UNIVERISTY OF PIRAEUS - DEPARTMENT OF INFORMATICS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc «Cybersecurity and Data Science»

ΠΜΣ «Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

MSc Thesis

Μεταπτυχιακή Διατριβή

Thesis Title: Τίτλος Διατριβής:	**Operational Technology (OT) Cyber-Risk Assessment for Maritime Vessels** Πλαίσιο Αξιολόγησης Κυβερνοκινδύνων Λειτουργικής Τεχνολογίας (OT) στον Ναυτιλιακό Κλάδο
Student's name-surname: Ονοματεπώνυμο φοιτητή:	**ANNA VAZINTARI** ΑΝΝΑ ΒΑΖΙΝΤΑΡΗ
Father's name: Πατρώνυμο:	**KONSTANTINOS** ΚΩΝΣΤΑΝΤΙΝΟΣ
Student's ID No: Αριθμός Μητρώου:	ΜΠΚΕΔ2201
Supervisor: Επιβλέπων:	**Despina Polemi, Professor** Δέσποινα Πολέμη, Καθηγήτρια

December 2025/ Δεκεμβρης 2025

3-Member Examination Committee

Τριμελής Εξεταστική Επιτροπή

Despina Polemi **Professor**	**Panagiotis Kotzanikolaou** **Professor**	**Konstantinos Patsakis** **Professor**
Δέσποινα Πολέμη Καθηγήτρια	Παναγιώτης Κοτζανικολάου Καθηγητής	Κωνσταντινός Πατσάκης Καθηγητής

Περίληψη

Η ραγδαία ψηφιοποίηση της ναυτιλίας έχει οδηγήσει στη σύγκλιση των παραδοσιακά απομονωμένων συστημάτων Operational Technology (OT) με δίκτυα IT, δημιουργώντας νέες επιφάνειες επίθεσης και αυξημένα επίπεδα κυβερνο-κινδύνου. Συστήματα όπως ECDIS, GPS/GNSS, αυτόματος πιλότος, PLCs πρόωσης/ισχύος, συστήματα έρματος και αυτοματισμών λειτουργούν πλέον διασυνδεδεμένα, ενώ δίαυλοι απομακρυσμένης συντήρησης και δορυφορικές επικοινωνίες αποτελούν κρίσιμες πηγές ευπάθειας. Παράλληλα, το ρυθμιστικό πλαίσιο (IMO MSC.428(98), IACS UR E26/E27, NIS2, TMSA, DryBMS, κ.λπ.) απαιτεί πλέον συστηματική και τεκμηριωμένη ενσωμάτωση της κυβερνοασφάλειας στο Safety Management System (SMS).

Η εργασία αναπτύσσει και εφαρμόζει ένα υβριδικό πλαίσιο OT cyber-risk assessment, συνδυάζοντας τα πρότυπα IEC 62443, NIST SP 800-82, ISO 31000/27005 και τη μεθοδολογία STRIDE. Το πλαίσιο εφαρμόζεται σε ένα αντιπροσωπευτικό πλοίο τύπου Panamax, περιλαμβάνοντας: καταγραφή OT περιουσιακών στοιχείων, μοντελοποίηση απειλών, ανάλυση ευπαθειών (CVI), ποσοτική αξιολόγηση κινδύνου (Rw) και ανάλυση διασυνδεσιμότητας/διάχυσης (Heat Intensity).

Η μελέτη αποκαλύπτει ότι ο συνολικός κυβερνο-κίνδυνος δεν είναι ομοιόμορφα κατανεμημένος· αντιθέτως συγκεντρώνεται σε λίγα, ισχυρά διασυνδεδεμένα συστήματα: Machinery Automation Server (MAS), OEM remote maintenance tunnel, Engine Control PLC, Steering Gear PLC, και οι δύο μονάδες ECDIS. Τα συστήματα αυτά σχηματίζουν τον «πυρήνα θερμότητας» (core heat cluster) όπου μια επιτυχής επίθεση μπορεί να προκαλέσει ταχεία διάχυση σε κρίσιμες λειτουργίες πλοήγησης, πρόωσης και αυτοματισμών. Δευτερεύοντα συστήματα (PMS, satcom, ballast PLC, cargo monitoring) παρουσιάζουν σημαντικό αλλά περιορισμένο βαθμό συστημικού κινδύνου, ενώ αισθητήρες και περιφερειακά συστήματα φέρουν χαμηλή συστημική επίδραση.

Τέλος, προτείνονται στοχευμένες στρατηγικές ενίσχυσης: αυστηρότερη διαχείριση απομακρυσμένης πρόσβασης, ενίσχυση ζωνών/απομόνωσης δικτύου, έλεγχος αλλαγών, παρακολούθηση συμβάντων, RBAC/MFA και ενσωμάτωση cyber-drills στο SMS. Τα αποτελέσματα δείχνουν ότι οι πλέον κρίσιμοι κίνδυνοι μπορούν να μειωθούν σημαντικά, αλλά ορισμένοι συστημικοί κόμβοι παραμένουν αμετάβλητα υψηλού κινδύνου λόγω της λειτουργικής τους σημασίας και διασυνδεσιμότητας.

Abstract

The rapid digitalisation of the maritime industry has merged previously isolated Operational Technology (OT) systems with IT networks, significantly expanding cyber-attack surfaces across vessels. Navigation, propulsion, machinery automation, ballast, cargo, and communication systems now operate through interconnected digital architectures, while satellite communications and OEM remote-maintenance tunnels further increase exposure. In parallel, the regulatory landscape—including IMO MSC.428(98), IACS UR E26/E27, the EU NIS2 Directive, TMSA and DryBMS—requires that cyber risk management be formally embedded into the Safety Management System (SMS).

This thesis develops and applies a hybrid OT cyber-risk assessment framework, integrating IEC 62443, NIST SP 800-82, ISO 31000/27005, and STRIDE threat modelling. The methodology is applied to a representative Panamax vessel and includes: comprehensive OT asset mapping, threat modelling, vulnerability scoring (CVI), quantitative risk evaluation (Rw), and connectivity-driven systemic heat analysis (Heat Intensity).

Findings show that cyber-risk distribution is highly concentrated rather than uniform. A small set of highly connected OT components forms a core systemic-risk cluster: the Machinery Automation Server (MAS), OEM remote maintenance tunnel, Engine Control PLC, Steering Gear PLC, and both ECDIS units. These nodes act as cross-domain propagation hubs, where compromise can cascade rapidly across propulsion, steering, navigation and automation systems. Secondary systems (PMS, satcom gateway, ballast PLC, cargo monitoring) contribute moderate systemic influence, while sensors and peripheral devices contribute marginally.

Based on these results, the thesis outlines a governance and continuous-assurance model focusing on configuration and firmware governance, strict vendor-access controls, enhanced network segmentation, centralised monitoring/logging, identity management (RBAC/MFA) and cyber-training integrated into the SMS. While mitigation reduces overall systemic heat, certain automation and navigation control points remain inherently high-risk due to their architectural criticality. The study demonstrates that the hybrid methodology provides a rigorous, auditable and maritime-specific approach to OT cyber-risk assessment and aligns with international regulatory and class requirements.

Contents

List of Tables

List of Figures

1 Introduction

The digital transformation of the maritime industry has led to a paradigm shift in how vessels and shipping companies operate. Systems traditionally isolated for safety and operational reliability-such as propulsion control, navigation systems (ECDIS), ballast water management, and engine monitoring-are increasingly interconnected through integrated networks and remote access technologies. This convergence between Information Technology (IT) and Operational Technology (OT) has enhanced efficiency, situational awareness, and maintenance capabilities but has also introduced new vulnerabilities and attack surfaces. Maritime OT systems, originally designed with minimal cybersecurity considerations, are now exposed to cyber threats that can compromise vessel safety, disrupt operations, and impact global trade. As the industry becomes progressively dependent on data-driven operations, Internet of Things (IoT) devices, and cloud-based monitoring, the resilience of shipboard and shore-based OT environments becomes a central concern of maritime cybersecurity governance [**Error! Reference source not found.**],[**Error! Reference source not found.**].

The evolving threat landscape has been reflected in an increasingly complex regulatory and standards ecosystem. The International Maritime Organization (IMO) issued Resolution MSC.428(98) [3], mandating the inclusion of cyber risk management in the Safety Management Systems (SMS) of ships from January 2021. At the same time, classification societies have developed notations and frameworks, such as IACS Unified Requirements UR E26 and UR E27 [4], [5], to guide shipowners in managing cyber risk across IT and OT domains. Moreover, maritime-specific frameworks like TMSA [6] and DryBMS [7] provide additional guidance for implementing security controls aligned with industry best practices.

Complementing these developments, the EU Directive (EU) 2022/2555, known as NIS2, marks a significant advancement in recognizing the maritime domain as part of Europe's critical infrastructure ecosystem [8]. Under NIS2, shipping companies, port authorities, and providers of maritime digital services are classified as essential or important entities, thereby becoming subject to mandatory cybersecurity risk management, incident reporting, and resilience obligations. Importantly, NIS2 extends its scope beyond traditional IT systems to encompass OT environments, reinforcing the requirement for an integrated cyber risk management approach that covers both onboard and shore-based operations.

Within this context, the need for systematic OT risk assessment methodologies tailored to the maritime environment has become imperative. Traditional IT-centric frameworks often fail to capture the operational interdependencies, safety implications, and regulatory nuances inherent to shipboard OT systems. This thesis, therefore, seeks to address this gap by exploring and adapting risk assessment models that are specifically suited to the maritime OT ecosystem.

1.1 Aim and Objectives

The main aim of this thesis is to develop and apply an Operational Technology (OT) risk assessment framework for maritime systems, aligned with international cybersecurity standards and regulatory requirements.

To achieve this aim, the thesis pursues the following objectives:

- To map the structure and interconnectivity of OT systems onboard ships, identifying potential interfaces with IT networks.
- To identify and classify cybersecurity threats and vulnerabilities specific to maritime OT environments.
- To analyze the current regulatory and standards landscape, including IMO, IACS UR E26/E27, TMSA, DryBMS, Rightship [9], ISO/IEC 27000 [10] series, BIMCO, and NIS2.
- To propose or adapt a risk assessment methodology tailored to maritime OT systems, integrating both technical and operational perspectives.

- To evaluate the effectiveness of existing controls and risk mitigation measures within representative maritime scenarios.

1.2 Research Questions

The research is guided by the following key questions:

- What are the primary cyber threats and vulnerabilities affecting OT systems onboard vessels?
- How does the cybersecurity posture of OT systems in shipping differ from other industrial control environments?
- Which existing risk assessment frameworks can be effectively adapted for maritime OT environments?
- How can OT risk management be operationally and procedurally integrated into a shipping company's cybersecurity governance model?
- What role do international standards and directives, including IMO 2021 and NIS2, play in shaping the risk management obligations of maritime operators?

1.3 Why OT Security is Critical for Shipping

OT security in the maritime sector is not merely a technical issue but a matter of safety, regulatory compliance, and business continuity. The compromise of an OT system—such as propulsion, navigation, or cargo handling—can lead to catastrophic outcomes, including loss of navigational control, environmental pollution, physical damage to assets, and human safety risks [11].

Furthermore, the maritime industry forms part of the global critical supply chain. A cyber incident affecting a single ship or port can trigger cascading disruptions in logistics, trade flows, and energy transport. Two of the most illustrative cases are the Colonial Pipeline attack [12]-[14] and the Port of Nagoya ransomware incident [15], both of which exposed the fragility of critical infrastructure when OT systems are indirectly or directly compromised through cyberattacks.

The Colonial Pipeline incident, although primarily initiated through an IT system breach, resulted in the shutdown of the entire fuel distribution network across the U.S. East Coast, causing fuel shortages, economic disruption, and widespread operational delays. The company was forced to halt pipeline operations as a precautionary measure due to the interconnected nature of its IT and OT systems, underscoring the reality that a cyberattack on business networks can propagate to, or necessitate the suspension of, OT operations. From a maritime perspective, this event highlighted that supply-chain dependencies in energy logistics, including tanker scheduling and bunkering operations, are tightly coupled with critical OT infrastructure, meaning that similar vulnerabilities could easily extend to shipping systems.

Similarly, the Port of Nagoya ransomware attack in July 2023 disrupted one of Japan's largest shipping and logistics hubs, temporarily paralyzing terminal operations and delaying thousands of cargo containers. The attack targeted the Nagoya Port Unified Terminal System (NUTS) — a digital platform integrating both administrative IT systems and certain operational control components. The incident led to the suspension of container loading and unloading activities for more than 24 hours, affecting major global shipping lines. This demonstrated that even partial system disruptions in port-based OT environments can have cascading effects across the maritime supply chain, including vessel delays, demurrage costs, and cargo mismanagement.

Both incidents provide valuable insight into the systemic interdependence between IT governance and OT operational safety. They reveal that cyber resilience cannot be achieved through IT protections alone, as operational continuity depends on the integrity, availability, and segmentation of OT systems. For the maritime industry, where navigation, propulsion, and cargo management are inherently operational in nature, a similar compromise could result not only in economic loss but in environmental disasters and safety hazards.

