cables in the Baltic Sea. Bridging the cybersecurity requirements and encouraging compliance with standards set forth by the IMO.

### 3.1.6 Clarifying Network Protection Safeguards for Ship

Modern ships are becoming more reliant on interconnected Information Technology (IT) and Operational Technology systems for navigation, propulsion, communication, management of cargo, and crew services. This interconnectivity increases efficiency as well as situational awareness, while at the same time opens the vessels to major cyber threats. Extensive network protection measures are necessary to allow for the mitigation of these threats. This section provides key protective measures as per the current science and global maritime cybersecurity frameworks. Ship networks require customized safeguards to counter maritime-specific cyber threats:

**1. Network Segmentation**

One of the main cybersecurity steps is to segment shipboard IT and OT networks into separate, isolated segments to contain the spread of cyber incidents. By way of example, critical systems like bridge navigation, controls for the engine should be isolated from crew and passenger networks using Virtual Local Area Networks (VLANs) and a Hardware firewall. This zoning will prevent attackers from buttressing laterally in ship systems, if there is a breach in non-sensitive areas. Aboard a cruise ship, crew WI-FI is separated from the bridge systems through VLANS and a hard hardware firewall. If the smartphone belonging to a crew member was infected by public internet sources, there is no danger of spreading to the navigational systems, as it is isolated [59], [60].

**2. Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)**

Firewalls control the movement of data between various network zones using security policies. IDS and IPS software detect network activity to instantly respond to malicious activity, thus they make firewalls work. These systems are important for detecting and dealing with potential cyberthreats to propulsion,

communication, and navigation systems. To restrict communication with its satellite communication module and cargo control system, a tanker uses a firewall. A data exfiltration is prevented using an IDS, which typically identifies a high number of outgoing connections, followed by the sending of alarms. Firewalls are very important for network security by filtering traffic based on set guidelines. There are numerous kinds of firewalls, including packet-filtering, stateful inspection, proxy, and NGFWs. Packet-filtering firewalls check each packet at the network layer, while stateful inspection firewalls also keep track of what is happening with each connection. At the application layer, proxy firewalls can fine-tune and filter traffic, giving more options for control. Traditional ways of filtering packets are joined with more advanced options in NGFWs, making the systems more powerful for defence. From the easy packet-filters of the late 1980s, firewall technology has advanced a lot to become the NGFWs that are commonly used today. To maintain firewalls, update them regularly, always monitor their status, and occasionally perform security audits. But firewalls encounter issues related to their setup and management, and they could be vulnerable to advanced persistent threats. Experiences from case studies prove that firewalls alone are not enough, so they should be part of a bigger security plan [61].

**3. Encryption**

Encryption is a fundamental element of cybersecurity, protecting data by converting it into an unreadable coded format without the appropriate decryption key. There are two primary types of encryption: symmetric, which uses the same key for encryption and decryption, and asymmetric, which uses a pair of keys, one for encryption and one for decryption. The evolution of encryption technologies has seen significant advancements from early substitution ciphers to sophisticated algorithms like the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). Recent trends in encryption include the development of post-quantum cryptographic algorithms designed to resist quantum computing threats. Best practices for implementing encryption involve using strong, standardized algorithms, regular updates to encryption protocols, and consistent application across all data states. Despite its strengths, encryption poses challenges such as computational intensity and key management complexities. Case studies demonstrate the effectiveness of encryption in protecting sensitive information but also highlight the critical need for efficient key management practices [61].

**4. Access Control and Authentication**

Multi-factor authentication, one-of-a-kind user accounts, and role-based access prevention allow only those with appropriate clearance to operate sensitive parts of the ship. Only authorized users with MFA on a container ship can interact with the ECDIS connected to the ship's navigation system. It diminishes the possibility of changes being made to voyage plans by someone unauthorized [32]. With MFA, individuals are required to provide more than one verification to access a system, which greatly reduces the likelihood of unauthorized entry. Earlier versions of MFA depended mostly on passwords, but now, many other methods like biometrics and behavioural analytics are supported. Nowadays, MFA includes

biometric measures, like fingerprint and face scans, to verify the user, and it also uses behavioural monitoring to catch unusual behaviour. Ships can check that their MFA suits their existing systems, teach people because it is beneficial, and frequently adjust and examine their processes for authentication. Even though MFA offers much security, it still deals with annoyance to users, bypass options such as SIM swapping, and is not always simple to implement [61].

# 4 Cybersecurity Measures

## 4.1 Maritime Cybersecurity Measures

Cybersecurity must be provided for both the IT and OT systems in the maritime sector to prevent unauthorized use, viruses, and other online risks to essential systems. Cybersecurity in maritime networks should protect both the IT and OT environments. Since ships depend more on computers, satellites, and robotic navigation, there are significant risks to security, operation, and shipping safety. To protect the organization, build tough policies, secure the system with firewalls and encryption, and continue to improve and monitor the security system. Figure 8 outlines the main cybersecurity strategies advised for environments in the maritime sector. It describes technical protections (e.g., firewalls, encryption), outlines team skills (e.g., crew training), and explains requirements, giving a complete look at how to secure ships from possible cyberattacks.

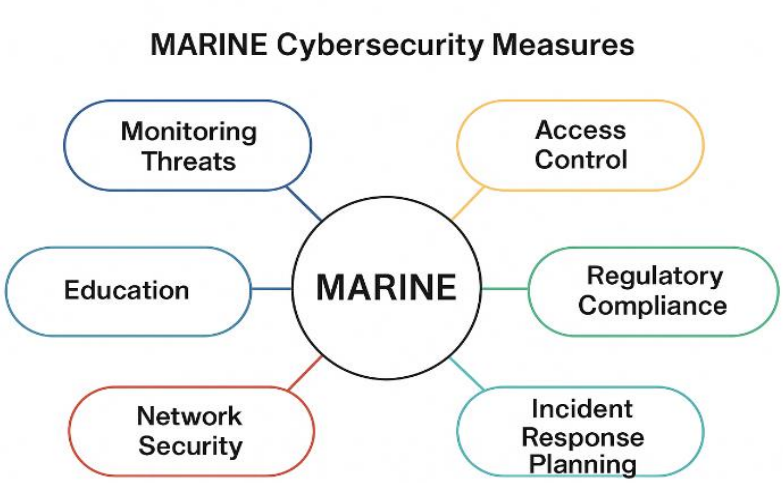


Figure 8: Marine Cybersecurity Measures.

### 4.1.1 Security Policy Development

A cybersecurity framework relies heavily on its security policy. In maritime communications, it is necessary to have effective policies explaining how to control access to vital systems, manage data, and report any security incidents. Designing these policies by considering issues such as being in remote regions, using satellite signals, and the interaction between IT and OT systems is important. Crew members should have a clear idea of what they are responsible for regarding security. Maritime defence is built around cybersecurity, using access control, management of data, and meeting standards set in resolutions MSC.428(98) and UR E26/E27 from the IMO [62]. Among the main aspects are:

**1. Centralized Access Management with Active Directory (AD)**

By assigning users to specified roles that correspond with job duties, AD's Role-Based Access Control (RBAC) simplifies permissions. Important elements consist of:

- **AGDLP Principle:** Group accounts inside of each other (Account, Global, Domain Local, Permission) to automate assigning rights. So, someone with a "Navigation Officer" role could join "Bridge Systems," a global organization, and thus receive authorization to use ECDIS and AIS within their region [63], [64].
- **Least Privilege Enforcement**: Activating the Least Privilege Enforcement policy prevents users from accessing systems they do not need. It leverages current permissions to set up the best possible roles [63], [65].
- **Automated Provisioning/Deprovisioning**: When someone's roles change (for example, during crew transfers), access is instantly revoked by identity management systems [64], [65].

**2. Security Audits Aligned with GDPR and NIS2**

Repeated audits make certain that businesses are always following new legislation.

- **GDPR Compliance:** Centres on ensuring the PII of crew/passengers is properly protected. Teams should routinely check for the safety of logbooks, access their data access logs, and report any breaches within three days [66], [67].
- **NIS2 Directive:** It ensures that critical maritime infrastructure, such as port systems and vessel traffic services, is audited. Checks include:
    - Incident Response Testing: Through simulations, ransomware was deployed on test navigation systems to assess the results [68].
    - Third-Party Vendor Assessments: Checking how they handle security for satellite communications [68].
- **MARINE Framework:** Helps with creating required checklists for GDPR, NIS2 and IMO MSC.428(98) and collects evidence for compliance checks [68].

**3. System Hardening via IEC 62443 Standards**

Ensures that industrial control system (ICS) protections are used in maritime operations technology (OT):

- **Risk Assessments:** Find any weak points in devices such as ballast controls or systems for engine monitoring. An example is designing power generation for a different section than crew Wi-Fi [66], [68].

- **Technical Controls:**
    - Default Password Elimination: Remove the vendor-provided passwords on satcom terminals as well as ICS workstations [66].
    - **Protocol Security:** Remove access to old protocols (such as Telnet/23) and use SSH for remote access to the system [66], [68].
- **Continuous Monitoring:** Add intrusion detection systems (IDS) to spot unusual traffic in ICS, focusing on the IEC 62443 "Detect" aspect [68].
- **Security Levels (SL):** Assign a security level of SL2-SL3 to all marine systems; fortify them by adding multiple firewalls for engine control [68].

By using these practices, risks like unlawful use of bridge systems or GPS are reduced as required by the NIS2 and IACS UR E26/E27 guidelines [67], [68].

### 4.1.2 Incident Response Plan

An Incident Response Plan (IRP) helps ensure that in case of a cyber incident, it can be handled efficiently and promptly. The sea is not easy to deal with because vessels are constantly on the move and often rely on remote communication. For this reason, an IRP is developed to meet the demands at sea, so events are swiftly addressed and their effect on ship operations is reduced.

- Incident identification and classification: For example, the IRP shows the vessel's crew how to notice and classify the incident if their navigation system is attacked by ransomware.
- Roles and responsibilities: Every member of the crew and IT workers knows precisely what actions to take in case of an emergency, including controlling systems or switching to manual operation of the power tools [66].
- Communication protocols: For each scenario, specific rules are given for telling teams within the company and any port authorities or regulators.
- Containment and eradication: Steps to separate infected networks or devices by cutting off a suspicious ECDIS link from the main network.
- Recovery and restoration: Backing up data and systems to recover them and checking their integrity before reattaching them to the network.
- Post-incident analysis. After an event occurs, the organization reviews the incident, improves the IRP, and makes sure the lessons are applied [68], [69], [70].

**Real-time example:**

The cargo management system of a shipping business gets infected with malware. The IRP allows the team to move to manual tracking of cargo, distinguish where the error occurred, and update their supervisors, avoiding large disruptions in their work [68], [69].

### 4.1.3 Firewalls and Access Control Policies

A cybersecurity framework for naval and transportation systems would not be complete without firewalls. They prevent authorized users from breaking into the network by scanning websites and protecting the network from cyberattacks. System administrators on ships need to configure firewalls so that communication between IT and OT systems is tightly managed. Best practices include:

- Network segmentation: Isolating the important OT equipment, like engine controls, from less safe networks protected by firewalls [70].
- Port filtering: Block any ports or protocols that are unnecessary to make network safer.
- Role-based access control: Ensure that sensitive navigation gear, such as on a bridge, can only be accessed by authorized crew members by using role-based access control.

**Real-time example:**
A firewall in a vessel is used to block all connections to the ECDIS except for those coming from the navigation officer using their workstation. As a result, crew devices cannot infect critical navigation systems with malware [70].

### 4.1.4 Multi-factor Authentication

MFA helps keep the ship's crew protected from various cyberattacks. At sea or elsewhere in the maritime world with weak security measures, MFA is necessary to secure sensitive data from unauthorized people. MFA is often based on three factors: information the user knows, items the user owns, and details about them. Critical systems such as navigation, propulsion, and communication can be secured on board ships using MFA.
MFA makes it difficult for anyone without approval to gain access to important systems [71], [72].