From a regulatory perspective, the intersection of IMO requirements and NIS2 obligations underscores that maritime OT security is now a strategic and legal imperative. Operators are expected to demonstrate due diligence in identifying, assessing, and mitigating cyber risks that could endanger not only their operations but also wider societal and economic stability.

Ultimately, the protection of OT systems forms the foundation of maritime cyber resilience. Without robust OT cybersecurity, even the most advanced IT defences remain insufficient, as operational control—the very core of safe and reliable shipping—depends on the integrity and availability of these systems.

2 Literature Overview

2.1 Information Technology (IT) vs Operational Technology (OT)

This chapter establishes the theoretical and academic foundation for analyzing maritime cyber risk within operational technology (OT) environments. It synthesises current research across three domains -academic scholarship, technical standards, and applied industry studies- to construct a coherent understanding of how cyber risk emerges, propagates, and can be systematically assessed in maritime systems. Whereas Chapter 3 will examine regulatory and industry practice, the implementation of cybersecurity through flag-state directives, class-society rules, and international frameworks, this chapter is concerned with the body of knowledge that underpins those practices. Its scope is therefore analytical rather than prescriptive: it interrogates what is known, theorised, and modelled in the literature about OT security, and identifies conceptual gaps that justify the methodological design later adopted in Chapter 4.

The chapter proceeds from a systems-theoretic premise: that the modern vessel functions as a cyber-physical ecosystem, in which digital information flows directly affect physical outcomes such as propulsion, navigation, and safety [16], [17]. This perspective reframes maritime cybersecurity from a technical subdiscipline of Information Technology (IT) to a branch of safety-critical systems engineering, demanding integrated models that account for human, technical, and organisational interdependencies. The literature review therefore moves through successive layers of abstraction, from the digitalisation of maritime operations to the taxonomy of cyber threats to the theoretical risk-management frameworks that attempt to model these phenomena. By doing so, it situates the thesis within a rigorous conceptual lineage and delineates the intellectual space not yet occupied by existing research.

Dimension	**IT systems**	**OT systems**	**Analytical implication for maritime cyber risk**
Primary objective	Confidentiality	Availability	Cyber incidents in OT have safety consequences
Update frequency	High, automated	Low, class-controlled	Requires risk-based patching
System lifespan	3–5 years	15–25 years	Long lifecycle creates legacy vulnerabilities
Connectivity	Internet/Cloud	Deterministic LAN/fieldbus	Demands segmented network design
Failure effect	Data/Financial loss	Physical damage	Escalates cyber risk to safety risk

Table 2.1 – Structural and Operational Differences between IT and OT Systems

2.2 The Maritime Digital Ecosystem and OT Context

2.2.1 Digitalization and System Convergence

The digital transformation of the maritime industry has fundamentally redefined how ships operate, communicate, and are maintained. Over the last two decades, vessels have evolved from self-contained mechanical platforms into cyber-physical systems (CPS) whose performance and safety depend on the continuous interaction between onboard automation and external data infrastructures [18]. Automation has penetrated every subsystem, from propulsion and power management to cargo handling and navigation, while satellite communications and low-earth-orbit (LEO) connectivity have enabled constant integration with shore-based analytics, fleet management, and predictive-maintenance platforms.

This convergence has effectively collapsed the historical separation between Information Technology (IT) and Operational Technology (OT). IT systems, those supporting enterprise logistics, voyage planning, and crew management, are now intertwined with OT systems that directly control propulsion, steering, ballast, and environmental functions. The result is a dual-domain ecosystem where informational and operational processes are interdependent, creating both unprecedented efficiencies and novel vulnerabilities [19]. From a cyber-risk perspective, this integration replaces the traditional perimeter-based model of defence with one of inter-domain dependency, in which a failure or intrusion in IT can rapidly propagate into safety-critical OT environments.

Analytically, this transformation constitutes a paradigm shift in maritime risk: cybersecurity is no longer a discrete IT discipline but an intrinsic component of system reliability. A single cyber event can now compromise physical safety in the same way as mechanical failure. Theoretical literature on complex systems [16], [20] supports this interpretation by describing such environments as tightly coupled systems-highly interactive networks where small perturbations cascade nonlinearly. Applying this framework to shipping, a malware infection on a navigation workstation or a misconfigured update from shore is not a localised anomaly but a systemic perturbation capable of triggering multi-domain effects.

2.2.2 Structure of Shipboard OT Systems

Operational Technology (OT) on board a vessel encompasses all hardware and software systems that monitor, control, or automate physical processes essential to safe operation. These systems can be grouped into five interrelated functional domains, each representing a distinct category of control functions but interconnected through shared communication architectures [18], [21]:

- Navigation and Bridge Systems – including the Electronic Chart Display and Information System (ECDIS), radar, Automatic Identification System (AIS), Global Navigation Satellite System (GNSS) receivers, and Dynamic Positioning (DP) systems. These are exposed to external data flows and satellite inputs, making them primary targets for spoofing or data-integrity attacks.
- Propulsion and Power Management Systems – comprising Engine Control Units (ECUs), Power Management Systems (PMS), and Integrated Automation Systems (IAS). Their compromise can result in loss of propulsion, blackout, or engine-room casualties.
- Cargo, Ballast, and Auxiliary Automation – such as Ballast Water Management Systems (BWMS), Cargo Control Units (CCU), and tank-monitoring Programmable Logic Controllers. Vulnerabilities in these systems threaten vessel stability and environmental compliance.
- Communication and Telemetry Infrastructure – including satellite terminals (VSAT, Inmarsat, Iridium), onboard routers and switches, and the Voyage Data Recorder (VDR). These provide the digital bridge between ship and shore and, thus, represent critical entry points for threat propagation.
- Safety and Environmental Systems – covering fire detection and suppression, alarm monitoring, bilge, steering, and exhaust-gas cleaning systems. These systems form the vessel's last defensive

layer; their manipulation or malfunction could convert a cyber incident into a safety or pollution event.

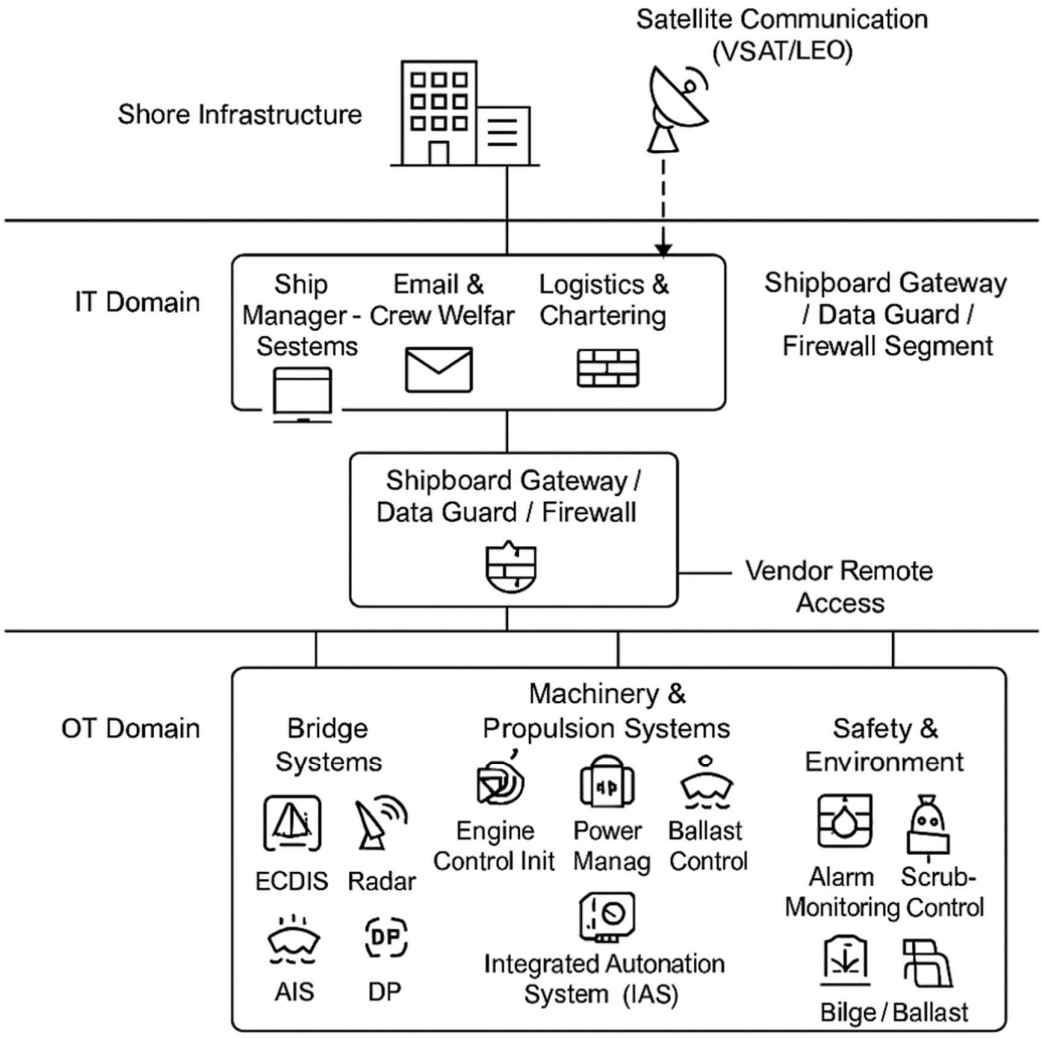

Figure 2.1 – IT and OT Architecture Convergence in Shipboard Systems

Analytically, this structure reflects a hierarchical but porous architecture: OT subsystems are designed for determinism and real-time control yet increasingly rely on IT-managed data networks and cloud connectivity for optimisation. Each additional interface—whether a remote diagnostics link, a crew laptop, or an IoT sensor—represents a potential coupling node where functional integration translates into cyber-risk amplification. The literature thus positions shipboard OT not as a static engineering domain but as an evolving socio-technical ecosystem, where resilience depends equally on design architecture, maintenance culture, and human–machine interaction [21].

2.2.3 Theoretical Perspective

To interpret this convergence, scholars draw upon systems and resilience theory to conceptualise maritime cyber risk as a function of complexity and feedback. Perrow's [20] Normal Accident Theory

posits that tightly coupled, complex systems inevitably experience failures from unanticipated interactions; Leveson's [16] System-Theoretic Accident Model and Processes (STAMP) extends this logic to control-system failures, framing accidents as losses of control rather than isolated malfunctions. In maritime OT contexts, these theories illuminate why traditional probabilistic risk models fail: cyber events are rarely linear cause–effect phenomena but emergent from interacting subsystems and human decision processes. Accordingly, the literature increasingly emphasises resilience engineering—the capacity of systems to absorb, adapt, and recover from disruptions—over static risk reduction [16]. This shift parallels the move from compliance-based cybersecurity toward adaptive risk management. Conceptually, it positions maritime cyber defence within the same epistemological family as safety science and systems engineering, reinforcing the need for multi-disciplinary frameworks that integrate governance, engineering, and behavioural perspectives.

A critical insight from the literature is that the cybersecurity posture of maritime OT diverges significantly from other industrial control environments, both structurally and operationally. In fixed terrestrial industries, such as energy, oil and gas, or manufacturing, OT networks benefit from stable infrastructure, continuous monitoring, and dedicated cybersecurity teams. Maritime systems, by contrast, operate within isolated, resource-constrained, and mobility-dependent contexts where physical remoteness and intermittent connectivity hinder real-time defence [21]. Equipment lifecycles in shipping extend up to two decades, producing technological heterogeneity unmatched in shore-based ICS environments: legacy PLCs coexist with modern Ethernet controllers, often without unified patch strategies [18]. Moreover, ships rely on satellite links with high latency and limited bandwidth, which constrains intrusion detection and remote-update mechanisms that are routine in energy or manufacturing sectors [6]. The regulatory landscape also differs; whereas terrestrial industries operate under sector-specific cyber regimes (e.g., NERC-CIP for energy, IEC 62443 enforcement in manufacturing), the maritime domain historically lacked binding cybersecurity mandates until the IMO 2021 Guidelines. Analytically, these distinctions produce a defensive asymmetry: maritime OT security is not weaker by design but operates under fundamentally different constraints prioritising availability, safety, and certification continuity over rapid threat mitigation. This context underscores the necessity for domain-specific adaptations of generic risk frameworks, a theme developed in Section 2.5.

2.3 Taxonomy of Maritime Cyber Threats

2.3.1 Conceptual Overview

Cyber threats in the maritime environment do not emerge from isolated technical faults but from the interaction of information, control, and human subsystems within a complex, networked vessel. The literature distinguishes maritime cyber threats by both technical mechanism and systemic effect [1], [21]. While generic IT threats—malware, ransomware, phishing—also affect shipping, their consequences differ fundamentally because shipboard systems couple digital logic with physical outcomes. As a result, risk manifests not merely as data compromise but as loss of navigational integrity, propulsion control, or environmental compliance [18].

Analytically, cyber threats in maritime OT can be conceptualised as causal perturbations within a tightly coupled system. They propagate across network, procedural, and organisational boundaries through what Perrow [20] described as complex interactions: small digital anomalies that align with human or procedural weaknesses to produce cascading effects. This section synthesises the literature into six dominant maritime threat classes, GNSS Spoofing and Jamming, Malware Infiltration, Ransomware, Supply-Chain Compromise, Insider Misuse, and Denial-of-Service (DoS), each illustrating a distinct propagation pathway and control-system dependency.

2.3.2 GNSS Spoofing and Jamming

Modern navigation depends critically on Global Navigation Satellite Systems (GNSS) for positioning, navigation, and timing (PNT). Empirical studies report a dramatic escalation of interference incidents since 2023, particularly in geopolitically sensitive zones such as the eastern Mediterranean, Black Sea, and Baltic [23]. Spoofing injects counterfeit satellite signals that mislead receivers into computing false coordinates; jamming blocks legitimate transmissions through signal saturation [24]. GPS Patron and Gdynia Maritime University detected over 84 hours of interference in the Baltic between June and November 2024, mostly jamming [25]. Windward telemetry analysis further found average positional jumps increasing from 600 km in 2024 Q4 to 6 300 km in 2025 Q1 [26].

Analytically, GNSS interference constitutes an epistemic vulnerability: it corrupts the vessel's situational awareness and undermines crew trust in all electronic aids to navigation. Bridge teams face cognitive overload, forced to reconcile contradictory sensor inputs without reliable reference [27]. Frameworks such as IEC 62443 and ISO 27005 mitigate data-integrity risks but do not directly address signal deception. Thus, mitigation relies on cross-domain redundancy—integrating radar, inertial, and optical navigation; deploying anomaly-detection algorithms; segmenting navigation networks; and enhancing crew recognition training [23]. This threat exemplifies how external information dependencies transform cyber events into safety hazards.

2.3.3 Malware Infiltration and Lateral Propagation

Malware remains the most pervasive maritime threat because it exploits both technological and behavioural vulnerabilities. Infection vectors include removable media used for chart updates, vendor laptops connected for maintenance, and remote-access sessions opened for diagnostics [28]. Once introduced, malware often spreads laterally across poorly segmented shipboard LANs linking bridge, engine, and administrative systems.

From a systems perspective, malware attacks reveal architectural fragility: ship networks are typically flat, unmonitored, and dependent on legacy operating systems. A single infection can thus compromise multiple safety-critical subsystems. The consequence is not limited to data loss but extends to functional unavailability-ECDIS display freezes, engine-control faults, or delayed automation responses [21]. Moreover, maritime operations amplify temporal risk: infections acquired in port may activate mid-voyage, when support resources are minimal.

NIST SP 800-82 Rev. 3 [29] recommends removable-media control and allow-listing; IEC 62443-3-3 [10] prescribes segmentation and malicious-code protection (SR 5.x / SR 7.x); and ISO 27005 formalises malware scenarios within risk registers [30]. Yet the literature highlights persistent implementation asymmetry—shipyards design to 62443 standards, but operators rarely maintain configuration discipline after delivery. Analytically, malware represents the archetypal IT–OT coupling risk, in which efficiency-driven connectivity undermines determinism and safety.

2.3.4 Ransomware and Enterprise Disruption

Ransomware transforms digital compromise into enterprise-scale operational paralysis. The Maersk NotPetya attack [31] demonstrated that cyber disruption of corporate IT can immobilise global logistics even when shipboard OT remains functional. Subsequent cases involving COSCO, MSC, and South-African port terminals confirm that ransomware is not isolated but systemic, leveraging shared IT infrastructures [32]-[34].

Analytically, ransomware reveals the economic and organisational dimension of cyber risk. ISO 31000 and ISO 27005 provide qualitative scales for severity but lack financial quantification, leading researchers to propose hybrid models such as FAIR (Factor Analysis of Information Risk) [35]. Frameworks like ISO 27001 and NIST CSF address continuity (Annex A.17; "Recover" function) but presuppose redundant terrestrial infrastructure-conditions rare at sea. The maritime literature thus calls

for distributed data replication and decentralised command fallback as design imperatives. In strategic terms, ransomware acts as a stress test for organisational resilience, validating the integration of business-continuity engineering into cyber-risk frameworks.

2.3.5 Supply-Chain Compromise

Supply-chain compromise attacks the maritime sector's structural reliance on vendor ecosystems. Ships integrate hundreds of components from different OEMs, many retaining remote access for diagnostics. A compromised supplier can therefore inject vulnerabilities at fleet scale [21]. Such attacks challenge the assumption of bounded accountability: shipowners are liable for security but lack visibility into vendor practices. IEC 62443-4-1 [19] introduces Secure Development Life-Cycle (SDL) requirements, and IACS UR E26 [4] mandates vendor cyber documentation during construction. However, post-delivery updates and maintenance remain unregulated, producing a lifecycle assurance gap. Analytically, supply-chain risk exemplifies trans-organisational interdependence -a governance rather than technical problem- and underscores the need for contractual cybersecurity clauses, cryptographic update validation, and independent vulnerability assessment.

2.3.6 Insider Misuse and Human Error

Human error and insider misuse continue to dominate maritime cyber-incident statistics [1]. The problem arises from socio-technical coupling: complex systems depend on disciplined behaviour, yet operational pressures incentivise shortcuts. Typical errors include unauthorised USB use, password sharing, and disabling controls for convenience. ISO 27001 (A.7) and ISO 27005 [6] address awareness training, but neither quantify reliability; hence scholars advocate integrating Human Reliability Analysis (HRA) into cyber-risk models. Analytically, insider threats expose a cultural asymmetry: crews treat cyber procedures as administrative overhead, not safety practice. The literature calls for procedural redesign-automated scanning, simplified controls, and non-punitive error reporting-to embed cyber hygiene within safety culture.

2.3.7 Denial-of-Service (DoS) and Communication Disruption

DoS attacks exploit the maritime sector's dependence on single-path satellite connectivity and limited bandwidth. Flooding, misconfiguration, or even heavy telemetry can saturate VSAT modems, disrupting communications, updates, and remote monitoring [21]. IEC 62443 (SR 5.x) and NIST SP 800-82 recommend segmentation and rate limiting [19], [29], but these assume redundant infrastructure rarely present on ships. The literature therefore treats DoS not only as a security event but as a resilience failure, arguing for architectural redundancy, QoS prioritisation, and procedural drills [2]. Analytically, DoS embodies the gap between theoretical standards and operational feasibility-a recurring theme across maritime cyber risk.

2.3.8 Maritime Cyber Threat Mapping

Threat class	Mechanism / entry vector	Affected systems	Immediate impact	Systemic implication
GNSS jamming / spoofing	Radio-frequency interference; falsified satellite signals	GPS, ECDIS, DP	False position, route deviation	Undermines trust in external data; exposes need for redundancy
Malware infection	Removable media; updates; remote vendor sessions	ECDIS, PMS, bridge PCs	Loss of data integrity; system unavailability	Demonstrates porous boundary between IT and OT
Ransomware / lateral propagation	Compromise of corporate IT, spread via shared credentials	Fleet management, port systems	Business interruption, schedule collapse	Illustrates IT–OT interdependence
Supply-chain compromise	Infected integrator software or firmware	PLCs, sensors, engine control	Manipulated logic, unsafe states	Shows dependency on third-party assurance
Insider / contractor misuse	Shared credentials, poor awareness	All subsystems	Misconfiguration, data loss	Human-factor amplification
Denial of service	Flooding satcom or bridge LAN	Comms and nav networks	Loss of situational awareness	Exposes resilience and redundancy gaps

Table 2.2 – Maritime Threat Taxonomy and Systemic Implications

Table 2.1 – Structural and Operational Differences between IT and OT Systems *illustrates how individual attack vectors scale into systemic failures when combined with organisational weaknesses.*

2.3.9 Systemic Insights

Across these threat classes, three systemic patterns emerge:

- **Hybrid propagation.** Maritime incidents rarely remain in one domain. [21] notes that 90 % of vessel-level cyber events originate ashore, traversing weak segmentation boundaries. The shipping enterprise is therefore a *cyber-ecosystem* rather than a perimeter-defended asset.
- **Trust-chain fragility.** GNSS spoofing and supply-chain attacks exploit systemic reliance on trust - trust in satellite constellations, in vendor code, and in human procedure. This fragility explains the rise of assurance-oriented frameworks such as IEC 62443 and IACS UR E26/E27 that formalise validation and testing requirements rather than prescribing fixed controls.
- **Socio-technical amplification.** Human error remains the most frequent initiating event. The persistence of shared passwords and uncontrolled USB use indicates that cultural and procedural inertia often outweigh technological sophistication. Consequently, risk management must integrate behavioural controls, awareness programmes, and procedural audits.

The strategic insight is that maritime cyber risk behaves less like conventional cybercrime and more like complex accident theory: multiple small degradations align to breach defences. Hence the necessity of multi-layered frameworks combining governance, engineering, and human reliability, analysed in Section 2.4, that capture both technological and organisational dimensions of risk.

2.4 Theoretical Frameworks for Cyber-Risk Management

2.4.1 Evolution of Risk Theory

The conceptual foundations of cyber-risk management are rooted in broader risk theory, which has evolved from deterministic reliability models to systems-based and adaptive governance paradigms. In the mid-20th century, risk was largely defined probabilistically, the product of likelihood and consequence, suitable for mechanical systems with stable parameters. However, as technological environments became more complex and interconnected, this reductionist view proved inadequate. Cyber threats, unlike mechanical faults, are intentional, adaptive, and dynamic; their probability cannot be derived empirically but must be reasoned qualitatively.

Modern frameworks therefore reconceptualise risk as a state of uncertainty within complex socio-technical systems. ISO 31000 [36] encapsulates this philosophical shift, defining risk as the “effect of uncertainty on objectives.” It reframes risk management from avoidance to decision optimisation under uncertainty, aligning with the safety-critical logic of maritime operations. By placing emphasis on governance, communication, and continual improvement, ISO 31000 elevates risk from an engineering calculation to a strategic management discipline. Analytically, this evolution mirrors the maritime industry’s transformation from reactive compliance to proactive resilience-from “avoiding failure” to “ensuring recoverability.”

2.4.2 Comparative Theoretical Constructs

Contemporary risk frameworks differ not by end goal, but by the level of abstraction and the epistemology they employ to structure uncertainty. The principal models relevant to maritime cyber-risk can be grouped as follows:

- Governance and Policy Frameworks (ISO 31000, ISO/IEC 27001). These treat risk as a governance construct: an interplay between policy, accountability, and assurance. ISO/IEC 27001 [10]

formalises governance through the Information Security Management System (ISMS), which institutionalises cyber risk within corporate oversight. The framework's Plan–Do–Check–Act (PDCA) cycle parallels the ISM Code's continuous improvement process, creating conceptual alignment between safety and cybersecurity governance. Its limitation lies in its IT heritage — controls designed for administrative networks are not inherently compatible with the deterministic constraints of OT environments.

- Process Frameworks (ISO/IEC 27005, NIST CSF 2.0). These represent the operational layer of risk theory, defining the stages by which risk is contextualised, analysed, and treated. ISO/IEC 27005 provides a procedural backbone for risk management, describing an iterative workflow that can embed other analytical methods such as STRIDE or Bow-Tie. The NIST Cybersecurity Framework (CSF 2.0) [38] complements this by defining five functional outcomes — Identify, Protect, Detect, Respond, and Recover — which serve as a maturity model for organisational capability. Analytically, the CSF transforms risk management into a learning process: maturity, rather than compliance, becomes the measure of resilience. Both frameworks thus operationalise uncertainty management as continuous adaptation.
- Technical and Systems Frameworks (IEC 62443, NIST SP 800-82 Rev. 3). These translate abstract risk processes into engineering-level control architectures. IEC 62443 defines a hierarchical model of Industrial Automation and Control System (IACS) security, introducing the zone–conduit concept and Security Levels (SL1–SL4). It provides the structural grammar for designing secure OT environments through segmentation, redundancy, and layered defence. NIST SP 800-82 [] complements this by providing operational guidance — access control, configuration management, incident response — making it the pragmatic implementation companion to 62443. Analytically, both frameworks embody the systems-theoretic principle that security emerges from architecture, not isolated controls. Their limitation is complexity: compliance demands substantial technical literacy and resources that smaller operators often lack.
- Quantitative and Scenario-Based Frameworks (FAIR, MEHARI, OCTAVE, Bow-Tie, FTA). These approaches seek to overcome the qualitative bias of governance and process models. The FAIR model (Jones & Ashenden, 2019) quantifies risk by mapping loss events to frequency and magnitude distributions, allowing financial estimation of cyber exposure. MEHARI and OCTAVE Allegro combine semi-quantitative scoring with scenario analysis to structure decision-making. In safety engineering, Bow-Tie Analysis and Fault-Tree Analysis (FTA) bridge causal logic with mitigation planning, linking cyber events to safety barriers [4]. Analytically, these models enrich cyber-risk discourse with causal transparency and traceability, though they rely on data seldom available in maritime contexts.

Together, these theoretical constructs constitute a multi-layered epistemology of risk, governance defines purpose, process defines logic, technical frameworks define structure, and quantitative models define measurement.