- Things to know: Password or PIN.
- Hardware token or OTP sent from an authentication app is something people can have.
- A way: Biometric solutions, such as using fingerprints or a person's face.

**Real-time example:**
The engineers onboard can use a hardworking token and a PIN code to control the ship's engines. The captain is authorized to use the navigation system using both her face and a password. Communication officers are given a temporary OTP on their secure app, so if a password is breached, it cannot be used by an unauthorized person [72].

### 4.1.5 Encryption and Secure Communication Protocols

Communication over satellites and remote methods used in the maritime industry depends on encryption for security. For security purposes, the main social media platforms must hide important data such as

navigation details, manifest lists, and crew messages by encrypting them. With encryption, any important information on the maritime system is protected from being seen or changed by others [73], [74] .

- Data in transit: TLS and VPNs should be applied to make communications between the ship and shore or among different parts of the ship secure [73].
- Data at rest: Sensitive information, such as logbooks and crew manifests, kept on the ship's systems should be encrypted [73].

**Real-time example:**

Shipping companies rely on encrypted email to share information between different vessels and their headquarters. Any data sent by the vessel to shore control centres is safe from attackers thanks to strong encryption on a VPN network.

# 5 Monitoring Systems and Tools

The security, performance, and resilience of maritime networks depend on using monitoring systems and tools. Ships depend on a combination of IT (Information Technology) and OT (Operational Technology) systems today, so monitoring systems need to be active all the time to catch cyberattacks, unexpected events, and make sure the ship meets international rules [75]. This chapter outlines how to successfully plan, make use of, and improve monitoring aboard ships, emphasizing SNMP, MRTG, NMS, SIEM, IDS/IPS, and their combination.

## 5.1 Planning and requirements gathering

For a monitoring system to function well, it must be planned carefully, and every requirement should be gathered. At this point, the following is necessary:

- **Analysing Network Architecture:**
  Draw a map of every IT and OT setup on the ship; identify where the bridge, engine, cargo, business, and crew systems interact. Network diagrams help to make things clearer [73].
- **Finding What Assets are Important:**
  The navigation, propulsion, communication, and safety systems are most important to watch because they maintain the ship's safe and steady operation [76].
- **Identifying the Objectives for Monitoring:**
  Tasks could be tracking how an organization operates, catching threats, ensuring IMO or NIS2 compliance, or handling multiple of these at the same time. Knowing the goals directs someone to the right type of tool and how to set alert triggers [77].

The table below shows the most important assets used in maritime environments, labelling them by type (navigation, propulsion, communication, business IT, and crew and passenger systems). For every category of assets, the table reveals systems and sets a priority for monitoring. The inventory helps to prioritize cybersecurity so that the most important shipboard areas are given the main attention.

**Table 5 Example Critical Asset Inventory.**

| Asset Type | Example Systems | Monitoring Priority |
|---|---|---|
| Navigation | ECDIS, AIS, Radar | High |
| Propulsion | Engine Control, PLCs | High |
| Communication | VSAT, Fleet Broadband | High |
| Business IT | Servers, Workstations | Medium |
| Crew/Passenger | Wi-Fi, Laptops | Low |

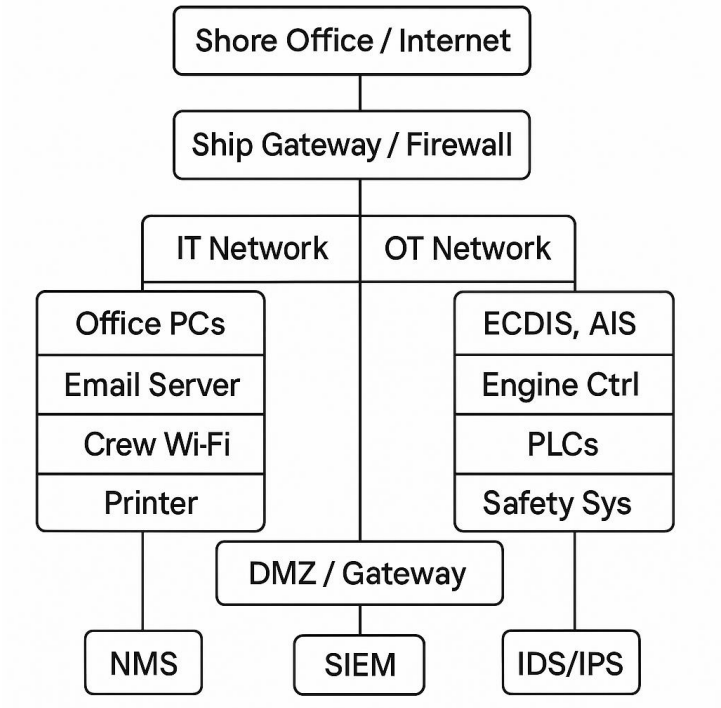


Figure 9: Ship Network Monitoring Architecture example.

Figure 9 gives a concrete example of how to build a network monitoring system aboard a ship. It demonstrates how monitoring tools such as NMS (Network Monitoring System), IDS/IPS, and SIEM all connect so they provide immediate visibility to security issues on the ship.

## 5.2 Preparation of Infrastructure

A solid monitoring system is achieved by paying attention to careful planning and requirements collection. In this phase, we need to:

- **Server Provisioning:**
  Setting up dedicated servers (either virtual or physical) should be used to run NMS, SIEM, IDS/IPS, and SNMP/MRTG collectors [78].
- **Network Configuration:**
  Give all monitoring solutions access to every part of the network. Turn on SNMP on essential devices and alter firewall rules to monitor all the data.
- **Security Considerations:**
  Preventing anyone from accessing this information is possible through access controls and encryption [73].

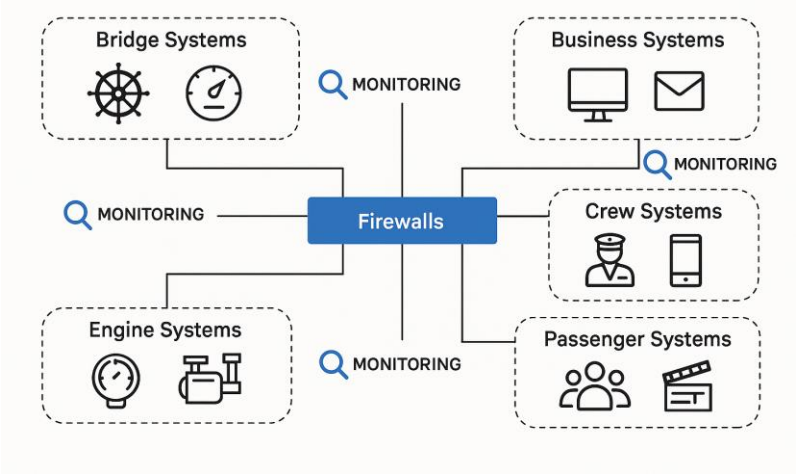


Figure 10: Example Vessel Network Segmentation.

Figure 10 displays clearly how a vessel could have a bridge, engine, business, crew, and passenger areas as part of its networks. This means showing where firewalls, access controls, and observation sensors should go, which serves as an outline for designing a secure network on a ship.

## 5.3 Monitoring tools installation and configuration

When the infrastructure is finished, it's time to install and configure the monitoring tools. Each of these tools is set up to cover one area: monitoring how a network performs, searching for threats, or helping supervise logs of events.

### 5.3.1 Network Monitoring System (NMS)

SolarWinds and PRTG NMS tools are used to track performance and find devices in real time. They collect information from routers, switches, firewalls, and similar devices to detect high latency, packet loss, and device failures.

- Device discovery: NMS can detect devices by using either SNMP or ping without human input [78].
- Alert configuration: Set up limits for important indicators such as CPU or bandwidth. To give an example, PRTG allows to be alerted if bandwidth use passes 80% or if a device is offline.

**Real-World Example:**
A company from Europe monitored its IT and OT networks with PRTG and received instant alerts when there were network blockages or device failures. As a result, performance and incident handling both improved [78].

### 5.3.2 Security Information and Event Management (SIEM)

SIEM platforms such as Splunk and IBM QRadar collect server, firewall, and IDS/IPS logs and help discover security problems as they happen.

1. **In constant monitoring and detection**
   - Log Collection: All logs received from NMS, IDS/IPS, firewalls, OT/IT devices, and endpoints on board the ship are collected by the SIEM [76].
   - Correlation and Alerting: Using rules specific to shipping, the SIEM identifies unusual events such as excessive ECDIS login failures and inexplicable access to engine controls [76].
   - Alert Review: The alert review takes place in real time by a team from the Security Operations Centre or other designated crew, who simply put, rate and sort the alerts according to importance [76], [68].

2. **Incident Identification and Categorization**
   - Incident Verification: The analyst confirms that the incident is real by checking if, for example, malware was found or access was unauthorized [71], [78].
   - Categorization: We classify incidents using their effect and level of importance (such as low, moderate, high, or critical) to direct who receives them and how resources are used [78].

3. **Containment and Mitigation:** Encouraging people to reduce risk and routine tests for pregnant people.
   **Initial Containment:**

   - Take the affected systems off the network (for example, cut off access to the infected workstation or partition the broken OT network [75].
   - Turn on manual modes for operation or movement as needed according to ClassNK fallback instructions [69].

**Mitigation Actions:**

- Making use of controls integrated with SIEM to obstruct malicious traffic and block especially dangerous accounts.
- Add endpoint or network blocking tools (for instance, EDR, set firewall rules) [75], [79].

**4. Eradication and Recovery:**

**Root Cause Analysis**:

The aim is to interrogate SIEM logs and the data from IDS/IPS to discover what happened and how widespread it might be [75], [79].

**System Restoration:**

- Recover the systems from clean backups
- Reunite split systems as soon as all tests have passed successfully.
- Should the main safety system be affected, go to a state that minimizes risk, such as lowering engine output [73].

**5. Communication and Reporting:**

**Internal Notification:**

Make sure the master, DPA, and IT manager are informed according to the communication plan for the incident (on board and at the office) [68], [78].

**External Notification:**

If any country's regulation calls for it, it is wise to pass on the problem to the authorities, the flag state, or CSIRT (e.g., as with the NIS2 24-hour rule) [68].

**Documentation:**

After the incident, put down actions, timelines, and results in the incident log as a reference [73].

**6. Post-Incident Review and Improvement:**

**Lessons Learned:**

Carrying out an after-security incident review so that it can be learnt from successes, observing where improvement is needed, and finding out how to prevent future problems.

**Update Playbooks:**

Changing correlation rules, response procedures, and training staff with insights from what was found [79].

In Figure 11, the workflow for handling incidents at sea is broken down by a Security Information and Event Management (SIEM) system. The process described includes detecting threats, alerting

others, stopping the threat, removing it, recovering the system, and analysing after the response for future improvements, accompanied by the key role SIEM plays in these efforts.

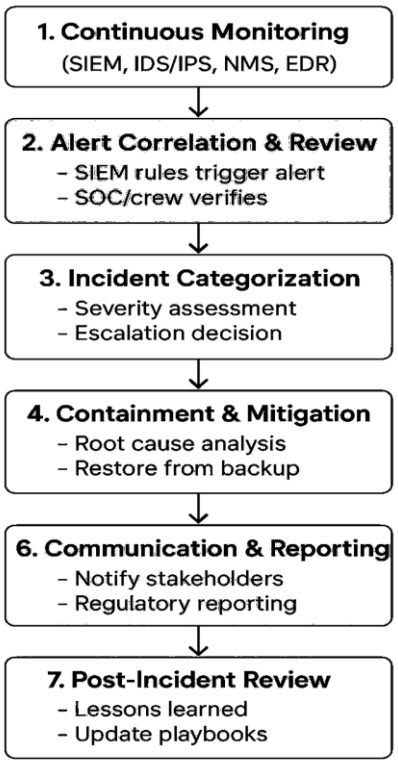


Figure 11: SIEM-Driven Maritime Incident Response.