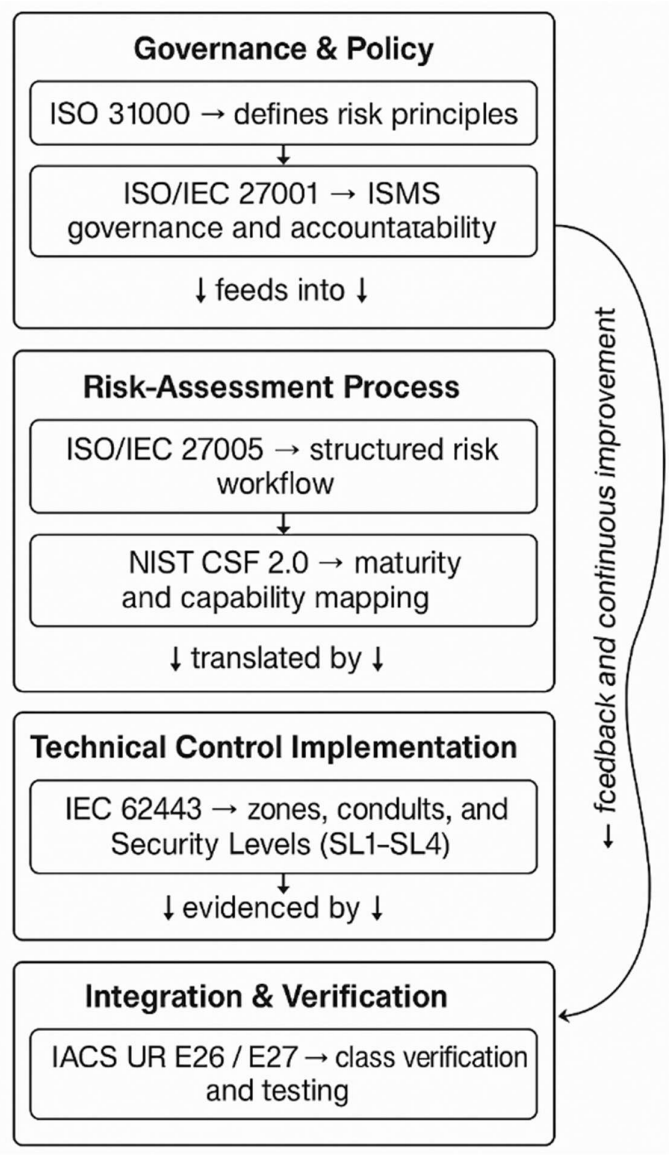

Figure 2.2 – Comparative Theoretical Framework Hierarchy

2.4.3 Comparative Evaluation in Maritime Literature

Academic and technical studies consistently adapt these frameworks to maritime contexts, but with differing degrees of conceptual fidelity. Research by DNV [2], ENISA [21], and Lloyd's Register [34] demonstrates that ISO 27005 provides the procedural core of maritime cyber-risk assessment, while IEC 62443 supplies the architectural model required for OT systems. Empirical trials confirm that combining the two produces a hybrid model capable of mapping both organisational and technical risk dimensions. In contrast, frameworks, such as FAIR and OCTAVE, remain underused in shipping, as they demand quantitative data and simulation capabilities absent in operational fleets. Bow-Tie Analysis and FTA, however, have gained traction because they allow integration with established safety management systems, visually mapping cyber causes to navigational or mechanical consequences [4] ABS, 2023).

Analytically, the literature demonstrates a hierarchical complementarity rather than competition between frameworks. ISO and NIST standards govern how organisations think about risk; IEC standards govern how systems are designed to embody that thinking. This stratification forms the

intellectual backbone of modern maritime cyber resilience: governance → process → architecture → verification.

2.4.4 Theoretical Limitations and Research Gap

Despite their breadth, the literature identifies persistent epistemic and practical gaps in existing risk frameworks:

1. Human-factor abstraction: Frameworks conceptualise human error qualitatively but lack behavioural metrics for crew performance or fatigue-related reliability [1].
2. Economic non-linearity: Financial quantification models such as FAIR are rarely calibrated for maritime operations, obscuring the relationship between cyber investment and safety outcomes.
3. Lifecycle discontinuity: Most standards focus on design and assessment phases, not the dynamic operational drift that occurs as vessels age and systems evolve [34].
4. Cross-framework fragmentation: Integration between governance, technical, and verification standards remains ad hoc, dependent on class interpretation rather than unified theory.

Analytically, these deficiencies underscore the need for a hybrid methodological approach-one that combines the procedural rigour of ISO 27005, the architectural precision of IEC 62443, and the adversarial logic of STRIDE. Such synthesis forms the theoretical justification for the methodological design presented in Chapter 4.

2.5 Adaptation of Frameworks to Maritime OT Environments

2.5.1 From Theory to Application

The translation of cyber-risk theory into maritime practice reflects a gradual but uneven process. Whereas generic frameworks such as ISO 27005 and NIST CSF articulate abstract risk principles, shipboard operational contexts impose unique technical, procedural, and environmental constraints: limited connectivity, class certification dependencies, and the primacy of safety over data confidentiality. Consequently, each framework has been selectively adapted to meet the availability- and integrity-dominated logic of OT systems [2]-[21].

Analytically, this adaptation demonstrates the maritime sector's evolution from cyber-compliance to cyber-resilience. ISO's governance philosophy supplies managerial accountability; NIST's process architecture structures capability growth; IEC's engineering standards operationalise security in hardware and network design; and IACS verification requirements embed these elements into enforceable design practice. The following subsections examine these layers as they manifest in contemporary shipboard functions.

2.5.2 Governance and Organisational Adaptations – ISO 31000 / 27001

At the governance layer, maritime operators apply ISO 31000 and ISO/IEC 27001 to frame cyber risk within existing Safety Management Systems (SMS) and International Safety Management (ISM) Code structures. The ISMS concept is repurposed as a cyber governance subsystem of the SMS, establishing documented accountability, roles, and continuous-improvement cycles analogous to those used for safety. Empirically, fleet operators such as Maersk and Shell have integrated ISO 27001 certification into their corporate compliance regimes, while classification societies (BV, DNV, ABS) embed ISMS evidence in their "Cyber Secure" or "Cyber Managed" notations, presented in more detail in Chapter 3. Analytically, this approach converts cyber risk into a board-level governance issue, ensuring executive oversight and alignment of cyber objectives with safety performance. However, literature notes a domain translation gap: ISO 27001's Annex A controls assume rebootable IT assets and rapid patching cycles, neither feasible nor certifiable in deterministic OT environments. Thus, in shipping, ISO 27001

functions less as a technical blueprint and more as a policy wrapper linking corporate governance to class-approved technical standards such as IEC 62443.

2.5.3 Risk-Process Adaptations – ISO 27005 and NIST CSF 2.0

ISO/IEC 27005 [30] forms the procedural nucleus of most maritime risk-assessment methodologies. Class societies require documented evidence of its five iterative stages—context, identification, analysis, evaluation, and treatment—when approving cyber-risk assessments for newbuilds under UR E26. Its flexibility allows the incorporation of domain-specific analytical methods for adversarial modelling and causal analysis, provided they align with the ISO 27005 workflow [18].

The NIST Cybersecurity Framework (CSF 2.0) [37] provides the complementary maturity model, describing outcomes rather than prescriptions. ABS and LR employ CSF profiles to benchmark operators' resilience levels, producing measurable capability matrices across the five core functions: Identify, Protect, Detect, Respond, and Recover. Analytically, this pairing transforms risk management into a learning system, ISO 27005 structures analytical logic, while NIST CSF measures progress and communication efficacy across technical and managerial hierarchies. The primary limitation lies in resource asymmetry: smaller shipowners seldom possess the staffing or data necessary to maintain continuous maturity assessment, reducing adoption beyond major operators.

2.5.4 Technical-Control Adaptations – IEC 62443 and NIST SP 800-82 Rev. 3

The most significant conceptual import into maritime OT comes from the IEC 62443 family. Originally conceived for industrial control systems, it has been re-contextualised for shipboard automation. Its zone-and-conduit architecture provides the structural language for vessel design: bridge, machinery, cargo, and safety subsystems are mapped into discrete security zones, with controlled data conduits governing communication between them. The associated Security Levels (SL1–SL4) allow designers to align protection depth with risk criticality—navigation and propulsion typically SL3, administrative networks SL1 or SL2.

In practice, IEC 62443 [19] functions as the engineering grammar underpinning class verification. DNV's Cyber Secure notation, BV's Cyber Managed, and ABS's FCI-CS all reference 62443 in design-approval templates. NIST SP 800-82 Rev. 3 complements this by supplying the operational control catalogue-access management, configuration, patching, and monitoring-used by system integrators and shipyards [29]. Together, they translate abstract governance goals into measurable, testable architecture. Analytically, these standards represent the physical embodiment of risk management: they transform risk appetite into design geometry. Yet they also expose the "design-time vs run-time paradox": while new vessels achieve compliance at delivery, operators often lack the resources or expertise to maintain zoning and conduit integrity throughout the ship's lifecycle [34]. Post-delivery degradation thus re-introduces vulnerabilities that frameworks theoretically remove.

2.5.5 Quantitative and Scenario-Based Frameworks – FAIR, MEHARI, and OCTAVE

Beyond governance, process, and technical architectures, the literature recognises quantitative and semi-quantitative risk-analysis models that complement qualitative frameworks. FAIR (Factor Analysis of Information Risk) translates cyber exposure into probabilistic financial loss distributions, allowing cost–benefit analysis of controls [6]. MEHARI and OCTAVE Allegro use semi-quantitative scoring and scenario libraries to evaluate asset criticality and treatment effectiveness [21].

In maritime studies, these models appear mainly in research and pilot projects rather than operational deployment. They provide analytical transparency and facilitate communication with financial and insurance stakeholders but require extensive datasets rarely available for vessels. Consequently, they remain conceptual complements to ISO 27005 rather than operational substitutes, enriching theoretical discourse on how risk can be quantified within safety-critical domains.

2.5.6 Safety-Derived Analytical Models - Bow-Tie and FTA

Beyond quantitative and qualitative frameworks, the maritime literature increasingly integrates Bow-Tie Analysis and Fault Tree Analysis (FTA) [6] as bridging tools between safety engineering and cyber-risk management. Both approaches originate in traditional reliability and accident analysis but have been adapted to capture cyber-induced failure paths. Bow-Tie Analysis visualises the causal chain from initiating cyber events to safety consequences, mapping preventive and mitigative barriers around a central “top event.” FTA, by contrast, decomposes complex system failures into contributing basic events, allowing analysts to estimate cumulative probabilities of cyber-induced safety incidents [2], [11]. Their inclusion in maritime risk studies demonstrates an emerging effort to fuse safety logic with cybersecurity frameworks, translating the deterministic reasoning of safety engineering into the probabilistic and adversarial context of cyber resilience. Analytically, Bow-Tie and FTA occupy a unique position: they do not identify threats but structure the causal propagation of risk, providing a critical bridge between cyber governance frameworks and operational safety management. While Bow-Tie and FTA extend the analytical reach of maritime risk assessment by visualising and quantifying how cyber events can escalate into safety incidents, they remain fundamentally reactive frameworks—tools for causal mapping and reliability validation once threats are already conceptualised.

2.5.7 Analytical Reflection and Transition

Framework	Primary Maritime Function	Research / Industrial Use	Analytical Strength	Limitation
ISO 31000	Corporate and strategic governance	Enterprise risk-policy design; alignment of safety and cybersecurity	Establishes risk principles and decision accountability	Abstract; no implementation guidance
ISO/IEC 27001	Management and organisational governance	Integration of ISMS into Safety Management System (SMS)	Institutionalises cyber governance; auditable and certifiable	IT-centric; lacks OT-specific controls
ISO/IEC 27005	Risk-assessment process	Fleet and ship-level risk registers	Flexible and iterative; integrates with causal and scenario tools	Qualitative; limited quantification
NIST CSF 2.0	Capability maturity benchmarking	Applied in audits and resilience scoring	Communicative clarity across stakeholders	Non-prescriptive; resource-intensive
IEC 62443	OT network architecture and engineering design	Bridge, propulsion, and automation integration	Defence-in-depth zoning and security-level logic	Complex implementation; maintenance burden
NIST SP 800-82 Rev. 3	Operational control and maintenance	Configuration management and vendor access	Practical technical controls for ICS	U.S.-centric scope; limited maritime fit
FAIR / MEHARI / OCTAVE	Quantitative and semi-quantitative analysis	Academic and pilot applications	Financial and scenario-based modelling of cyber impact	Data requirements; limited validation
Bow-Tie / FTA	Safety–cyber interface modelling	Navigation, propulsion, port operations	Causal clarity linking cyber failure to safety outcomes	Semi-quantitative; no dynamic feedback

Table 2.3 – Frameworks Mapped to Maritime Functions

The matrix illustrates how diverse frameworks complement one another across the maritime cyber-risk spectrum. ISO and NIST standards provide governance and procedural scaffolding; IEC 62443 and NIST 800-82 translate those principles into engineering controls; and quantitative models such as FAIR and OCTAVE extend analytical depth. Together, they form a multi-dimensional assurance architecture aligning organisational policy, procedural rigour, and technical design.

None of the risk or safety models discussed thus far explicitly define the mechanism for identifying, categorising, and modelling threats in a systematic and repeatable manner. This methodological gap separates risk governance from threat analysis. To bridge it, the literature introduces threat-modelling methodologies that operationalise the reviewed frameworks by systematically mapping adversarial behaviour, data flows, and system boundaries. The following section therefore examines these analytical tools, most notably the STRIDE model, to demonstrate how theoretical frameworks are translated into practical, architecture-driven analyses within maritime OT environments.

2.6 Threat-Modelling Methodologies and Analytical Tools

2.6.1 Conceptual Basis

Within cyber-risk management, threat modelling serves as the analytical mechanism that translates abstract risk theory into operational scenario logic. While risk frameworks such as ISO 27005 define how risk is managed, threat-modelling methods define what is being managed—identifying the adversarial paths through which vulnerabilities could lead to system compromise [6]. In industrial and maritime contexts, threat modelling is particularly significant because OT networks are deterministic and functionally complex, making exhaustive enumeration of attack paths impractical.
The purpose of threat modelling in this context is therefore twofold:

- To provide structured identification of potential attack vectors across the multi-layered shipboard environment (bridge, engine, cargo, communications, and safety systems); and
- To enable traceable linkage between identified threats, system components, and mitigating controls defined in frameworks such as IEC 62443 and ISO 27005.

Academically, this discipline evolved from software-engineering security analysis [6] into systemic adversarial modelling. In ICS and maritime research, threat-modelling techniques are used not merely for design assurance but for risk quantification and prioritisation (DNV, 2022). By embedding threat modelling within a risk framework, the analysis moves from control checklists toward causal reasoning, enabling structured evaluation of how cyber events propagate through cyber–physical systems.

2.6.2 Comparative Analysis of Threat-Modelling Approaches

Multiple threat-modelling methodologies have been proposed across domains. Their theoretical distinction lies in how they conceptualise threats, assets, and attacker intent. The literature identifies five major approaches relevant to OT systems [21][41]:

- STRIDE [39]: A category-based framework that classifies threats into six archetypes: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE's analytical strength is its taxonomic simplicity and compatibility with system-architecture diagrams. Each threat category maps directly to specific system assets and trust boundaries, facilitating structured identification of attack surfaces. It is well suited for environments where system topologies (like bridge or engine networks) are known but empirical attack data are scarce.
- PASTA (Process for Attack Simulation and Threat Analysis): A risk-centric, seven-stage methodology that integrates business impact, attacker motivation, and simulation of attack paths [41]. Its advantage lies in holistic risk linkage, but its complexity and data demands make it impractical for shipboard OT, where adversarial intelligence and telemetry are limited.

- VAST (Visual, Agile, and Simple Threat): Derived from agile development, VAST uses visual modelling to represent component-level and operational-level threats. It is efficient for dynamic cloud systems but lacks constructs for real-time control dependencies, making it less applicable to maritime OT, which prioritises deterministic operations over rapid iteration [37].
- MITRE ATT&CK for ICS: A knowledge base of adversary tactics and techniques specific to industrial environments. It excels at post-incident forensics and threat intelligence correlation but does not generate new scenarios—it classifies observed ones. In maritime contexts, its use is primarily for aligning findings with known adversary behaviours rather than for forward-looking risk assessment [43].

Analytically, these methods occupy a spectrum of abstraction: from categorical enumeration (STRIDE) to behavioural simulation (PASTA) and post-facto taxonomy (MITRE ATT&CK). The literature recognises that maritime OT environments, constrained by limited data and high system determinism, require a lightweight, architecture-driven method capable of integration with ISO 27005 and IEC 62443 processes. STRIDE uniquely satisfies these criteria by providing categorical breadth, procedural simplicity, and architectural traceability.

2.6.3 Rationale for Selecting STRIDE

The adoption of STRIDE as the analytical instrument in this thesis is grounded in three interrelated criteria: conceptual alignment, operational feasibility, and integrative potential.

- Conceptual Alignment – STRIDE complements the risk-identification and analysis phases of ISO 27005. Each threat category corresponds to potential deviations from asset integrity, authenticity, or availability, which can be systematically evaluated using IEC 62443-defined controls (SR 1.x–SR 7.x). Thus, STRIDE acts as the threat generator within the risk-analysis workflow.
- Operational Feasibility – STRIDE's model requires only system architecture diagrams and functional mappings—resources readily available from ship design documentation. It does not depend on large datasets or real-time telemetry, making it applicable to maritime case studies where quantitative threat data are scarce [2].
- Integrative Potential – By associating each STRIDE category with corresponding IEC 62443 security requirements and ISO 27005 control treatments, STRIDE enables traceability from threat origin to mitigation strategy. This traceability is essential for class verification (UR E26/E27) and aligns with the IMO's requirement for demonstrable cyber-risk management processes [3].
- Analytically, STRIDE represents a middle ground between theoretical completeness and operational pragmatism. It provides a rigorous but lightweight framework that can model multi-domain threats, ranging from spoofing in GNSS navigation to privilege escalation in engine-control networks, without exceeding the analytical capacity of shipboard risk teams. For this reason, STRIDE is employed in this thesis as the central analytical tool within a hybrid ISO 27005 / IEC 62443 framework, detailed in Chapter 4.

2.6.4 Integration with Risk Frameworks

In the proposed hybrid model, STRIDE acts as the bridge between qualitative and structural risk analysis:

- Within ISO 27005, STRIDE populates the risk-identification phase with systematic threat categories, ensuring that no adversarial vector is overlooked.
- Within IEC 62443, each STRIDE threat maps to specific Security Requirements (SRs) — for instance, Spoofing relates to SR 1.x (Identification and Authentication), Tampering to SR 3.x (System Integrity), and Denial of Service to SR 5.x (Resource Availability).
- Within NIST SP 800-82, STRIDE findings inform the configuration and monitoring of access controls, zoning, and network segmentation.

Figure 2.3 – STRIDE Threat-Modelling Pipeline for Shipboard OT

Analytically, this integration operationalises the risk-to-control feedback loop: threats are identified through STRIDE, contextualised through ISO 27005, mitigated through IEC 62443, and validated through IACS UR verification. This synergy converts threat modelling from an abstract exercise into a measurable and auditable component of maritime cyber-risk management.

2.7 Literature Gaps and Analytical Synthesis

The review of existing literature reveals a maturing but still fragmented understanding of cyber-risk management in maritime operational technology (OT) environments. Collectively, research and standards have achieved substantial conceptual progress in defining cyber risk, developing governance structures, and extending control frameworks from information technology (IT) into industrial and safety-critical domains. The integration of ISO 31000, ISO/IEC 27001, and ISO/IEC 27005 has created a managerial and procedural backbone for risk governance, while technical frameworks such as IEC 62443 and NIST SP 800-82 provide architectural and control-level translation. Complementary analytical approaches—including FAIR, MEHARI, and OCTAVE—have enhanced the quantification of risk and decision transparency. Finally, Bow-Tie and Fault-Tree Analysis (FTA) extend this logic by visually linking cyber events to safety consequences, reinforcing the systemic coupling between digital resilience and maritime safety assurance.

Yet, despite this proliferation of frameworks and analytical models, the literature exposes several persistent gaps that constrain their effectiveness within the maritime context:

- Empirical scarcity and operational opacity: Most studies rely on theoretical modelling or incident anecdotes; systematic data on real cyber events aboard vessels remain limited due to confidentiality and underreporting [21]. As a result, validation of framework efficacy under live maritime conditions is sparse.
- Fragmented integration between governance, process, and technical layers: While standards exist at each level, few studies demonstrate a unified implementation across shipboard networks, corporate governance, and vendor ecosystems. Maritime cyber-risk management remains procedurally disjointed, with overlaps, gaps, and ambiguous accountability between shore and vessel operations.
- Underdeveloped threat-modelling methodologies: Existing frameworks describe risk workflows but lack systematic methods for identifying, classifying, and tracing threats across IT–OT boundaries. This creates a methodological vacuum between theoretical risk management (ISO 27005) and architectural security engineering (IEC 62443).
- Limited quantification and human-factor modelling: Quantitative frameworks such as FAIR are data-intensive and rarely applied in operational fleets. Moreover, human performance, fatigue, and training—central to maritime risk—are seldom parameterised in cyber-risk analyses (Lind, 2021).
- Lifecycle discontinuity: Risk assessments typically occur at design or class-approval stages but degrade through vessel operation and retrofits. Few models account for risk drift or system evolution across the ship's lifecycle [34].

Analytically, these deficiencies reveal that maritime cyber-risk management remains conceptually rich but methodologically shallow. Theoretical frameworks articulate what should be done, yet the analytical mechanisms for how to do it—particularly in identifying, modelling, and prioritising OT-specific threats—are immature. The literature therefore calls for a hybridised methodology that unifies the procedural rigour of ISO 27005, the architectural precision of IEC 62443, and the causal logic of threat-modelling tools such as STRIDE. Such integration would provide a complete analytical chain from governance intent to operational control, closing the gap between theory and applied risk assessment in maritime cyber-physical systems.

This identified gap forms the foundation for the methodological framework developed in Chapter 4, where a hybrid ISO 27005 / IEC 62443 / STRIDE model is proposed to systematically assess cyber risk

across shipboard OT domains. By operationalising risk theory through threat-modelling logic, the proposed approach aims to translate abstract resilience principles into a structured, repeatable, and auditable maritime-specific methodology.

3 Regulatory and Industry Context

3.1 Introduction

Cybersecurity within the maritime domain has evolved from an IT concern into a regulatory, operational, and commercial imperative. As vessels become increasingly digitised and interconnected, the International Maritime Organization (IMO), classification societies, and industry associations have introduced a layered system of governance to address cyber risk throughout the ship lifecycle. This regulatory ecosystem integrates policy (IMO), technical standardisation and assurance (IACS and class societies), and commercial or contractual mechanisms (BIMCO, TMSA, DryBMS, RightShip). Together, these instruments form a continuum of governance that links design, operation, and compliance under a shared objective of maritime cyber resilience. The purpose of this chapter is to examine these frameworks comparatively and analytically identifying their scope, interdependencies, and gaps. Unlike Chapter 2, which explored the analytical and methodological foundations of cyber risk assessment, this chapter focuses on how regulatory and industry mechanisms translate those principles into enforceable practice across the maritime sector.

3.2 Vessel Types and Framework Applicability Context

Effective assessment of maritime cyber risk requires a clear understanding of the operational and technical diversity among vessel classes. Each ship type represents a distinct cyber-physical environment shaped by automation intensity, communication topology, and safety-critical dependencies. This diversity explains why sectoral frameworks and initiatives addressed in this chapter (such as IMO MSC-FAL.1/Circ.3, IACS UR E26/E27, TMSA, DryBMS, RightShip) apply unevenly across the global fleet [21].

3.2.1 Bulk Carriers

Bulk carriers transport unpackaged dry commodities such as coal, grain, and iron ore. They are generally categorised by deadweight tonnage (DWT) as follows:

- Handysize (≤ 40,000 DWT): limited automation; manual cargo and ballast operations.
- Handymax / Supramax (40,000–60,000 DWT): moderate automation including remote ballast and cargo monitoring.
- Panamax (60,000–80,000 DWT): integrated bridge and machinery control.
- Capesize (≥ 120,000 DWT): high dependence on centralised automation and power-management systems.

Bulk carriers typically operate under the ISM Code and DryBMS, and their cyber exposure concentrates on propulsion, ballast, and cargo-control subsystems. While automation levels are modest, increasing digital integration in maintenance and reporting systems is expanding their vulnerability perimeter.

3.2.2 Tankers (Crude, Product, Chemical, and LNG/LPG Carriers)

Tankers are among the most automation-intensive vessels, reflecting stringent safety and environmental-protection regulations [6][44]. They include:

- Product and Chemical Tankers (10,000–80,000 DWT): advanced valve and cargo-control PLCs.

- Crude Oil Tankers (80,000–320,000 DWT): redundant inert-gas, cargo-monitoring, and engine-control systems.
- Liquefied Gas Carriers (LNG/LPG, 100,000–200,000 m^3): complex cryogenic containment and reliquefaction systems managed through distributed control and emergency shutdown networks.

LNG carriers have refinery-level automation density, relying on process-control and safety systems that are frequently maintained via remote vendor connections. Frameworks such as TMSA 4, IACS UR E26/E27, and IMO MSC-FAL.1/Circ.3 explicitly reference these vessels. SIGTTO guidelines further complement them by mandating network segregation, access control, and change-management practices for gas-handling automation.

3.2.3 Container Ships

Container vessels are the most digitally interconnected ships in operation. They integrate propulsion and navigation with logistics systems and port data exchanges.

- Feeder (< 2,000 TEU): low integration; regional operations.
- Panamax (≈ 4,000–5,000 TEU): moderate integration of bridge, machinery, and cargo systems.
- Post-Panamax (5,000–10,000 TEU): full propulsion and cargo automation with energy-management systems.
- Ultra-Large Container Ships (≥ 18,000 TEU): fully networked automation and real-time data exchange with port community systems.

Because of their reliance on electronic data interchange (EDI) and port logistics networks, container ships face the highest exposure to supply-chain cyber threats. Relevant frameworks include ISO/IEC 27001, IEC 62443, and EU NIS2, which address authentication, critical-system segregation, and incident reporting.