### 5.3.3 Intrusion Detection/ Prevention Systems (IDS/IPS)

Devices such as Palo Alto Networks NGFW or Snort are used in IDS/IPS to look for signs of cyber threats in network traffic. An IDS is created to spot attacks, while an IPS defends against them and can prevent them right away.

- Signature-based detection: Identifies attacks by using known methods of threat signatures.
- Behaviour-based detection: Finds unseen problems, for instance, unusual crosstalk between OT and IT networks [80].

**Real-World Example:**
Both maritime and industrial sectors prefer Snort due to its flexible design and many rules.

### 5.3.4 SNMP and MRTG for Ship Network Monitoring

SNMP is a basic way to keep an eye on and manage networks by using switches, routers, firewalls, and servers. With SNMP on board ships, status, traffic information, and alerts from both the IT and OT network areas can be retrieved quickly. Thanks to IEC 61162-460-compliant ship monitoring software,

devices on board a ship can be checked for health, invasions of devices, and bad behaviour, as the system sends automatic alerts when anything happens [81].

This open-source tool, called Multi Router Traffic Grapher uses SNMP to create graphs with details on how much bandwidth is being used as time goes on. MRTG produces visual graphs of traffic, so maritime IT experts can see if there are any uncommon spikes, lots of used up bandwidth, or any signs of slow or unsafe system performance.

Best Practices:

- Make sure SNMP agents are put on every crucial shipboard device.
- Set up SNMP traps so that alerts are delivered right away.
- MRTG is used to create traffic and bandwidth graphs for important network interfaces.
- Include SNMP and MRTG output in SIEM or NMS solutions for all-around monitoring.

**Compliance:**

SNMP and MRTG are advised in the guidelines because they let users always monitor, respond to dangers fast and meet standards such as IEC 61162-460 and DNV cyber secure notations [81], [82] .

.

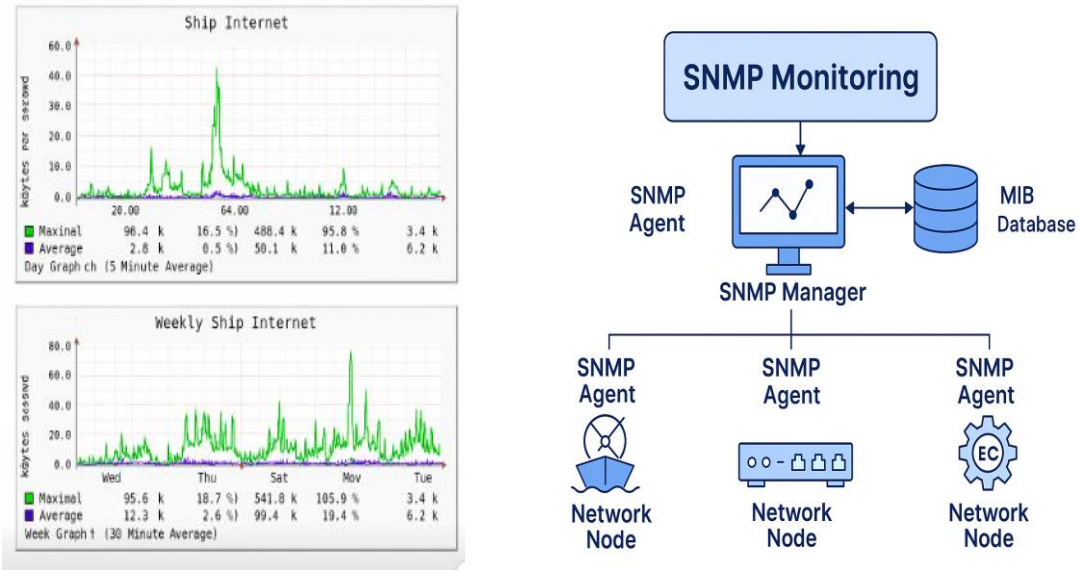


Figure 12: Example MRTG and SNMP monitoring tool.

This figure demonstrates how MRTG (Multi Router Traffic Grapher) and SNMP (Simple Network Management Protocol) are employed to check the performance of networks on ships. It has graphs and dashboards that let us view bandwidth usage, see the current status of devices, and monitor network activity, all showing why it is necessary to keep an eye on things in IT security.

## 5.4 Integration and Data Flow

When we use monitoring tools in combination, data is smoothly delivered, and we can see everything from one place.

**NMS and SIEM Integration:**
The output of NMS performance can be shared with the SIEM to help relate security events [73].

**DS/IPS and SIEM Integration:**
Any event with security concern spotted by IDS/IPS is handed over to SIEM to be looked at in greater detail and handle the incident.

**SNMP/MRTG Integration:**
Metrics collected by SNMP and shown by MRTG graphs can be brought into SIEM or NMS dashboards to display all information in one place.

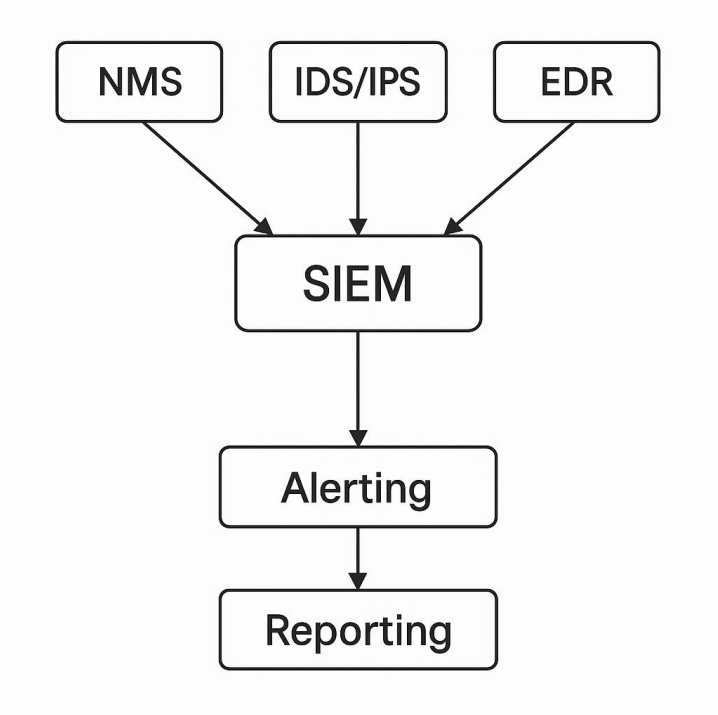


Figure 13: Integrated Monitoring Data Flow.

The diagram illustrates how data from NMS, IDS/IPS, and EDR (Endpoint Detection and Response) is transferred to a central SIEM platform. It explains the process of generating alerts and reports and how they are shared with the appropriate members, stressing the role of integrated monitoring for both awareness and reacting to situations quickly.

## 5.5 Monitoring and Optimization

It is very important to regularly check and improve the website.

**Dashboards:**

Display of KPIs, like bandwidth, the status of devices, and security warnings, using graphical dashboards

**Alert Tuning:**

Routinely look over and update the limits for alerts so that non-critical ones are avoided without missing the crucial ones [75].

The table outlines the key performance indicators (KPIs) that shipboard cybersecurity systems use to monitor operations. The field looks at factors such as network speed, occurrences of failed logins, the presence of malware, and reports on system uptimes, and identifies which monitoring systems work best (for example, NMS, MRTG, SIEM, IDS/IPS). It shows the applicable data for both operations and security to keep monitoring and respond fast to incidents.

**Table 6 Example Monitoring Dashboard KPIs.**

| KPI | Description | Tool |
|---|---|---|
| Bandwidth Usage | Network throughput per segment | NMS, MRTG |
| Failed Logins | Number of failed authentications | SIEM |
| Malware Detections | Detected malware incidents | IDS/IPS |
| Device Uptime | Availability of critical devices | NMS |

## 5.6 Training and Documentation

To monitor well, it is necessary to have efficient staff and complete documentation.

**Staff Training**:

Perform regular sessions on how to notice and deal with emergencies. Having simulated exercises and drills is an important part of compliance [83].

**Documentation:**

Ensure installation, configuration, and operation guides are always up to date so operations are not affected if team members change [73].

# 6 Testing and Evaluation

Assessing the cybersecurity of maritime networks is necessary to ensure that the safety measures protect against changing dangers. In the maritime sector, with IT and operational technology working together, complete testing ensures the security and safety of navigation, propulsion, and vital ship systems. The contents of this chapter explain methods for determining the cyber resilience of maritime networks, primarily targeting vessel infrastructure. The process is supported by using the Purdue Model (Purdue Enterprise Reference Architecture) as the vital reference for structuring network security and setting up different security zones. To minimize the security risk, the model divides networks into five layers, so that critical OT devices are separated from IT and other networks.

Advanced platforms like Nozomi Networks and Forescout are then added to monitor networks, find threats, and ensure compliance based on the architecture put in place. Nozomi Networks is known for its expertise in securing OT and IoT devices, delivering AI-based detection of threats and management of vulnerabilities, especially designed for the marine industry. Unlike others, Forescout combines IT, OT, and IoT device visibility, automates policy oversight, and deals with security emergencies promptly. When used together, these tools guarantee that segmentation controls, IDS, and access policy are functioning as expected in line with DNV, NIST, and the Purdue Model.

Here, we look at the testing methods, helpful tools, and key results involved in checking the Ship's cybersecurity so that we can see how theoretical frameworks and updated technology help guard against cyberattacks in the maritime sector.

## 6.1 Maritime Networks Cybersecurity Testing and Evaluation

In this chapter, the maritime cyber resilience framework is given a thorough test and evaluation. The focus is to test security zones, security safeguards for the network, and incident response by using simulated cyberattack situations and assessing for vulnerabilities. These results reveal how the framework works effectively to detect, prevent, and manage threats to shipboard networks in real situations.

### 6.1.1 PERA Model: Purdue Enterprise Reference Architecture for Maritime Cybersecurity

The Purdue Model, which is another name for the Purdue Enterprise Reference Architecture (PERA), is designed to help manage and secure industry control systems (ICS). At Purdue University in the early 1990s, the model was developed to divide an industrial network into several layers, each responsible for

its tasks and the limits of communication [16], [84]. This is particularly important for marine use, because combining IT with OT increases how well the industry operates while also increasing risks from cyberattacks [85], [86].

A reference architecture from the Purdue Model is used in this study to assess and structure ship network segmentation. The Purdue Model separates the maritime network into parts, from physical devices and sensors (Level 1) to computers in use by businesses and connections to the outside (Levels 3–5). Using these four layers in testing allows us to evaluate the resilience of both OT and IT systems step by step. For this reason, penetration tests and vulnerability assessments are arranged so that each OT zone (Levels 0–2), operations management (Level 3), and IT/business zone (Levels 3.5–5) is tested on its own, ensuring area segmentation is tough and lateral movement within zones is low. As well as supporting defence-in-depth, this method fits with the leading industry guidelines for assessing maritime cybersecurity. Using the Purdue Model ensures that ship control systems are kept separate from IT and outside networks. Each level uses its procedures for protecting the network and spotting possible dangers [87], [88].