3.2.4 Passenger, Cruise, and Ro-Ro Vessels

Passenger and roll-on/roll-off (Ro-Ro) vessels exhibit the greatest IT/OT convergence of any maritime class. Large cruise ships integrate industrial control systems with hotel management, entertainment, and passenger-service networks. Such interconnection between safety-critical and public systems expands the attack surface exponentially. Ferries and Ro-Ro ships, while smaller, also connect propulsion and ramp automation with ticketing and scheduling systems, making them susceptible to lateral attacks from corporate IT domains. These vessels are primarily governed under the ISM Code, SOLAS, and class cybersecurity notations.

3.2.5 Offshore and Specialised Vessels

Offshore support vessels (OSVs), drilling units, dynamic-positioning (DP) ships, and research vessels operate with mission-specific control architectures integrating propulsion, positioning, environmental monitoring, and safety systems. They often follow IEC 62443-based segmentation, yet their constant satellite connectivity and remote vendor maintenance create distinct supply-chain attack vectors. Cyber governance typically derives from class notation and IACS guidance, rather than sectoral frameworks like TMSA or DryBMS.

3.2.6 Comparative Summary

Vessel Type	Typical Size Class	Automation Complexity	Network Exposure	Cyber-Risk Profile	Applicable Frameworks
Bulk Carrier	Handysize–Capesize (≤ 180k DWT)	Medium	Moderate	High – propulsion/ballast dependency	DryBMS, ISM
Tanker (Crude/Product/LNG/LPG)	10k–320k DWT / 100–200k m³	High	Medium–High	Very High – process-control safety	TMSA, IACS UR E26/E27, IMO, SIGTTO
Container Ship	Feeder–ULCS (≤ 24k TEU)	Very High	Very High	Very High – supply-chain exposure	ISO 27001, IEC 62443, NIS2
Passenger / Ro-Ro	Variable	Very High	Extreme	Very High – IT/OT convergence	ISM, IMO
Offshore / Specialised	Variable	High	Variable	Moderate – vendor remote maintenance	IEC 62443, Class Rules

Table 3.1 – Vessel Types and Framework Applicability Summary

Each vessel type presents a unique cyber-risk posture determined by automation intensity, connectivity, and regulatory coverage. Bulk carriers remain low automation but are increasingly exposed through digital reporting. Tankers, especially LNG/LPG carriers, require process-control-level cyber resilience. Container ships face global network exposure through logistics systems. Passenger and Ro-Ro vessels blur the line between operational and public IT environments. Offshore vessels depend heavily on remote vendor networks, heightening supply-chain dependency. This contextual understanding provides the foundation for analysing the regulatory and assurance frameworks that follow.

3.3 IMO Guidelines and Regulatory Integration

The International Maritime Organization (IMO) established the regulatory foundation for maritime cyber risk management through the publication of the MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management in June 2017[45]. These guidelines urged shipowners, operators, and managers to integrate cyber risk considerations into their existing Safety Management Systems (SMS) under the International Safety Management (ISM) Code, thereby embedding cyber resilience within the broader framework of operational safety and environmental protection [46].

The IMO guidelines adopt five functional pillars - Identify, Protect, Detect, Respond, and Recover - which mirror the structure of the NIST Cybersecurity Framework. The document promotes a risk-based approach whereby each company identifies its critical systems, assesses potential vulnerabilities, and implements proportional controls to ensure continuity of essential operations. Although intentionally non-prescriptive, the circular provided the conceptual baseline for integrating cybersecurity into maritime safety governance.

This guidance was further strengthened through the adoption of Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, which was approved by the Maritime Safety Committee at its 98th session in June 2017 and entered into force on 1 January 2021. The resolution made it mandatory for all companies and ships subject to the ISM Code to incorporate cyber risk management into their SMS. From this date, cyber resilience became an auditable element during ISM and Document of Compliance (DOC) verification processes, marking a pivotal shift from voluntary compliance to regulatory enforcement. The chronological development of cyber risk integration under the ISM Code is summarised as follows:

Year	Development	Description
2016	Awareness and consultation	IMO's MSC 96 recognised the rising cyber threat and initiated proposals for guidance.
June 2017	MSC-FAL.1/Circ.3 issued	IMO released voluntary Guidelines on Maritime Cyber Risk Management promoting integration within the SMS.
June 2017	Resolution MSC.428(98) adopted	Formally required that cyber risk management be addressed in compliance with the ISM Code.
1 January 2021	Enforcement	Cyber risk management became a mandatory ISM requirement, subject to flag and class audit verification.

Table 3.3 – Key Maritime Cybersecurity Regulatory Milestones

This transition represents a milestone in maritime safety regulation. Cyber risk management is now recognised as a core operational requirement, ensuring that both organisational and technical controls are embedded in daily operations. However, the IMO's framework remains principle-based rather than prescriptive, leaving implementation detail to classification societies and industry bodies. This has led to a proliferation of technical and sectoral frameworks -such as those from IACS, BIMCO, and industry associations -which provide practical guidance and measurable criteria for compliance.

3.4 The EU NIS2 Directive and Regional Cyber Governance (Expanded Technical Analysis)

The NIS2 Directive (Directive (EU) 2022/2555) [8] represents the most significant reform of European cybersecurity legislation to date, establishing a harmonised and enforceable baseline of cyber-controls for critical infrastructure sectors. Entering into force in January 2023, NIS2 replaces the original 2016 NIS Directive and substantially broadens both the scope of regulated entities and the technical requirements imposed upon them.

In the maritime domain, NIS2 applies to shipping companies, ship-management offices, ports, terminals, classification societies operating in the EU, and digital service providers supporting maritime operations. These entities are categorised as essential or important, with mandatory security measures, reporting obligations, and supervisory enforcement.

3.4.1 Technical Cybersecurity Requirements Under NIS2

NIS2 defines a set of mandatory risk-management measures (Article 21) that organisations must implement. These measures are highly technical and extend well beyond traditional safety management.

(1) Risk Analysis & Information System Security

Operators must implement:

- asset inventories,
- vulnerability assessment procedures,
- network segmentation across IT and OT domains,
- multi-layered security architecture aligned with ENISA best practices.

(2) Incident Detection, Logging, and Monitoring

NIS2 requires:

- real-time anomaly detection (IDS/IPS),
- event logging across IT/OT networks,
- centralised security monitoring (SIEM),
- retention of logs to support forensic analysis.

(3) Identity, Access, and Privilege Management

Mandatory adoption of:

- strong authentication mechanisms (MFA),
- privileged access controls (PAM),
- secure remote-access policies for vendors and OEMs,
- role-based access control aligned with least-privilege principles.

(4) Business Continuity and Disaster Recovery

Operators must maintain:

- tested business-continuity plans (BCP),
- backup and redundancy mechanisms,
- cyber-incident restoration capabilities,
- operational resilience procedures for OT systems, including fallback to manual modes where applicable.

(5) Supply-Chain Security

This is one of the most impactful maritime provisions:

- mandatory supplier evaluation,
- cybersecurity requirements for vendors of navigation, communication, and control systems,
- contractual controls over maintenance access and software updates,
- continuous monitoring of third-party risks.

This requirement directly affects OEMs of ECDIS, DP systems, PLCs, VDRs, SATCOM terminals, and maintenance contractors -a domain not covered explicitly by IMO or IACS.

(6) Cryptography & Data Protection

NIS2 mandates:

- encryption of data in transit and at rest,
- secure key management,
- integrity validation for critical data flows (e.g., cargo manifests, port–ship EDI).

(7) Policies & Procedures for Vulnerability Disclosure

Operators must establish:

- vulnerability-management protocols,
- patch-management processes applicable to both IT and OT,
- coordinated disclosure mechanisms with ENISA.

3.4.2 Mandatory Incident Reporting

NIS2 introduces a strict, three-phase incident reporting regime:

Report	Deadline	Purpose
Early Warning	within 24 hours	Notify national authority of suspected significant incident
Incident Notification	within 72 hours	Provide impact assessment, indicators of compromise, and mitigation measures
Final Report	within 1 month	Root-cause analysis, long-term remediation and lessons learned

Table 3.4 – NIS2 Incident Reporting Regime

This is considerably more rigorous than IMO guidance, which does not prescribe binding reporting timelines.

3.4.3 Enforcement, Audits, and Penalties

Unlike IMO, NIS2 includes legal enforcement mechanisms:

- On-site and off-site audits by national cyber authorities
- Administrative fines up to €10 million or 2% of global turnover
- Personal liability for management in cases of negligence
- Compulsory remediation orders and follow-up inspections

This means EU maritime organisations face a dual compliance burden:

- Flag/class verification under ISM/IMO
- Cyber authority enforcement under NIS2

3.4.4 Integration with Maritime OT and ICS Environments

For maritime operators, NIS2 intersects directly with onboard OT systems including:

- ECDIS and navigation suites
- Engine and power-management PLCs
- Cargo-handling systems
- Ballast-water treatment automation
- Safety systems (GMDSS, fire detection)
- SATCOM and remote-support platforms

NIS2 requires segmentation between IT and OT, monitored remote-access channels, secure update pathways, and supply-chain assurance for OEM software -areas not explicitly covered under IMO but essential for cyber resilience.

3.4.5 Relationship with IMO, SOLAS/ISM, and IACS

NIS2 complements the global IMO framework in the following ways:

- IMO/SOLAS/ISM → vessel-level safety and SMS integration
- NIS2 → enterprise, port, and digital infrastructure cybersecurity
- IACS UR E26/E27 → engineering design and technical requirements
- Class notations → verification and assurance

Together, they create a multi-layered regulatory architecture:

Global safety (IMO) → Regional cybersecurity (NIS2) → Technical enforcement (IACS) → Assurance (Class) → Operational governance (TMSA/DryBMS/RightShip).

3.5 IACS Unified Requirements E26 & E27

In 2022, the International Association of Classification Societies (IACS) introduced the Unified Requirements (URs) E26 and E27 [4][5], marking a significant step toward harmonized cyber resilience for ships and systems. IACS translated the IMO's strategic guidance into detailed technical requirements through the publication of URs E26 and E27, effective for all newbuilding contracts signed on or after 1 January 2024. Together, these URs form the engineering cornerstone of maritime cyber resilience, establishing a harmonised baseline across all IACS member societies.

- UR E26 [4]– Cyber Resilience of Ships addresses cyber risk management at the system and ship level. It requires shipbuilders and designers to implement secure network architectures, segregate critical control domains (such as propulsion, power management, and navigation), define access control and authentication procedures, and ensure recovery mechanisms for safety-critical systems. E26 thus ensures that cyber resilience is embedded as a design feature rather than an afterthought.
- UR E27 [5]– Cyber Resilience of Onboard Systems and Equipment complement E26 by focusing on the component level. It defines the expectations that individual systems—such as ECDIS, dynamic positioning, propulsion control, and cargo automation—must satisfy in terms of security hardening, patchability, data integrity, and communication protection. Compliance with E27 ensures that system suppliers and OEMs meet uniform cybersecurity expectations, reducing fragmentation across the supply chain.

Together, the two requirements form a dual-layer model; E26 governs the integration and interaction of systems on board, while E27 governs the resilience of the individual subsystems that constitute that network. This hierarchical alignment ensures that cybersecurity is treated both top-down (at the design and architecture level) and bottom-up (at the equipment and software level). The URs operationalise the IMO's MSC-FAL.1/Circ.3 and Resolution MSC.428(98) principles by translating policy objectives into measurable engineering criteria. They provide a common language for shipyards, equipment manufacturers, classification societies, and flag administrations, enabling consistent assessment across different vessel types and jurisdictions. Each IACS member society is obliged to incorporate these requirements into its own classification rules, ensuring uniform adoption within a specified timeframe.

The verification model introduced by UR E26 and E27 also represents a significant procedural innovation. Compliance is assessed during design approval, construction, and commissioning phases, with documented evidence of cyber risk assessments, network testing, and secure configuration management. This shifts cybersecurity assurance from post-delivery audits to a lifecycle validation model, embedding resilience from concept to operation. However, while the URs mark a landmark advance, they are not without limitations. Their scope applies only to newbuildings, leaving the vast existing global fleet—comprising tens of thousands of vessels—outside their mandatory remit. Moreover, while the URs define what must be achieved, they do not prescribe how, leaving interpretation and implementation details to individual class societies and shipyards. This flexibility allows adaptation but may also lead to variability in enforcement and maturity across different flags and builders.

Despite these constraints, the introduction of UR E26 and E27 signifies a structural transformation in maritime engineering philosophy: cybersecurity is no longer treated as an IT compliance function, but as a core safety attribute of vessel design. This transition underpins the broader paradigm shift from reactive compliance to resilience by design.

3.6 Class Notations

The International Association of Classification Societies (IACS) has mandated that cyber risk be addressed through class-specific guidelines aligned with IMO Resolution MSC.428(98). These schemes emerged as industry-led initiatives several years before the formalisation of the IACS Unified Requirements E26 and E27, responding to IMO MSC-FAL.1/Circ.3 (2017) and to industrial control-system standards such as IEC 62443 and NIST SP 800-82. By translating general regulatory guidance into auditable and verifiable criteria, class notations provided the maritime sector with its first structured mechanism for assessing cyber maturity. The following review summarises how each society operationalises those frameworks for OT risk management in shipping.