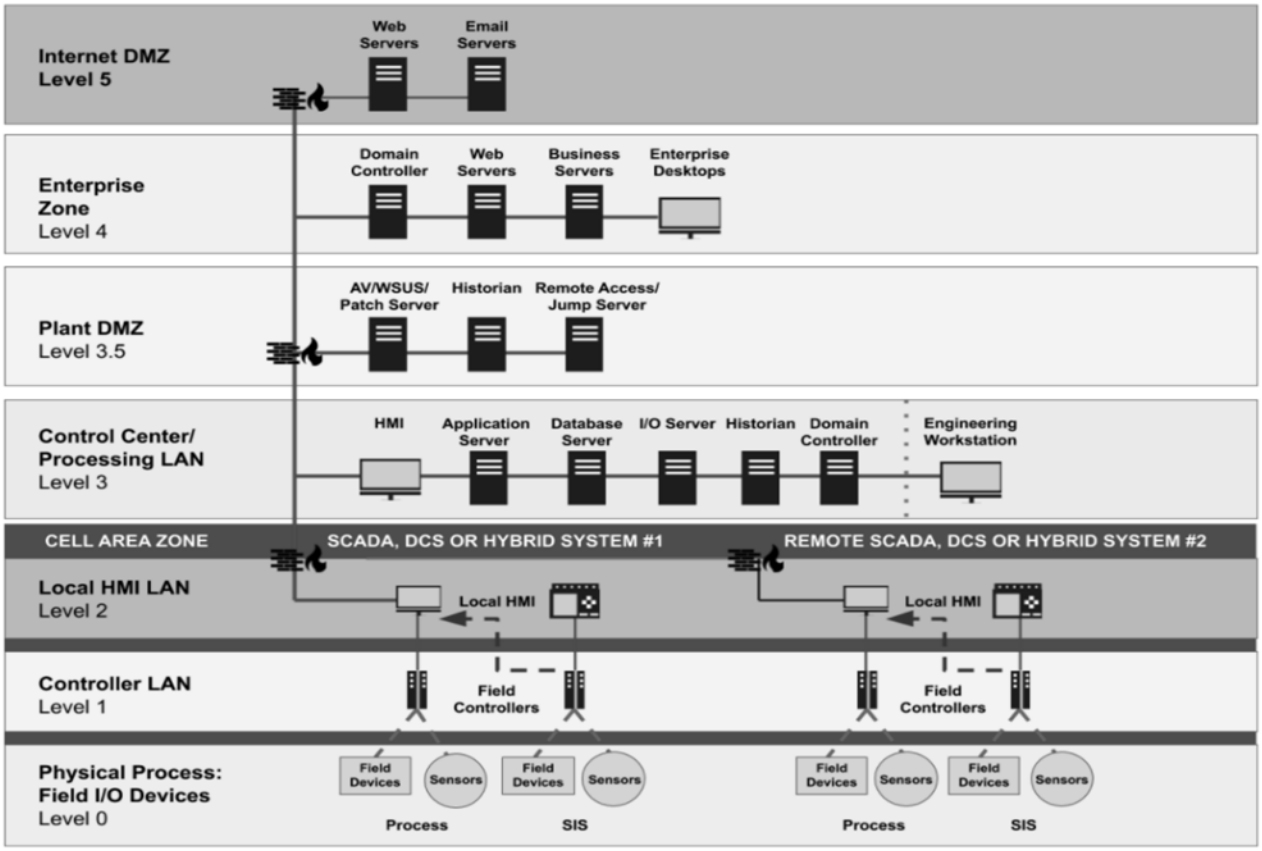


Figure 14: The Purdue Model for ICS Security [88].

The figure reveals the Purdue Model, which is a well-known standard for securing industrial control systems (ICS). It highlights all the layers in the OT system, starting at the enterprise level and ending

with field devices, and explains how using segmentation and access controls can protect key assets on ships.

**Table 7 The structure of the Purdue Model** [89].

| Level | Description | Maritime Example |
|---|---|---|
| Level 0 | Physical process (sensors, actuators) | Engine sensors, navigation sensors |
| Level 1 | Intelligent devices (PLCs, RTUs) | Propulsion PLCs, ballast control units |
| Level 2 | Local control and supervision (SCADA, HMIs) | Bridge automation, ship monitoring systems |
| Level 3 | Site-wide control and operations management | Ship management servers, historian databases |
| Level 3.5 | Demilitarized zone (DMZ) | Network buffer between OT and IT, filtering data |
| Level 4 | Business logistics (ERP, admin IT) | Crew/passenger admin, business applications |
| Level 5 | Enterprise network (corporate IT, cloud) | Ship-to-shore comms, remote support, internet |

Table 7 describes the structure of the Purdue Model that applies to maritime industrial control systems (ICS) and onboard networks. It lists the different tiers starting with Enterprise (Level 5), then Manufacturing Operations (Levels 4–2), Process (Level 1), and Physical Process (Level 0). Every layer in the table explains the main functions, systems, and data flows used in maritime operations. It points out that IT and OT should be separated and managed properly based on the Purdue Model, ensuring that the network onboard the ship is secure and stable.

The OT side, which runs operations and critical safety features, is in Levels 0–3. The tasks at these levels relate to IT, business functions, transport, and external conversations. The DMZ (Level 3.5) stands in the middle, applying strong rules and separating OT from IT to stop cyber threats from spreading [22].

In terms of the benefits of Security and Segmentation, the Purdue Model allows maritime organizations is:

- Layered security is important: Keep the most critical OT systems separate from IT and external networks [86], [90] .
- Secure each layer by using firewalls, VLANs, and monitoring, so if one area is attacked, it doesn't become a problem in the rest [22].
- Recommend the Purdue Model, which is supported by NIST 800-82 and IEC 62443, for use in the security of Industrial Control Systems [16], [86].

Although first introduced in 1983, the Purdue Model is widely used in OT environments at sea. Maritime cybersecurity guides often refer to these principles, treating them as top practices for designing a ship's network [85], [86]. The Purdue Model separates ship control systems from IT and Internet networks,

enhancing safety onboard. Every level uses cybersecurity controls and surveillance methods to enable defense-in-depth [87]. Because it has been proven useful elsewhere, maritime organizations should use the Purdue Enterprise Reference Architecture (PERA) as the main structure for planning future cybersecurity and resilience efforts on ships. The Purdue Model's suggestions of network division and extra protection steps allow ship operators to identify and handle OT and IT security risks. Using this strategy means meeting recognized international standards such as IEC 62443 and NIST Cybersecurity Framework and building a lasting platform for handling risks, responding to cyberattacks, and strengthening maritime cybersecurity [86], [89], [91], [92].

### 6.1.2 Network Security Testing Procedures

A strong and reliable cyber resilience strategy in the maritime sector requires a well-structured method for testing networks. In this part, a step-by-step approach from the Purdue Model is suggested to assess all important kinds of technology for weaknesses, the efficiency of segmentation, and how accessible the team may be during an incident [89], [91], [92].

**Step 1: Creating a Network Diagram with the Purdue Model**

The first thing to do is draw the ship's network architecture based on the Purdue Enterprise Reference Architecture (PERA). One should find all assets, information flows, and trust rules in each section, ranging from devices and control systems at Levels (0–3), all the way to business IT and external links at Levels (4–5) [89], [91], [92]. By making a map, specialists find it easier to protect and test each separate part of the system.

**Step 2: Start with Layered Security Assessment**

Separate assessments of security should be done for all the Purdue Model layers.

- OT Zones (Levels 0–3): Focus is on industrial control systems, sensors, propulsion, and navigation equipment.
- DMZ/IT Zones (Levels 3.5–5): computers for crew and staff, and connections to the external network are the main concerns in DMZ/IT Zones.

Because of this separation, potential problems specific to each area are handled, while IT and OT are kept apart securely [89], [91].

**Step 3: Putting the Tools Online and Distributing Roles**

It is good practice to use advanced tools designed for every zone.

- Asset discovery, constant system monitoring, finding anomalies, and vulnerability handling should be handled using Nozomi Networks in those parts of the infrastructure where OT assets live. By using Nozomi's AI, NIST and IEC 62443 standards are easier to follow, as it shows risks linked to legacy and IoT devices [16], [93].

- For Zone 3.5 to 5, also known as DMZ and IT zones, Forescout is recommended since it supplies a full inventory of networked devices, secure zone partitioning, and proper policy observation. Forescout helps stop unauthorized or uncompliant devices from connecting to the network, which supports the cyber expectations of IMO and DNV [94].

**Step 4: Testing Activities**

Recommended testing activities include:

- Penetration testing and vulnerability scanning: Nozomi and Forescout were used to run penetration and scanning tests on OT devices and at the IT/OT boundary to detect any issues and review how machines are separated.
- Configuration and segmentation validation: It's important to go over the configuration to make sure the firewall, VLAN, and access control are isolating different zones as intended.
- Simulated incident response drills: Issue red team/blue team practice incident exercises to assess how a team would handle and react to actual alerts, using Nozomi and Forescout to send notifications automatically [16], [94], [95], [96] .

**Step 5: Making Sure the Setup Is Legitimate**

All testing activities should comply with IEC 62443, NIST Cybersecurity Framework, DNV Cyber Secure notations, and IMO recommendations. Necessary information about the findings and remedies should be organized for continuous use, and it is useful if a regulatory inspection takes place.

Using this proven and assisted method based on the Purdue Model and using tools by Nozomi Networks and Forescout allows maritime organizations to discover, deal with, and prevent cyber threats in every device file, ensuring rules are followed and security improves [91], [92], [93], [94].

### 6.1.3 Vulnerability Assessment and Exploration

Assessing potential vulnerabilities in advance is necessary for current ships, as using both OT and IT systems in ship operations makes it hard to predict threats. As part of solving this, maritime organizations should arrange their vulnerability management processes using the Purdue model and rely on platforms like Nozomi Networks and Forescout to cover the whole network infrastructure [7], [94], [97].

**Nozomi Networks for OT Vulnerability Assessment (Purdue Levels 0–3)**

Nozomi Networks should be deployed on the OT parts of the ship's network, meaning Levels 0 to 3 of the Purdue Model that control physical elements and supervision. It identifies ship assets automatically, monitors them continuously, and finds anomalies in real time for systems like the propulsion link,

navigation sensors, and engine management units [7]. Tracking every OT asset with Nozomi Networks helps operators discover any old firmware, irregular system changes, and unusual network behaviour that might point to existing risks. Indeed, it might identify PLCs that aren't yet secured and uncommon data links between the automation and propulsion systems on vessels [7].

By being so visible, important problems can be dealt with quickly, and major risks can be lessened. Nozomi Networks fulfils the standards in IEC 62443-3-3 [98], [99] and NIST CSF 2.0, each of which demands strong management and protection of assets within industrial systems [99].

**Forescout for IT/OT Asset Compliance (Purdue Levels 3.5–5)**

The upper part of the Purdue Model, including the demilitarized zone (DMZ), business IT systems, and external network connections (Levels 3.5 to 5), can benefit from Forescout for asset compliance and policy enforcement. The platform brings together IT and OT monitoring, always ensuring that devices comply with security and regulatory requirements [94], [100]. Since Forescout can identify non-compliant devices, unauthorized crew or contractor laptops that try to enter OT networks are quickly separated, limiting where an attacker can move [23], [100]. Since Forescout strongly isolates IT and OT zones, the solution meets the DNV guidelines for continuous monitoring and splitting the network and the IMO's rules for safeguards on bridge, cargo handling, and propulsion systems [23], [100].

Making Nozomi Networks and Forescout part of a Purdue Model-based approach can improve maritime organizations' cyber defence. With this approach, any weaknesses in OT and IT are found quickly, and compliance with IEC 62443, NIST CSF 2.0, DNV, and IMO standards is maintained [23], [12], [100] [7], [94].

**Table 8 Recommended Tools and Security Functions by Purdue Layer** [85], [101], [102].

| Purdue Layer | Recommended Tool | Security Functions | Compliance Alignment |
|---|---|---|---|
| Levels 0–3 (OT) | Nozomi Networks | Asset discovery, anomaly detection, vulnerability management | IEC 62443, NIST CSF |
| Level 3.5 (DMZ) | Forescout | Segmentation enforcement, boundary protection | DNV, IMO, NIST CSF |
| Levels 4–5 (IT) | Forescout | Device compliance, policy monitoring, incident response | DNV, IMO, NIST CSF |

Table 8 outlines which security tools and security functions should be used at each layer of the Purdue Model. It finds suitable defences like firewalls, IDS/IPS, EDR, and network monitoring tools to address the needs in each group (e.g., Enterprise, Operations, Control, Field, and Process). The security functions related to the distinctions (access control, catching anomalies, log management) are indicated in the table for each layer. Using the Purdue Model, specific tools and functions can be shown in the table and

so the table acts as a reference for creating layered defences in maritime networks to protect from almost all cyber dangers.

### 6.1.4 Testing of Incident Detection and Response

Finding and reacting to incidents is very important in marine cybersecurity, helping to keep threats from jeopardizing boat or crew safety or performance. Because IT and OT systems are so closely linked on modern vessels, using advanced detection and response tools that give real-time vision over all networks is crucial. Applying Nozomi Networks and Forescout products is suggested in this section, using the Purdue Model, as the best way to enhance the cyber safety of ships.

**Nozomi Networks for OT Incident Detection and Response (Purdue Levels 0–3)**

Nozomi Networks should be put into action on the first four levels of the Purdue Model, where it provides ongoing monitoring, top-quality anomaly detection, and effective response to shipboard emergencies. AI-supported analytics are used within the platform to capture normal patterns of activity so that suspicious behaviour like command execution, sensor variations, or surprising communication is quickly flagged as potentially malicious [10], [11], [103]. If a threat is detected, Nozomi Networks can issue automatic alerts, cut off the risky assets, and offer steps to solve the problem. Leaving aside the topic of safety, if an improper message arrives at a propulsion PLC, the system can rapidly flag the incident, log the actions on the network, and suggest containment options to avoid additional complications. This way of operating meets the guidelines suggested by IEC 62443 and the NIST Cybersecurity Framework, both of which urge continuous observation, prompt detection, and fast action in industrial control companies [10], [103].

**Forescout for IT/OT and Cross-Domain Incident Response (Purdue Levels 3.5–5)**

In Layer 2.5 of the Purdue Model and above (DMZ, business IT systems, and external network connections), Forescout is advised as the main solution for noticing and dealing with incidents. Forescout connects different domains, so it can spot suspicious activity such as attempts at unauthorized access, movement between different systems, and policy rule breaks.

If an attack happens, such as a phishing threat attacking a workstation (Level 4) or an action to cross the IT/OT boundary, Forescout's tools automatically stop any affected devices, ensure no malicious packets are used, and save thorough logs for review. The system enables compliance with DNV cyber secure class notations, IMO recommendations on cyber safety, and the NIST CSF "Detect" and "Respond" abilities, each of which calls for fast recognition and handling of cyber dangers [66], [70], [104].

**Combined Action and Accurate Regulation**

When Nozomi Networks and Forescout work hand in hand, maritime companies can reliably detect and deal with incidents anywhere in the Purdue Model hierarchy. Thanks to this approach, both OT and IT networks are observed continually, dangers are discovered quickly, and any incidents are soon controlled. It further helps comply with common reporting methods, prepare for external audits, and be in step with the newest standardized maritime cybersecurity checks suggested by the IMCSO [105].

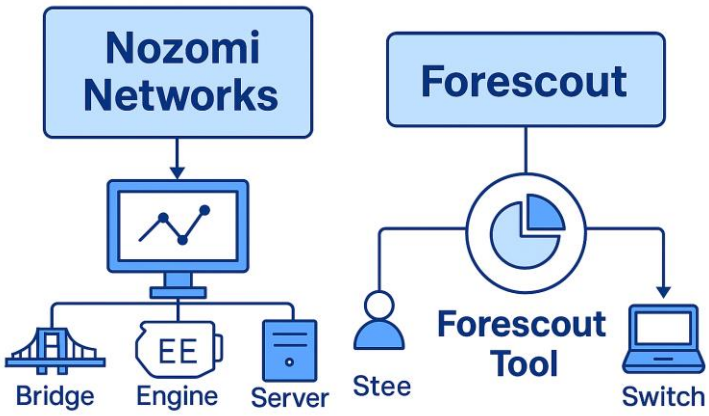


Figure 15: Nozomi Networks vs. Forescout Monitoring Architecture in a Maritime Environment.

Figure 15 demonstrates there are two sets of bars, each showing the deployment of monitoring solutions from Nozomi Networks and Forescout in the maritime industry. It discusses their role in seeing the ship's assets, discovering threats, and monitoring the network within both the IT and OT domains, which helps determine the right cybersecurity technology for vessels.

### 6.1.5 Enhancing the Ship Cyber Resilience Test Procedure

The ship cyber resilience test method matches IACS UR E26 4.2.2.4.3 and IEC 62443 and analyses the vessel's cybersecurity and ability to bounce back from cyber events [106], [107]. This procedure needs to be followed these steps:

**Step 1: Pre-Test Preparation**

- Marking out and specifying which key systems will be analysed, for example, navigation, motors, and communication equipment [107].
- Introduce and activate network-monitoring solutions (such as Nozomi Networks or Forescout), to create performance and security data baselines [94], [103].
- Ensure that true security staff are watching the testing and recording every incident or unusual activity.

**Step 2: Simulated Attack Scenarios**

- **Scenario 1: Phishing Attack Simulation**
  A phishing attack simulation is the example that will be used in this case. Simulate phishing emails to gauge crew's awareness and action toward these kinds of attacks [59].
- **Scenario 2: Malware Injection**
  In scenario two, malware is installed onto the device. Put isolated malicious software into a testing environment to see if the defences can detect and fix it [107].
  **Scenario 3: DDoS Attack Simulation (IT Layer Impact)**
  Checking how an attack on the DMZ firewall or VPN concentrator can prevent people from accessing or frequently updating the OT network controls. Core OT network segregation generally keeps things isolated, but IT-level disturbances can reduce visibility and diagnostics between the ship and the shore [107], [108].
- **Scenario 4: Unauthorized OT Access Attempt**
  Attempting to enter the OT environment without permission. Undertake unauthorized login procedures to OT systems to check how well the firewall and access controls are working [94].

**Step 3: Dealing with the Incident and Evaluation**

Note how quickly we can find problems, respond, and restore systems in every case [11]. Match outcomes with legal requirements and set standards to determine where additional improvements are required [107], [108] .

Updating the organization's security policies, technical measures, and safety training schedules after each test, according to the [59].

**Important Results from Security Testing**

Critical security updates were missed in the legacy OT systems, and because of this, the systems became more vulnerable to common dangers [106].

Many OT systems did not provide proper access controls, which made it easy for someone unauthorized to access the system [108]. There were problems with existing IDS configurations not being able to detect some smart attacks, showing that using advanced analytics is necessary [103].

The table below outlines the important security testing activities in maritime cybersecurity and gives the common tools used for each activity. Among the activities it includes are vulnerability scanning, penetration testing, examining system configurations, and exercise programs aimed at handling incidents. The table shows which tools (for instance, Nessus for scanning, Metasploit for penetration tests, and Wireshark for analysing data) are commonly used to manage and address risks in shipboard

networks. The table helps ensure security assessments are carried out in an organized way and proves the benefits of these steps for the lasting cyber protection of the maritime sector.

**Table 9 Security Testing Activities and Tools** [27], [87], [101].

| Testing Activity | Purdue Layer(s) | Recommended Tool(s) | Purpose/Outcome |
|---|---|---|---|
| Asset inventory & vulnerability scan | Levels 0–3 | Nozomi Networks | Identify OT assets and vulnerabilities |
| Segmentation validation | Level 3.5 (DMZ) | Forescout | Ensure OT/IT separation and firewall effectiveness |
| Policy enforcement & compliance check | Levels 4–5 | Forescout | Verify device compliance and access control |
| Incident detection & response drill | All layers | Nozomi & Forescout | Test alerting, isolation, and response procedures |

### 6.1.6 Ship's Cyber Resilience Evaluation

In the assessment, the ship's ability to stay stable and be restored after being attacked by cyber threats was evaluated thoroughly. The team brought together outcomes from network testing, vulnerability assessments, and incident response practices, giving everyone a clear picture of the vessel's cybersecurity status [102].

**Resilience Metrics**

• **Time to Detection:** The amount of time it takes monitoring systems to see when a threat occurs [103].

• **Response time:** The period it takes to begin and complete actions to handle an incident [94].

• **Restoring time**: Maintaining essential equipment and keeping systems working during and after designed simulated cyberattacks against navigation and propulsion [107].

**Recommendations for Improvement**

**Automated Patch Management:**

To promptly remove malicious threats, keep installing updates on OT equipment whenever they are due and no longer depend on staff to remember [105].

**Enhanced Role-Based Access Control:**

Only allow people who need it access to the main systems by setting permissions very strictly. Detecting and analysing difficult threats is the focus of these analytics.

**Advanced Threat Detection Analytics:**

Bring in AI SIEM solutions to improve how the organization spots the latest and most advanced security threats [71].

**Routine Crew Cybersecurity Drills:**

As advised by the IMO in 2021, routinely train shipboard employees on how to handle phishing and other cyberattacks [59].

The assessment has discovered what a ship does well in cybersecurity and where it can improve. If a ship takes these recommendations, it can more actively safeguard its cybersecurity and become aligned with leading maritime cybersecurity rules and regulations.

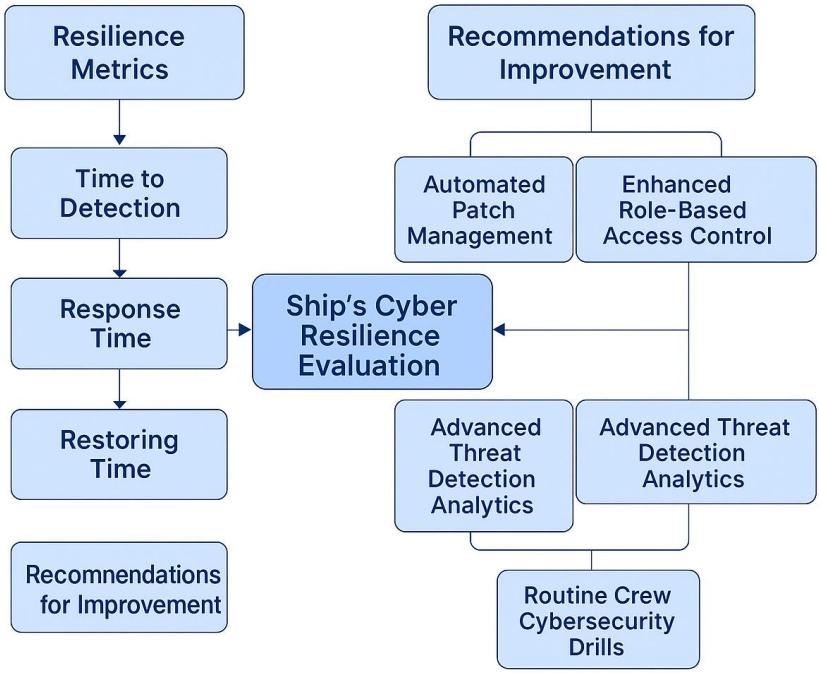


Figure 16: Ship's Cyber Resilience Evaluation: Metrics and Improvement Pathways.

This figure sums up how a ship's cyber resilience is checked by looking at key indicator values and recommends future enhancements. It uses the assessment outcomes to mark areas of concern, provides ways to address them, and guides on measures to improve the ship's ability to deal with cyber incidents. As Nozomi Networks and Forescout are widely trusted in the maritime sector, we should not overlook the fact that cybersecurity developments are evolving fast. ShipNerdNews reports that companies use Darktrace and Marlink, which add another level of security and support using artificial intelligence and managed services [71], [109]. Deploying these tools gives further security advantages in challenging or risky operational settings.

For their cybersecurity, maritime organizations can use the Purdue Model and rely on tools such as Nozomi Networks and Forescout to get complete and instant monitoring and control across all network levels. With the addition of AI-based detection or managed security offerings, security will be more elastic to new threats, and the business will keep meeting compliance and resilience standards worldwide.

# 7 Discussion and Recommendations

In 2025, cybersecurity threats to the maritime industry are expected to grow a lot because ships are now more digital and connected with AI, IoT, and remote management systems. Changes such as digitization may allow operations to be better coordinated, but they have unfortunately exposed ports and their vessels to more cyber risks, among them ransomware, malware, fake GPS, and being accessed without permission [110], [111], [112].