3.6.1 DNV – Cyber Secure Notation (Norway)

DNV's "Cyber Secure" scheme [47] is one of the most mature IACS implementations. It integrates IEC 62443 for technical segmentation and ISO/IEC 27001 / 27005 for information-security governance, structured around ISO 31000 principles of continuous improvement. Three notation levels -Basic, Advanced, and +- represent progressive compliance with IEC 62443 security levels. The notation mandates documented risk assessments within the ship's Safety Management System (SMS) under IMO MSC.428(98) and independent verification by DNV surveyors. Its strength lies in prescriptive OT requirements and life-cycle assurance; however, implementation can be resource-intensive for smaller operators (DNV, 2022; IEC, 2021; ISO, 2018).

3.6.2 ABS – FCI-CS Framework (United States)

The American Bureau of Shipping's Functional–Consequence–Impact Cyber Security (FCI-CS) framework [48] combines NIST SP 800-82 control-system guidance, IEC 62443 architecture, and ISO 31000 / 27005 risk-assessment methodology. It quantifies cyber risk through three axes: Functional impact, Operational consequence, and Business impact. This semi-quantitative model links technical vulnerabilities to safety and commercial outcomes, providing a defensible prioritisation method. The FCI-CS is widely applied in shipyards and newbuild projects where NIST's engineering logic aligns well with OT integration processes. Its limitation is the complexity of data collection required for consequence modelling (ABS, 2023; NIST, 2022).

3.6.3 Lloyd's Register – Digital Ship Notation (United Kingdom)

Lloyd's Register (LR) introduced its Digital Ship Notation [49] to certify cyber-secure digital platforms. It combines IEC 62443 technical controls with ISO/IEC 27001 and 27019 governance for energy and automation systems, structured under the NIST Cybersecurity Framework (CSF) five-function model. LR emphasises continuous assurance—requiring onboard network monitoring, incident logging, and vendor certification—bridging cyber and condition-based maintenance processes. Its strength is real-time verification across vessel digital twins; however, dependency on continuous connectivity can pose practical constraints during ocean passages (Lloyd's Register, 2023; ISO, 2017).

3.6.4 Bureau Veritas – Cyber Managed / Cyber Secure Notation (France)

Bureau Veritas (BV) applies a management-system approach integrating IEC 62443, ISO 27005, and NIST CSF into its Cyber Managed and Cyber Secure [50] notations. These frameworks embed cyber risk into the vessel's SMS and focus strongly on procedural maturity, crew awareness, and supplier control. BV's multi-tiered verification aligns with IMO MSC-FAL.1/Circ.3 guidelines and includes on-site audits for bridge, engine-room, and cargo control systems. The methodology is process-centric rather than purely technical, promoting continuous governance but relying on company culture for consistency (BV, 2022).

3.6.5 ClassNK – Cyber Security Guidelines for Ships (Japan)

Japan's ClassNK has issued the "Cyber Security Guidelines for Ships" (3rd edition, 2023) [51], combining IEC 62443, ISO 27001, and the NIST CSF. It introduces a life-cycle approach encompassing design, construction, and operation stages, supported by checklists for shipyards and vendors. The guidelines are coordinated with Japan's MLIT regulatory framework and integrate OT controls into the vessel certification process. Their comprehensive coverage makes them an effective baseline for Asian operators, though heavy documentation requirements can challenge smaller shipowners (ClassNK, 2023).

3.6.6 Korean Register (KR) – Cyber Security Guideline for Smart Ships (Korea)

The Korean Register framework targets next generation "smart ships." It merges IEC 62443, NIST SP 800-82, and ISO 31000 principles with safety-integrity-level (SIL) concepts from functional safety. KR defines Cyber Maturity Levels (CML 1–4) that parallel IEC 62443 Security Levels [52]. Its methodology emphasises network segmentation, secure software updates, and remote-operation resilience. The inclusion of SIL criteria links cyber events to physical safety outcomes, a valuable contribution for autonomous-ship design (KR, 2023; IEC, 2021).

3.6.7 RINA – Cyber Secure Notation (Italy)

The RINA Cyber Secure notation integrates ISO/IEC 27001, IEC 62443, NIST CSF, and ISO 22301 for business continuity [53]. It distinguishes between Design and Operational compliance phases, ensuring both shipyard and operator adhere to consistent security practices. The framework's hallmark is resilience planning—explicit requirements for backup, recovery, and incident-response capabilities. RINA's inclusion of ISO 22301 bridges cybersecurity and continuity management, but the notation is less prescriptive for technical OT controls.

3.6.8 Russian Maritime Register of Shipping (RS) – Cyber Safety Guidelines (Russia)

The RS Cyber Safety Guidelines (2021) adapt IEC 62443 and the Russian standard GOST R ISO/IEC 27001, embedding IMO MSC.428(98) compliance into national regulation [54]. RS emphasises network architecture, remote-access control, and system redundancy for offshore installations and Arctic vessels. Its prescriptive checklists support conformity audits but offer limited flexibility for innovative shipboard technologies.

3.6.9 Indian Register of Shipping (IRS) – Guidelines on Cyber Security for Ships (India)

The IRS Cyber Security Guidelines (2022) combine ISO 27001, IEC 62443, and NIST CSF, closely following IMO and BIMCO recommendations [5554]. The framework focuses on risk identification, awareness training, and governance within the ISM Code. IRS provides a practical compliance pathway for medium-sized shipping companies in emerging markets, prioritising procedural controls and vendor risk management over complex quantitative analysis.

3.6.10 China Classification Society (CCS) – Cyber Security Management System for Ships (China)

The CCS standard integrates IEC 62443, ISO 27001, and China's national network-security regulation GB/T 22239-2019 [56]. It underpins cyber-secure certification for smart and autonomous vessels under China's digital-ship initiative. The CCS approach blends industrial-control security with national data-

sovereignty requirements, enforcing both technical and regulatory compliance. It represents one of the few frameworks linking maritime cyber resilience with state-level cyber governance.

3.6.11 Observations and Comparative Analysis

1. Universal baseline: All IACS members align with IMO MSC.428(98), embedding cyber risk within the ISM Code.
2. Technical nucleus: IEC 62443 appears in every framework, confirming its status as the global OT standard.
3. Governance layer: ISO 27001 / 27005 and ISO 31000 provide risk-management structure and alignment with corporate processes.
4. Operational methodology: NIST SP 800-82 and NIST CSF supply control mapping and incident-response guidance.
5. Regional variation: European societies favour ISO integration, Asian societies blend national policy and smart-ship requirements, and the Americas adopt quantitative risk models.

Most classification societies, including ABS, DNV, and KR, apply the NIST Cybersecurity Framework (CSF) as a governance and maturity model while drawing on NIST SP 800-82 for technical guidance on securing industrial control systems. Thus, NIST CSF defines what risk-management processes must exist, whereas NIST SP 800-82 prescribes how these processes are technically implemented within shipboard OT environments. From an academic perspective, IACS frameworks embody a three-tier convergence model:

- Normative layer: ISO and IEC standards define controls and technical specifications.
- Procedural layer: NIST CSF and ISO 31000 define risk-management and response processes.
- Regulatory layer: IMO MSC.428(98) and ISM Code impose compliance and accountability.

Together, these layers form a hybrid governance–management–engineering model, transitioning maritime cybersecurity from static compliance to dynamic systems-engineering resilience and continuous assurance across the ship–shore interface.
The following matrix summarizes all IACS frameworks:

IACS Member	Framework / Notation	Underlying Standards & Models	Core Orientation & Features	Relevance to OT Risk Assessment
DNV (Norway)	**Cyber Secure Class Notation** (2022)	IEC 62443, ISO/IEC 27001 & 27005, ISO 31000, IMO MSC.428(98)	Maturity-tiered (Basic / Advanced / +) framework integrating technical and management controls. Independent verification and vessel-specific certification.	Defines security zones and conduits, risk governance, and verification audits across shipboard OT.
ABS (USA)	**FCI-CS – Functional, Consequence, Impact Cyber Security** (2023)	NIST SP 800-82, IEC 62443, ISO 31000 / 27005, IMO MSC.428(98)	Semi-quantitative model using F-C-I matrix for consequence-based risk assessment. Maps to NIST CSF functions.	Quantifies operational impact on navigation, propulsion, ballast, and communication systems.
Lloyd's Register (LR) (UK)	**Digital Ship & Cyber Secure Notation** (2023)	IEC 62443, ISO 27001 & 27019, NIST CSF, IMO MSC-FAL.1/Circ.3	Continuous assurance model with live monitoring, vendor certification, and digital-twin integration.	Promotes ongoing compliance and real-time risk monitoring for OT networks.
Bureau Veritas (BV) (France)	**CYBER MANAGED / CYBER SECURE Notation** (2022)	IEC 62443, ISO 27005, IMO MSC.428(98), NIST CSF	Management-system-driven approach; integrates cyber controls within Safety Management System (SMS).	Focuses on governance, crew awareness, and procedural defences for bridge and engine-room OT.
ClassNK (Japan)	**Cyber Security Guidelines for Ships (3rd ed.)** (2023)	IEC 62443, ISO 27001, NIST CSF, IMO MSC.428(98)	Aligned with Japan's Ministry of Land, Infrastructure, Transport & Tourism (MLIT) policies. Risk-based checklists for shipbuilders, owners, and vendors.	Covers full life cycle: design → construction → operation, with detailed OT asset inventories.
Korean Register (KR) (Korea)	**Cyber Security Guideline for Smart Ships** (2023)	IEC 62443, ISO 27001, ISO 31000, NIST SP 800-82	System-of-systems framework for smart-ship platforms, integrating safety and remote-operation systems.	Introduces hybrid model combining safety integrity levels (SIL) and cyber maturity levels (CML).

RINA (Italy)	**Cyber Secure / Ship Cyber Secure Notation** (2022)	ISO 27001, IEC 62443, NIST CSF, ISO 22301 (Business Continuity)	Focuses on resilience and recovery; integrates cyber continuity with safety management.	Emphasises risk treatment, business impact, and post-incident recovery for OT disruptions.
Russian Maritime Register of Shipping (RS)	**Cyber Safety Guidelines for Ships and Marine Installations** (2021)	IEC 62443, GOST R ISO/IEC 27001, IMO MSC.428(98)	Provides prescriptive control requirements for network architecture and remote-access policies.	Targets shipyards and offshore installations; OT-centric with national standards alignment.
Indian Register of Shipping (IRS)	**Guidelines on Cyber Security for Ships** (2022)	ISO 27001, ISO 31000, IEC 62443, NIST CSF	Focuses on risk identification and mitigation aligned with IMO circulars and BIMCO guidelines.	Promotes awareness, governance, and compliance audits for mixed IT/OT infrastructures.
China Classification Society (CCS)	**Cyber Security Management System for Ships – CCS Notations** (2023)	IEC 62443, GB/T 22239-2019 (China Network Security Standard), ISO 27001, IMO MSC.428(98)	Incorporates national cybersecurity law with international standards. Risk assessment tied to digital-ship projects and autonomous vessels.	Adapts IEC 62443 principles to Chinese maritime digitalisation frameworks.

Table 3.5 – IACS Member Cybersecurity Frameworks and Notations

3.7 BIMCO Guidelines and Contractual Instruments

BIMCO (Baltic and International Maritime Council) plays a pivotal role in bridging regulatory expectations with operational and commercial implementation. It has produced two key instruments widely recognised as industry benchmarks:

- BIMCO Guidelines on Cyber Security Onboard Ships (5th Edition, 2024) – developed in collaboration with ICS, INTERCARGO, and INTERTANKO, these guidelines provide detailed methodologies for conducting cyber risk assessments, implementing network segregation, managing software updates, and preparing response plans. They serve as practical guidance for complying with IMO MSC-FAL.1/Circ.3 and integrating cybersecurity into the SMS (BIMCO, 2024).
- BIMCO Cyber Security Clause (2021) – a contractual provision incorporated into charter parties, ship management, and supply agreements. The clause allocates responsibilities, defines due diligence obligations, and outlines cooperation requirements in the event of a cyber incident (BIMCO, 2019).

Together, these initiatives extend cybersecurity governance from the technical and organisational domains into the legal and commercial sphere, ensuring that cyber risk is addressed as both a safety and liability issue. BIMCO's frameworks thus complement IMO and IACS guidance by embedding cyber resilience in day-to-day operations and contractual relationships.

3.8 Sectoral Management and Vetting Frameworks

Alongside regulatory and class-based frameworks, the maritime industry has established a complementary ecosystem of sectoral management and vetting programs that integrate cyber risk management into daily operations and corporate governance. These frameworks—TMSA, DryBMS, and RightShip's Digital Safety Management and Safety Score—operate as soft-law mechanisms that drive compliance through commercial incentives. Although voluntary, adherence to them is effectively mandatory in practice, since a company's participation and performance directly influence its chartering prospects, vetting approval, and reputational standing.

Together, TMSA, DryBMS, and RightShip's DSM/Safety Score form a cohesive market-based enforcement layer that bridges the gap between statutory compliance and operational performance. They extend the intent of IMO MSC-FAL.1/Circ.3 and the ISM Code into the managerial sphere while complementing the design-level assurance provided by IACS UR E26/E27 and class notations.
Although these systems remain voluntary frameworks, their combined influence has effectively made cybersecurity a precondition for market participation. Through charterer expectations, insurance incentives, and reputation effects, they have driven the industry toward a culture where cyber resilience is recognised as a core component of operational excellence and corporate governance.