Cyber threats against both OT and IT systems installed on ships and in ports have been increasing lately. As a result of such attacks, there have been disruptive incidents, big financial losses, and sea safety being affected. Especially, outdated systems, weak IoT devices, and older software make air, sea, and land travel routes easy targets for hackers [111], [112].

Groups such as the International Maritime Organization (IMO) have moved to raise cybersecurity standards, ensuring that organisations in the maritime industry manage cyber risks in their Safety Management Systems (SMS) in line with MSC.428(98) [110], [112], [113] guidelines. But it remains challenging for many smaller companies to comply, so these operators have difficulty in following all the requirements and are still exposed to various dangers [110], [113].

The industry is now applying more than one approach to deal with these problems. They should use zero trust security approaches as well as deploy intrusion detection systems, firewalls, and security programs on each computer, and rely on AI-based tools for fast alerting. Belongings to ensure effective cybersecurity, crew training is carried out on schedule, vulnerabilities are regularly monitored, and shipping companies obey best-practice guidelines such as those created by BIMCO [113].

Still, with new risks appearing, it is important to adapt all the time. It has become clear that we need to address these new threats and keep cybersecurity investments high by using expert advice to follow the protections in the relevant laws [110], [111], [112].

## 7.1 Contributions to Maritime Cybersecurity

This thesis introduces several important ideas to maritime cybersecurity:

It first introduces current problems in maritime cybersecurity, explains key vulnerabilities, and outlines useful best practices, especially for those who may not have accessible practical advice [111], [114].

Next, the study presents a practical method for applying the Purdue Model to protect both OT and IT systems, using examples from Nozomi Networks and Forescout [111], [115] .

The thesis goes on to highlight that human factors are key to achieving cyber resilience. Analysis of the devices, risk training, and simulated incident response points to the lasting risk of human error and the value of continual training [111], [116]. Furthermore, it defines a planned procedure for evaluating ships' cyber resilience by means of scenarios, based on IACS UR E26, IEC 62443, and NIST CSF. The

research on Ship clearly illustrated that the steps discussed can be used by other organizations in practical ways [111], [115].

The thesis serves as a link between academic research and industry practices, combining empirical data, required guidelines, and suggestions for practical action, to further develop complete systems for maritime cybersecurity risk assessment and management [111], [117] [118].

## 7.2 Recommendations

The studies and research examined here prompt me to advance these recommendations to promote better cyber resilience at sea:

**Adopt a Layered Cybersecurity Architecture:**

Cybersecurity programs in maritime firms must be built on the Purdue Model which supports dividing OT and IT networks logically and layered protection [89], [119].

**Deploy Advanced Monitoring and Detection Tools:**

For OT, use Nozomi Networks, and for IT/OT, use Forescout. They offer instant visibility of assets, alert users when suspicious activity happens, and automatically implement cybersecurity policies needed for quickly spotting and dealing with cyber threats [7], [94].

**Integrate Emerging Technologies and Managed Services:**

Because Nozomi Networks and Forescout are commonly used, the ongoing developments in cybersecurity technology must not go unnoticed. Darktrace, which relies on AI to spot threats, and Marlink, which provides managed security services, add more levels of security and help with operations Applying these solutions can make a vessel safer, mainly when situations become complex or difficult.

**Strengthen Crew Training and Awareness:**

People are still a big target for threats. It is necessary for all crew to receive standard training in cyber safety, phishing awareness, and how to handle cyber incidents. When students and organizations are educated, the odds of a successful cyberattack are sharply reduced [87], [111].

**Conduct Regular Risk Assessments and Drills:**

Monitoring risks, running vulnerability scans, and practicing simulated incident responses should be regular parts of a ship's work. Because of this, weaknesses are spotted early and handled right away, and the team is ready to handle real emergencies [110], [112].

**Align with Evolving Regulations and Best Practices:** Following regulations such as MSC.428(98), ISO/IEC 27001, and NIS2 is very important. Shipping companies must update their cybersecurity plans as regulations keep changing [110], [112] .

# 8 Conclusion

The thesis has discussed the rapidly evolving subject of maritime cybersecurity, with a focus on what distinguishes maritime cybersecurity from other types and what needs to be secured. The research indicates that maritime cyber risks include technical, human, and organizational aspects. It is obvious from examining standards, risk frameworks, and practical testing that the maritime sector should use an overall, multiple-layer strategy to stay cyber resilient.

Research demonstrates that technical features in the industry, such as GPS, the Internet of Things, and remote management, are very useful for operations, but also add more opportunities for attacks Cases of ransomware, phishing, and unauthorized access indicate the risk ships face for disruptions, financial damage, and serious dangers on the water.

The research confirms that the Purdue Model works well as a network protection tool. Proper cybersecurity in maritime relies on adding Nozomi Networks and Forescout tools, resilience test simulations, and ongoing crew education. It is important for resilience and staying up to date with regulations to align with the IMO, IEC 62443, and ISO/IEC 27001 guidelines. This research set out to address several key objectives related to maritime cybersecurity resilience. The following points summarize how each objective was met and the outcomes achieved.

**Designing Secure Ship Security Zones**

The study successfully established a framework for segmenting shipboard networks into secure zones, isolating critical operational technology (OT) systems such as navigation and propulsion from administrative IT networks. This approach, informed by industry standards and best practices, significantly reduced the risk of cyber incidents propagating across the vessel's digital infrastructure. The use of firewalls, access controls, and monitoring points ensured that each zone had tailored security measures appropriate to its operational importance and risk profile, mission security.

**Implementing Network Protection Safeguards**

Main network security measures were deployed, covering advanced monitoring tools (for example, Nozomi Networks and Forescout), intrusion detection and prevention systems, and solutions for endpoint detection and response. Because of these safeguards, the system quickly spotted and solved network issues related to cyber threats. Once these tools were linked to shipboard systems, they showed they stop unauthorized access and lessen the effects of cyber threats.

**Developing a Ship Cyber Resilience Test Procedure**

A thorough procedure for evaluating cyber resilience was constructed and used by simulating different kinds of attacks. They examined how the vessel could spot, deal with, and recover from dangers including ransomware, phishing and unauthorized access. The study demonstrated that checking and testing security efforts frequently and continually training the crew are both necessary.

**Proposing Recommendations for Continuous Improvement**

The research gave practical steps to strengthen and preserve cyber resilience going forward. This meant providing workers with ongoing cybersecurity information, keeping systems updated, patching them regularly, and always monitoring and reporting on possible threats. By following IMO, IEC 62443, and ISO/IEC 27001, the proposed measures were shown to be practical and meet current requirements across the industry.

Through completing each research objective, this work has offered practical ideas and strong recommendations for better maritime cyber defence. The results show that focusing on different forms of defence, training crew, and obeying global regulations can better protect a ship's systems from increasing risks of cyberattacks.

## 8.1 Outlook and Future Work

Advances in technology will lead to the maritime industry encountering new and harder cyber threats. Future studies must address using AI and machine learning for way-ahead threat analysis, adopting blockchain for secure exchange, and building quantum-resistant security codes [120]. Progress in maritime cyber resilience will depend on cooperation among the industry, the rules enforcers, and educational institutions. Future studies ought to deal with these areas, expanding on now existing approaches and novel technological breakthroughs:

1. **Maritime ecosystems are investigated across a wide range of ecosystems**

   Examining cybersecurity strategies from all kinds of maritime organizations may reveal what to do right and where weaknesses lie. An example is looking at the results achieved by applying risk management frameworks like IACS UR E26/E27 or NIST CSF 2.0 in different forms of shipping, like autonomous systems versus their traditional counterparts [121]. This research can be improved by using case studies such as the International SMART Ship Project, which shows how technology standardization improves both navigation and resistance to threats. According to the journal [27], authors argue that using both advanced, component-specific and overall cybersecurity solutions is needed in the maritime sector.

2. **Modeling Threats with Data that is Always Up to Date**

   Studies should now put greater emphasis on using up-to-date maritime data from AIS feeds, VSAT, and engine control systems in threat models. The scenarios tested in Multi-Agent Reinforcement Learning (MARL) could help develop algorithms that predict situations such as attackers spoofing crew GPS or ransomware on crew ECDIS displays [27]. If models were dynamic, ships could decide on their security posture according to their surroundings, for instance, where they travel or the type of goods on board. Evaluations of the DLTIF framework (Deep Learning Threat Identification

Framework) in revealed that it can perform better than traditional methods in discovering cyber threats by using dynamic AI-based modelling [27].

**3. Studying how people in organizations work and the culture they build**

Because most cyber incidents happen due to human error, studies are needed on how well crews are trained, how they behave, and how organizations are managed properly. As an illustration, researchers may consider how IMO-endorsed cyber risk tools are advantageous in Safety Management Systems (SMS) [121] or check the guidelines in BIMCO's paper on cybersecurity on ships. Looking at bridge team studies in cyber incident tests, Wärtsilä and Carnival Corporation [122] discovered that by being transparent and grouping together, crews were able to respond faster. By joining forces with Singapore institutions, the Estonian Maritime Academy demonstrates how teams can be made more cybersecurity-aware on ships and ashore [123].

**4. Using AI, machine monitoring, and automating responses**

Applying research on AI to Security Information and Event Management (SIEM) systems could transform how real-time threats in OT/IT networks are detected. When adaptive incremental passive-aggressive machine learning (AI-PAML) [27] is added to radar (RADAR) or voyage data recorders (VDR), it could help a vessel avoid zero-day exploits without the need for human intervention. In addition, blockchain, which is suggested for digital records of ships [121] could be introduced with AI to secure information and better control its use. Dual Stack Machine Learning (S2ML), built on entropy analysis of network traffic, has been successful in marking down Distributed Denial-of-Service (DDoS) attacks, a big danger for ship-to-shore communication.

**5. Regulatory and Supply Chain Collaboration**

The maritime sector's reliance on global supply chains necessitates studies on enforcing cybersecurity standards among third-party vendors. Initiatives like the EU's NIS Directive and INTERPOL's Operation 404 [27] highlight the importance of cross-border cooperation. Future research could evaluate the scalability of platforms like Information Sharing and Analysis Centers (ISACs) [114], which aggregates threat intelligence across stakeholders, or assess the impact of IACS UR E26/E27 [124] on reducing vulnerabilities in newly constructed vessels. The Maritime and Port Authority of Singapore's work with TalTech [125] highlights how R&D projects and testbeds together create new solutions that meet cybersecurity regulations

A holistic approach to maritime cyber resilience requires integrating technical advancements (e.g., AI, blockchain) with human-centric strategies (e.g., training, organizational governance) and robust regulatory frameworks. By addressing these interdisciplinary priorities, future research can mitigate evolving threats such as GPS jamming, ransomware, and supply chain compromises, ensuring the security of global maritime operations.

# References


[1] E. Erstad, R. Hopcraft, H. A. Vineetha, and K. Tam, "A human-centred design approach for the development and conducting of maritime cyber resilience training," *WMU Journal of Maritime Affairs*, vol. 0, no. 0, pp. 241–266, Mar. 2023, doi: 10.1007/S13437-023-00304-7.

[2] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *Networks*, vol. 2, no. 1, pp. 123–138, 2022, doi: 10.3390/network2010009.

[3] J. F. Carias, L. Labaka, J. M. Sarriegi, and J. Hernantes, "An approach to the modeling of cyber resilience management," *in Proceedings of the Global Internet of Things Summit (GIoTS), Nov. 2018*, Nov. 2018, doi: 10.1109/GIOTS.2018.8534579.

[4] I. N. Putra, A. Octavian, A. K. Susilo, and Y. N. Santosa, "An Assessment of Cyber Resilience in the Maritime Domain Using System Dynamics and Analytical Hierarchy Process (AHP)," *Transactions on Maritime Science*, vol. 13, no. 2, Jun. 2024, doi: 10.7225/TOMS.V13.N02.W06.

[5] C. Park, C. Kontovas, Z. Yang, and C. H. Chang, "A BN driven FMEA approach to assess maritime cybersecurity risks," *Ocean and Coastal Management, vol. 235, Mar. 2023*, doi: 10.1016/J.OCECOAMAN.2023.106480.

[6] 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, Oct. 2020*, no. 10, doi: 10.3390/JMSE8100768.

[7] Nozomi Networks, "Maritime Cybersecurity." Accessed: Jun. 08, 2025. [Online]. Available: https://www.nozominetworks.com/industries/maritime-cybersecurity

[8] Forescout, "IT/ OT Convergence: Come for OT, Leave with TO (takeout)." Accessed: Jun. 10, 2025. [Online]. Available: https://resources.forescout.com/ot_and_to_virtual_borderless.html

[9] Gartner, "Best Operational Technology Security Reviews 2025 | Gartner Peer Insights." Accessed: Jun. 10, 2025. [Online]. Available: https://www.gartner.com/reviews/market/operational-technology-security

[10] Nozomi Networks, "OT Security Best Practice Guide." Accessed: Jun. 09, 2025. [Online]. Available: https://www.nozominetworks.com/blog/ot-security-best-practices

[11] Nozomi Networks, "Industrial Cyber Threat Detection & Response." Accessed: Jun. 09, 2025. [Online]. Available: https://www.nozominetworks.com/solutions/threat-detection-and-response

[12] Industrial Cyber, "New Forescout platform offers maritime operators device visibility, advanced threat detection." Accessed: Jun. 09, 2025. [Online]. Available: https://industrialcyber.co/news/new-forescout-platform-offers-maritime-operators-device-visibility-advanced-threat-detection/

[13] Darktrace, “Revolutionizing OT Risk Prioritization with Darktrace 6.3.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.darktrace.com/blog/revolutionizing-ot-risk-prioritization-with-darktrace-6-3

[14] Cisco, “Cisco Secure Network Analytics (formerly Stealth watch) At-a-Glance.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/secure-network-analytics-aag.html

[15] Manage Engine, “Palo Alto Log Analyzer | Palo Alto Firewall Monitoring - ManageEngine Firewall Analyzer.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.manageengine.com/products/firewall/palo-alto-firewall-log-analyzer.html

[16] Nozomi Networks, “Maritime Cybersecurity.” Accessed: May 24, 2025. [Online]. Available: https://cdn.prod.website-files.com/645a4534705010e2cb244f50/64911703c1eb2dea69ae9ea2_Nozomi-Networks-Maritime-Solution-Brief.pdf

[17] Forescout, “Enhances Cyber Resilience for the Maritime Industry.” Accessed: May 23, 2025. [Online]. Available: https://www.forescout.com/press-releases/forescout-enhances-cyber-resilience-for-the-maritime-industry/

[18] IBM, “QRadar.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.ibm.com/qradar

[19] Splunk, “Splunk Attack Analyzer.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.splunk.com/en_us/products/attack-analyzer.html

[20] Elastic, “Elastic Security Solution.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.elastic.co/security

[21] Nozomi Networks, “The Latest OT/IoT Cybersecurity Threat Landscape – 2H 2024 Review.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.nozominetworks.com/resources/ot-iot-cybersecurity-threat-landscape-2h-2024-review

[22] Claroty, “ICS Security:The Purdue Model.” Accessed: Jun. 09, 2025. [Online]. Available: https://claroty.com/blog/ics-security-the-purdue-model

[23] S. Stoynov and B. Nikolov, “Approach to Ship’s IT and OT Systems Cybersecurity Improvement,” *Pedagogika-Pedagogy*, vol. 93, no. 7s, pp. 185–196, Aug. 2021, doi: 10.53656/PED21-7S.16APPR.

[24] A. Dimakopoulou and K. Rantos, “Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0,” *Journal of Marine Science and Engineering 2024, Vol. 12, Page 919*, vol. 12, no. 6, p. 919, May 2024, doi: 10.3390/JMSE12060919.

[25] DNV, “Maritime cyber security services and solutions.” Accessed: Jun. 08, 2025. [Online]. Available: https://www.dnv.com/services/maritime-cyber-security-services-and-solutions-73927/

[26] DNV, “Ensuring cyber-secure vessel designs and supply.” Accessed: Jun. 08, 2025. [Online]. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/yards/

[27] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, “Maritime Cybersecurity: A Comprehensive Review,” Sep. 2024, doi: 10.48550/ARXIV.2409.11417.

[28] N. Berg, J. Storgård, and J. Lappalainen, “The Impact of Ship Crews on Maritime Safety. Turku, Finland: Turun Yliopiston merenkulkualan koulutus- ja tutkimuskeskuksen julkaisuja, 2013.” Accessed: Jun. 08, 2025. [Online]. Available: https://mkkdok.utu.fi/pub/A64-impact of crews on safety.pdf

[29] X. Shi, H. Zhuang, and D. Xu, “Structured survey of human factor-related maritime accident research,” *Ocean Engineering*, vol. 237, p. 109561, Oct. 2021, doi: 10.1016/J.OCEANENG.2021.109561.

[30] G. Di Bucchianico, A. Vallicelli, N. A. Stanton, and S. J. Landry, “Human factors in transportation: Social and technological evolution across maritime, road, rail, and aviation domains,” *Boca Raton, FL, USA: CRC Press, 2016*, pp. 1–452, Sep. 2016, doi: 10.1201/9781315370460.

[31] IACS, “IACS Unified Requirement E26, 2022.” Accessed: May 15, 2025. [Online]. Available: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

[32] IACS, “IACS Unified Requirement E27, 2022.” Accessed: May 15, 2025. [Online]. Available: /https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e27_rev.1_sep_2023_cln.pdf

[33] IMO, “Guide to Maritime Security and the ISPS Code.” Accessed: Jun. 09, 2025. [Online]. Available: https://seatracker.ru/viewtopic.php?t=49861

[34] N. P. H. Adams, R. J. Chisnall, C. Pickering, and S. Schauer, “How port security has to evolve to address the cyber-physical security threat: Lessons from the sauron project,” *International Journal of Transport Development and Integration*, vol. 4, no. 1, pp. 29–41, 2020, doi: 10.2495/TDI-V4-N1-29-41.

[35] C. Kapalidis, S. Karamperidis, T. Watson, and G. Koligiannis, “A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships,” *Journal of Marine Science and Engineering, vol. 10, no. 10, Oct. 2022*, doi: 10.3390/JMSE10101486.

[36] I. Progoulakis, N. Nikitakos, D. Dalaklis, A. Christodoulou, A. Dalaklis, and R. Yaacob, “Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure,” pp. 227–248, 2023, doi: 10.1007/978-3-031-25296-9_12.

[37] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, “Cyber Physical Systems Security for Maritime Assets,” *Journal of Marine Science and Engineering 2021, Vol. 9, Page 1384*, vol. 9, no. 12, p. 1384, Dec. 2021, doi: 10.3390/JMSE9121384.

[38] K. Christopher, “Port Security Management,” *Port Security Management*, Mar. 2009, doi: 10.1201/9781420068931.

[39] V. Wendler-Bosco and C. Nicholson, “Port disruption impact on the maritime supply chain: a literature review,” *Sustainable and Resilient Infrastructure, vol. 5, no. 6, pp. 378–394, Nov. 2020*, doi: 10.1080/23789689.2019.1600961.

[40] Y. C. Yang, “Risk management of Taiwan’s maritime supply chain security,” *Safety Science, vol. 49, no. 3, pp. 382–393, Mar. 2011*, doi: 10.1016/J.SSCI.2010.09.019.

[41] A. H. Becker *et al.*, “A note on climate change adaptation for seaports: A challenge for global ports, a challenge for global society,” *Climatic Change, vol. 120, no. 4, pp. 683–695, Oct. 2013*, doi: 10.1007/S10584-013-0843-Z.

[42] UNCTAD, “Review of maritime transport 2022.” Accessed: Jun. 09, 2025. [Online]. Available: https://unctad.org/system/files/official-document/rmt2022_en.pdf

[43] IACS, “IACS Unified Requirement E22, 2022.” Accessed: May 15, 2025. [Online]. Available: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf

[44] IACS, “Rec 166 New Corr2 CLN - Safer and Cleaner Shipping.” Accessed: Jun. 09, 2025. [Online]. Available: https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new-corr2-cln

[45] The Maritime Executive, “Hackers Steal from Cyprus Shipping Company.” Accessed: Jun. 09, 2025. [Online]. Available: https://maritime-executive.com/article/hackers-steal-from-cyprus-shipping-company

[46] BBC, “North Korea ‘jamming GPS signals’ near South border.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.bbc.com/news/world-asia-35940542

[47] Security Week, “Attackers Exploit Flaw in Software Used by US Ports.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.securityweek.com/attackers-exploit-flaw-software-used-us-ports/

[48] Resilient Navigation and timing Foundation, “Hackers took ‘full control’ of container ship’s navigation systems for 10 hours.” Accessed: Jun. 09, 2025. [Online]. Available: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/

[49] GPS World, “Spoofing in the Black Sea: What really happened?” Accessed: Jun. 09, 2025. [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

[50] Incibe, “The Port of Barcelona suffers a cyber attack.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/port-barcelona-suffers-cyber-attack

[51] The Guardian, “Defence shipbuilder Austal hit with data breach and extortion attempt.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.theguardian.com/technology/2018/nov/02/defence-shipbuilder-austal-hit-with-data-breach-and-extortion-attempt

[52] Latent Spaces - Performing Ambiguous Data, “Shanghai Signal Spoofing in Maritime Traffic (2019).” Accessed: Jun. 09, 2025. [Online]. Available: https://latentspaces.zhdk.ch/unrealdata/shanghai-signal-spoofing-in-maritime-traffic

[53] Insurance Business, “James Fisher and Sons hit by cyber breach.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.insurancebusinessmag.com/uk/news/marine/james-fisher-and-sons-hit-by-cyber-breach-190689.aspx

[54] SkyTruth, “Systematic data analysis reveals false vessel tracks.” Accessed: Jun. 09, 2025. [Online]. Available: https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/

[55] iSite Computers, “Ransomware Attacks in South Africa: What You Need to Know,” *https://isite.co.za/*, Accessed: Jun. 09, 2025. [Online]. Available: https://isite.co.za/ransomware-attacks-south-africa/

[56] Bleeping Computer, “LockBit ransomware claims attack on Port of Lisbon in Portugal.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-claims-attack-on-port-of-lisbon-in-portugal/

[57] DP World, “Media Statement: Update on Cybersecurity Incident.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.dpworld.com/australia/news/releases/media-statement-update-on-cybersecurity-incident/

[58] The Business Times, “A ransomware attack hit a vendor to DBS. What is a ransomware attack and how does it affect companies?” Accessed: Jun. 09, 2025. [Online]. Available: https://www.businesstimes.com.sg/startups-tech/technology/ransomware-attack-hit-vendor-dbs-what-ransomware-attack-and-how-does-it-affect-companies

[59] IMO, “Maritime cyber risk.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[60] K. Tam and K. Jones, “Cyber-Risk Assessment for Autonomous Ships,” *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, Dec. 2018, doi: 10.1109/CYBERSECPODS.2018.8560690.

[61] A. Hakim, N. Aini, and M. R. Khan, “Firewalls, intrusion detection/prevention, encryption, and multi-factor authentication in cybersecurity solutions,” *Cybersecurity solutions*, pp. 6–8, Jul. 2024, doi: 10.1177/1460458217706184<SPAN.

[62] DNV, “Maritime Cyber Security Regulations.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/

[63] Tenfold, “Role-based Access Control in Active Directory.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.tenfold-security.com/en/rbac-role-based-access-control/

[64] Corma, “Leveraging Active Directory for Role-Based Access Control.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.corma.io/blog/leveraging-the-active-directory-for-effective-role-based-access-control

[65] Delinea, “Role Based Access Control Active Directory.” Accessed: Jun. 09, 2025. [Online]. Available: https://delinea.com/products/secret-server/features/role-based-access-control-rbac

[66] Finnish Shipowners’ Association, “Maritime cybersecurity—best practices for vessels.” Accessed: May 19, 2025. [Online]. Available: https://shipowners.fi/wp-content/uploads/2021/09/Maritime-Cyber-Security-–-Best-Practices-for-Vessels.pdf

[67] ThreatSpan Ltd., “ThreatScene MARINE Cyber Security Framework v1.0 – RELEASE 1.0.” Accessed: May 19, 2025. [Online]. Available: https://nee.gr/wp-content/uploads/2024/11/ThreatScene-MARINE-Framework-v1.0-RELEASE-1.pdf

[68] Fortinet, “IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/iec-62443

[69] ClassNK (Nippon Kaiji Kyokai), “Guidelines for Cyber Resilience of Ships.” Accessed: May 19, 2025. [Online]. Available: https://www.classnk.or.jp/hp/pdf/activities/cybersecurity/gl_CyberResilienceofShips_202407e.pdf

[70] Virtuemarine, “Top Cybersecurity Strategies for Maritime Operations.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.virtuemarine.nl/post/top-cybersecurity-strategies-for-maritime-operations

[71] DARKTRACE, “Cybersecurity for Maritime: Definition & Examples.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.darktrace.com/cyber-ai-glossary/cybersecurity-in-maritime

[72] Hartmann Bros Marine Service, “Implementing Multi-Factor Authentication (MFA) in a Vessel: Enhancing Maritime Cybersecurity.” Accessed: Jun. 11, 2025. [Online]. Available: https://hbmsusa.com/article/implementing-multi-factor-authentication-mfa-vessel-enhancing-maritime-cybersecurity

[73] Threat Span Ltd., “MARINE Cyber Security Framework v1.0.” Accessed: Jun. 09, 2025. [Online]. Available: https://nee.gr/wp-content/uploads/2024/11/ThreatScene-MARINE-Framework-v1.0-RELEASE-1.pdf

[74] Hartmann Bros Marine Service, “Enhanced Maritime Cybersecurity: Implementing Multi-Factor Authentication in Compliance with IACS E26/E27.” Accessed: Jun. 11, 2025. [Online]. Available: https://hbmsusa.com/article/enhanced-maritime-cybersecurity-implementing-multi-factor-authentication-compliance-iacs

[75] ABS, “Cybersecurity Implementation for the Marine and Offshore Industries.” Accessed: Jun. 11, 2025. [Online]. Available: https://ww2.eagle.org/content/dam/eagle/publications/cutsheets/

[76] BIMCO, “About BIMCO.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.bimco.org/about-bimco/

[77] DNV, “DNV Annual Report 2024.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.dnv.com/annualreport/

[78] GlobalSpec, “ABS - 251 - Guide for cybersecurity implementation for the marine and offshore industries volume 2.” Accessed: Jun. 09, 2025. [Online]. Available: https://standards.globalspec.com/std/14364455/251

[79] DRAGOS, “Incident Response for Operational Technology (OT).” Accessed: Jun. 09, 2025. [Online]. Available: https://www.dragos.com/resources/whitepaper/incident-response-for-operational-technology-ot/

[80] Mats Nordin, “Implementing a monitoring system using PRTG.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/504829/Nordin_Mats.pdf?sequence=2

[81] Cyberreason, “A Guide to Post-Incident Review.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.cybereason.com/resources/post-incident-review

[82] Nozomi Networks, “Guide to Maritime Cybersecurity.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.nozominetworks.com/blog/improving-maritime-cybersecurity-and-operational-resiliency

[83] Z.-X. Wu, S. Rind, Y.-H. Yu, and S.-J. Cho, “The development of a ship’s network monitoring system using SNMP based on standard IEC 61162-460,” *Journal of the Korean Society of Marine Engineering*, vol. 40, no. 10, pp. 906–915, Dec. 2016, doi: 10.5916/JKOSME.2016.40.10.906.

[84] Compliance Hub, “Navigating Compliance: A Practical Guide to the New Maritime Cybersecurity Regulations.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.compliancehub.wiki/navigating-compliance-a-practical-guide-to-the-new-maritime-cybersecurity-regulations/

[85] T. J. Williams, “The Purdue enterprise reference architecture,” *Computers in Industry, vol. 24, no. 2–3, pp. 141–158, Sep. 1994*, doi: 10.1016/0166-3615(94)90017-5.

[86] IMarEST, “Maritime cybersecurity – Proceedings of the International Ship Control Systems.” Accessed: Jun. 09, 2025. [Online]. Available: https://library.imarest.org/record/10734/files/10734.pdf

[87] David Garton, “US Department of Energy. Purdue Model Framework for Industrial Control Systems.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf

[88] N. Pajunen, “Overview of Maritime Cybersecurity,” 2017, Accessed: Jun. 09, 2025. [Online]. Available: http://www.theseus.fi/handle/10024/123045

[89] A. Trent, “Compliance Analysis of Cyber Security Standards.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.utupub.fi/bitstream/10024/175703/1/Trent_Amir_Compliance_Analysis_of_Cyber_Security_Standards.pdf

[90] Zscaler, “What Is the Purdue Model for ICS Security?” Accessed: Jun. 09, 2025. [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

[91] Palo Alto Networks, “What Is the Purdue Model for ICS Security? | A Guide to PERA.” Accessed: May 22, 2025. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-the-purdue-model-for-ics-security

[92] Fortinet, “What Is the Purdue Model for ICS Security?” Accessed: Jun. 09, 2025. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/purdue-model

[93] Mission Secure, “Maritime Cyber Security: A Comprehensive Approach.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach

[94] Nozomi Networks, “Securing the Digital Port: USCG Cybersecurity Compliance for U.S. Maritime Port Operators.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.nozominetworks.com/blog/securing-the-digital-port-uscg-cybersecurity-compliance-for-u-s-maritime-port-operators

[95] Forescout, “Forescout Enhances Cyber Resilience for the Maritime Industry.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.forescout.com/press-releases/forescout-enhances-cyber-resilience-for-the-maritime-industry/

[96] Turku University of Applied Sciences, “ARPA – Applied Research Platform for Autonomous Systems.” Accessed: Jun. 13, 2025. [Online]. Available: https://www.turkuamk.fi/en/project/arpa-applied-research-platform-for-autonomous-systems/

[97] Mission Secure, “A Comprehensive Guide to Maritime Cybersecurity.” Accessed: Jun. 09, 2025. [Online]. Available: http://www.missionsecure.com/hubfs/Assets/eBooks/A Comprehensive Guide to Maritime Cybersecurity_Final.pdf

[98] Nozomi Networks, “Maritime Cybersecurity Brief.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.nozominetworks.com/resources/maritime-cybersecurity-solution-brief

[99] UpGuard, “What is IEC/ISA 62443-3-3:2013? Cybersecurity & Compliance.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.upguard.com/blog/isa-62443-3-3-2013

[100] Cisco, “Products - ISA/IEC-62443-3-3: What is it and how to comply?” Accessed: Jun. 09, 2025. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html

[101] DNV, “Maritime cyber security - Safeguarding ships & operations.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/

[102] Fortinet, “A Solution Guide to Operational Technology Cybersecurity.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-solution-guide-to-ot-cybersecurity.pdf

[103] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” Feb. 2024, doi: 10.6028/NIST.CSWP.29.

[104] Thales Group, “Thales teams with Nozomi Networks to expand cyber incident detection capabilities on industrial infrastructure.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.thalesgroup.com/en/worldwide/security/press_release/thales-teams-nozomi-networks-expand-cyber-incident-detection

[105] ICS, “Cyber Security Onboard Ships - ICS Guidelines.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

[106] Industrial Cyber, “IMCSO issues cybersecurity assessment methodology for maritime vessel joining cyber risk registry.” Accessed: Jun. 09, 2025. [Online]. Available: https://industrialcyber.co/risk-management/imcso-issues-cybersecurity-assessment-methodology-for-maritime-vessel-joining-cyber-risk-registry/

[107] IEC, “IEC 62443-4-1:2018.” Accessed: Jun. 09, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/33615

[108] IACS, “UR E26 New - Withdrawn - Safer and Cleaner Shipping.” Accessed: Jun. 09, 2025. [Online]. Available: https://iacs.org.uk/resolutions/ur-e/ur-e26-new/ur-e26-new

[109] NIST, “NIST, Guide to Industrial Control Systems (ICS) Security.” Accessed: Jun. 09, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

[110] DRYAD GLOBAL, “Cybersecurity Threats in Maritime for 2025.” Accessed: Jun. 11, 2025. [Online]. Available: https://channel16.dryadglobal.com/cybersecurity-threats-in-maritime-for-2025

[111] Ship Nerd News, “Maritime Cybersecurity: The Most Sensible Solutions In 2025.” Accessed: Jun. 09, 2025. [Online]. Available: https://shipnerdnews.com/maritime-cybersecurity-most-sensible-solutions/

[112] LinkedIn, “(21) Maritime Security in 2025: Navigating the Evolving Landscape.” Accessed: Jun. 11, 2025. [Online]. Available: https://www.linkedin.com/pulse/maritime-security-2025-navigating-evolving-cphre/

[113] Ship Universe, “2025 Maritime Cybersecurity Regulations: A Simplified Breakdown.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.shipuniverse.com/2025-maritime-cybersecurity-regulations-a-simplified-breakdown/

[114] EY - Global, “5 Measures to Improve Cybersecurity in the Maritime Sector.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.ey.com/en_pl/insights/cybersecurity/5-measures-to-improve-cybersecurity-in-the-maritime-sector

[115] R. Peura, “Maritime Cybersecurity and Improvement of Project Execution Process,” *M.Sc. thesis, Tampere University of Technology, Dec. 2017*, Dec. 2017, Accessed: May 25, 2025. [Online]. Available: https://trepo.tuni.fi/handle/123456789/25339

[116] A. G. Kwadwo Forson, “Assessing maritime cyber security awareness in navies of the Gulf of Guinea countries, M.Sc. dissertation, World Maritime University.” Accessed: Jun. 09, 2025. [Online]. Available: https://commons.wmu.se/cgi/viewcontent.cgi?article=3060&context=all_dissertations

[117] C. Park, “Cybersecurity risk assessment in the maritime industry,” *M.Sc. thesis, Liverpool John Moores University, Mar. 2024,* Mar. 2024, doi: 10.24377/LJMU.T.00022728.

[118] R. Sørensen, “How to Improve the Cybersecurity Awareness in The Shipping Industry,” 2023, Accessed: May 25, 2025. [Online]. Available: http://www.theseus.fi/handle/10024/816179

[119] Fortinet, “Global Leader of Cybersecurity Solutions and Services.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.fortinet.com/

[120] Supreme Freight, “Cybersecurity in Shipping: New Standards and Best Practices for 2025.” Accessed: Jun. 09, 2025. [Online]. Available: https://supremefreight.com/cybersecurity-in-shipping-new-standards-and-best-practices-for-2025/

[121] Virtual Maritime Academy, “The Future of Maritime Cybersecurity: Trends to Watch in 2025.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.virtualmaritime.academy/the-future-of-maritime-cybersecurity-trends-to-watch-in-2025/

[122] Wartsila, “Strength in numbers: why maritime cyber security is a team sport.” Accessed: Jun. 09, 2025. [Online]. Available: https://www.wartsila.com/insights/article/strength-in-numbers-why-maritime-cyber-security-is-a-team-sport

[123] Oleksiy Melnyk, Oleksandr Drozdov, and Serhii Kuznichenko, “Cybersecurity in maritime transport.” Accessed: Jun. 09, 2025. [Online]. Available: https://lexportus.net.ua/vipusk-1-2025/melnyk_1111.pdf

[124] Marpoint, “2024: A Year of Rising Tides in Maritime Cybersecurity.” Accessed: Jun. 09, 2025. [Online]. Available: https://marpoint.gr/blog/2024-a-year-of-rising-tides-in-maritime-cybersecurity/

[125] Science|Business, “TalTech announces maritime cybersecurity collaboration with Singapore research institutions.” Accessed: Jun. 09, 2025. [Online]. Available: https://sciencebusiness.net/network-updates/taltech-announces-maritime-cybersecurity-collaboration-singapore-research