3.8.1 OCIMF – Tanker Management and Self-Assessment (TMSA 4)

The Tanker Management and Self-Assessment (TMSA) program, maintained by the Oil Companies International Marine Forum (OCIMF), provides the principal management framework for the tanker sector. Structured around fourteen "Elements" of operational excellence, it promotes continual improvement in safety, environmental protection, and security. Within TMSA 4 (OCIMF, 2022), cyber risk management is explicitly incorporated into Element 13 (Security Management) and Element 14 (Maritime Security). Operators must implement a documented cyber policy within the Safety Management System (SMS), undertake regular IT/OT risk assessments, and establish controls for vendor and remote access. Further requirements include crew awareness training, cyber-incident drills, and formal post-incident learning.

Evidence of compliance -risk registers, configuration-change records, access logs, and incident reports-is reviewed during vetting inspections conducted by oil majors. As a result, TMSA functions as a commercial enforcement mechanism: a low cyber-maturity score may restrict access to lucrative charter opportunities. Nevertheless, the framework's self-assessment nature introduces subjectivity, and its reliance on documentary evidence limits the degree of technical validation of shipboard control systems. Despite these constraints, TMSA has become one of the most effective instruments for embedding cyber governance and accountability within tanker-fleet operations.

3.8.2 INTERCARGO & RightShip – Dry Bulk Management Standard (DryBMS)

The Dry Bulk Management Standard (DryBMS), jointly developed by INTERCARGO and RightShip, extends similar governance principles to the dry-bulk sector. Comprising twenty "Elements," it defines a structured pathway for safety and performance improvement, with cybersecurity integrated under Element 12 (Security).

DryBMS requires operators to maintain a cyber policy aligned with the SMS, perform IT/OT-inclusive risk assessments, and establish robust controls for remote access, software updates, and supply-chain management. It also emphasises crew competence, training, and periodic internal audits that evaluate cyber preparedness.

The framework has filled a long-standing regulatory vacuum for older bulk carriers not covered by newer technical rules. Because DryBMS is directly linked with RightShip's inspection and vetting system, its adoption provides tangible commercial benefits, improving operator reputation and marketability. Yet, it remains voluntary and self-declared; assessment results depend heavily on management interpretation and lack external verification. Even so, DryBMS has created a sector-specific baseline for cyber governance and strengthened the alignment between operational practices and the IMO's and ISM Code's expectations.

3.8.3 RightShip – Digital Safety Management (DSM) and Safety Score

RightShip's Digital Safety Management (DSM) platform and its associated Safety Score constitute the industry's first attempt to quantify safety and cyber resilience through data analytics. The DSM model aggregates documentary evidence—cyber policies, risk assessments, vendor controls, and incident records—alongside inspection data and DryBMS submissions to evaluate an operator's cyber-governance maturity.

Cyber indicators are integrated into the overall Safety Score, which is used by charterers, financiers, and insurers as a proxy for operational reliability. A weak cyber profile can reduce an operator's score, affecting chartering potential and insurance premiums. In this way, RightShip transforms cyber maturity into a measurable market variable, making cybersecurity performance a determinant of commercial success.

However, DSM and the Safety Score face limitations. Their scoring algorithms are proprietary, the weighting of cyber criteria within the composite score is not publicly disclosed, and evaluations rely largely on documented evidence rather than direct technical testing. Nonetheless, they represent a significant innovation in data-driven governance, enabling the quantification of cyber resilience and fostering competition toward higher safety standards.

3.9 Synthesis of Framework Interactions

The current maritime cybersecurity governance architecture is multi-layered, interdependent, and evolving toward convergence. Each framework—regulatory, technical, assurance, operational, and cross-sectoral—addresses a distinct aspect of the cyber-resilience continuum. Together, they form a complex but complementary ecosystem that combines mandatory regulation, voluntary assurance, and commercial enforcement mechanisms.

Table 3.1 – Vessel Types and Framework Applicability Summary summarises the relationship between the main frameworks examined in this chapter, highlighting their domain, cyber-integration focus, and regulatory or market nature. The maritime cybersecurity governance ecosystem operates through five interdependent layers:

Layer	Frameworks	Primary Function	Nature of Enforcement
Regulatory	IMO (ISM Code, MSC-FAL.1/Circ.3)	Policy and safety integration	Mandatory (via flag states)
Technical / Engineering	IACS UR E26 & E27	Cyber resilience by design	Mandatory (newbuilds ≥ 2024)
Assurance	Class Notations (DNV, ABS, LR, BV, RINA)	Technical verification and certification	Voluntary but market-driven
Contractual	BIMCO Cyber Clause	Allocation of risk and duty of care	Voluntary but legally binding
Operational / Commercial	TMSA, DryBMS, RightShip DSM	Continuous performance and vetting	Voluntary but commercially enforced

Table 3.2 – Regulatory and Industry Framework Integration Matrix

3.9.1 Analytical Integration

The frameworks form a governance continuum:

- IMO defines what must be achieved, policy and safety intent.
- IACS and Class define how it must be engineered and verified.
- BIMCO defines how it is contractually allocated.
- TMSA, DryBMS, and RightShip define how it is operationally monitored and rewarded.

3.9.2 Identified Gaps – Structural Weaknesses in the Governance Chain

Despite significant progress, several systemic deficiencies persist that undermine the coherence of this continuum.

1. **Legacy Fleet Coverage:** The IACS URs apply only to newbuilds contracted after 2024, leaving over 90 % of the global fleet outside formal design-level regulation. Retrofitting cybersecurity into legacy OT systems is constrained by certification stability, vendor dependency, and economic feasibility. Without a retrofit compliance pathway, the industry risks a two-tier cyber landscape—modern ships with regulated resilience and legacy vessels relying on ad hoc defences.
2. **Audit Fragmentation:** Vessels often undergo multiple overlapping audits—ISM verification, class surveys, TMSA assessments, RightShip inspections—each with distinct criteria and evidence expectations. This redundancy increases administrative burden while generating inconsistent audit outcomes, as there is no shared taxonomy for cyber maturity. Some operators therefore "audit to the audience" rather than to objective risk outcomes.
3. **Supply-Chain Governance:** Cyber resilience is only as strong as its weakest supplier. Engine, ECDIS, and communication vendors frequently maintain proprietary software with opaque security postures. Neither IMO nor IACS frameworks currently impose verifiable vendor-assurance obligations beyond manufacturer self-declaration, leaving a critical gap in lifecycle control.

4. **Metric Inconsistency:** Current frameworks use incompatible maturity scales—TMSA employs qualitative levels (1-4), class notations use binary compliance, and BIMCO relies on subjective "reasonable measures." The absence of standardised Key Cyber Risk Indicators (KCRIs) prevents benchmarking across fleets, hindering insurers, financiers, and regulators from quantifying systemic exposure.
5. **Information-Sharing Deficiency:** There is limited feedback between flag administrations, classification societies, and industry vetting platforms. Cyber incident data are rarely aggregated or anonymised for learning due to liability fears and confidentiality clauses. Consequently, risk assessment remains reactive and case-based, restricting evidence-based policy evolution.

Analytically, these deficiencies are not random but structural: they occur at the junctions between governance layers—policy vs. engineering, assurance vs. contract, and contract vs. operations. Addressing them requires a cross-domain framework capable of aligning technical verification, regulatory oversight, and commercial incentives under common metrics.

3.9.3 Toward Harmonised Governance – The Case for a Maritime Cyber Resilience Code

To overcome fragmentation, scholars and industry bodies increasingly advocate a Maritime Cyber Resilience Code (MCRC)—a unified framework integrating regulatory, technical, and operational layers under a single lifecycle model. Conceptually, such a code would function similarly to the ISM Code, establishing mandatory cyber-resilience principles applicable to both new and existing tonnage.

Core Components of a Future MCRC

1. Policy Integration: Formal incorporation of cyber resilience within SOLAS or the ISM Code, providing statutory authority for enforcement.
2. Technical Baseline: Adoption of IACS UR E26/E27 and IEC 62443 principles as universal design and maintenance standards.
3. Assurance Convergence: Recognition of class notations through mutual-acceptance protocols, ensuring audit equivalence and reducing redundancy.
4. Operational Continuity: Alignment with TMSA and DryBMS to maintain consistency between design compliance and day-to-day operation.
5. Data and Metrics Framework: Establishment of standardised maturity indices and anonymised incident-reporting mechanisms feeding into flag and class analytics.

4 OT Cyber Risk Assessment Methodology

4.1 Framework Selection

This chapter presents the methodology developed for assessing cyber risks in shipboard Operational Technology (OT) systems. Unlike traditional IT risk management processes, OT systems in the maritime domain operate under real-time, safety-critical conditions and strict availability requirements. Consequently, cyber-risk assessment for vessels must integrate technical system analysis with organizational and regulatory objectives.

The methodology builds directly on the regulatory and theoretical bases established in the previous chapters. It aims to provide a structured, repeatable, and auditable process for analysing cyber risks in maritime OT environments, where failures can compromise safety, environmental protection, or voyage continuity.

To achieve this, the proposed approach adopts a hybrid framework that combines three complementary international standards:

1. IEC 62443 – for technical system segmentation, control zones, and defence-in-depth architecture.
2. NIST SP 800-82 – for operational lifecycle management aligned with the NIST Cybersecurity Framework (Identify–Protect–Detect–Respond–Recover).
3. ISO 31000 – for structured risk identification, evaluation, treatment, and review.

These frameworks were selected because each addresses a distinct layer of maritime OT cybersecurity. IEC 62443 ensures technical robustness, NIST SP 800-82 provides operational applicability, and ISO 31000 secures governance and decision-support integration. Together they create a methodology that is both technically credible and organizationally practical for the shipping industry.

4.2 Risk Assessment Steps for Shipboard OT Systems

4.2.1 Asset Identification

The first step is to identify and classify OT assets across shipboard domains, including:

- Navigation systems (ECDIS, GPS, AIS, radar integration)
- Propulsion and engine control systems (Main Engine Control, PLCs, VDR)
- Ballast and cargo management systems (pumps, valves, tank-level sensors)
- Communication systems (satellite links, GMDSS, ship–shore data exchange)
- Auxiliary systems (HVAC, power management, alarm monitoring)

Each asset is evaluated for its criticality, connectivity, and exposure to IT or external networks. This process forms the foundation for defining zones and conduits under IEC 62443-3-2. An Asset Register and Data Flow Diagram (DFD) are developed to visualise interdependencies and communication paths. These artefacts are created during the asset-identification phase by the vessel's technical management team, often in cooperation with the cybersecurity assessor and ship's automation personnel. Their development does not rely on pre-existing documents but is built from both technical sources and operational insights gathered throughout the assessment. Information is collected from system schematics, automation manuals, and network topology drawings, and supplemented with interviews of crew, OEM engineers, and system integrators. This ensures that both visible and hidden interconnections are captured—including remote maintenance links, Wi-Fi bridges, or shared operator terminals. Because most vessels do not maintain a detailed digital inventory, the Asset Register is often constructed manually using spreadsheets or CMDB-style templates. It catalogues each OT component (hardware, software, and network devices) with details such as:

- Function and operational domain

- Physical location
- Network address and interface
- Criticality and redundancy level
- Assigned IEC 62443 security zone

The Data Flow Diagram (DFD) is developed in parallel to illustrate how data moves between these zones and conduits. Using tools such as Microsoft Visio, Draw.io, or Lucidchart, it maps interfaces between navigation, propulsion, and communication systems. The DFD highlights communication dependencies and potential exposure points—forming the analytical basis for applying the STRIDE threat-modelling framework in the next stage. This documentation process is consistent with IEC 62443-3-2 (system zoning and conduit identification), NIST SP 800-82 (asset inventory and control-system mapping), and IMO MSC-FAL.1/Circ.3 (Step 1: Identify systems, assets, and data critical to operations). Developing these artefacts early provides traceability for all subsequent steps—linking each asset to its potential threats, vulnerabilities, and mitigation measures.

4.2.2 Threat Modelling

The second step in the OT cyber-risk assessment process is Threat Modelling, which identifies and categorizes potential attack vectors that may exploit vulnerabilities in shipboard control systems. In this methodology, threat modelling is performed using the STRIDE framework, adapted specifically for maritime Operational Technology (OT) environments. STRIDE provides a structured, repeatable, and comprehensive approach for identifying threats across six fundamental categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Originally developed for IT systems by Microsoft, STRIDE is flexible and can be effectively applied to OT systems, especially when combined with the architectural and process models of IEC 62443 and NIST SP 800-82.

Application of STRIDE in Maritime OT Systems

Each STRIDE category is contextualized to the shipboard environment as follows:

STRIDE Category	Example in Maritime OT Context	Potential Consequence
Spoofing	Manipulation of GPS or AIS signals to transmit false position or identification data.	Navigation error, collision hazard, route deviation.
Tampering	Unauthorized modification of PLC parameters, firmware, or control logic.	Machinery malfunction, propulsion failure, or cargo-handling error.
Repudiation	Lack of system logging or user traceability for maintenance or remote access sessions.	Inability to determine cause or accountability after an incident.
Information Disclosure	Leakage of operational or voyage data via satellite, Wi-Fi, or vendor maintenance connections.	Competitive or regulatory exposure, loss of confidentiality.
Denial of Service (DoS)	Flooding of bridge or engine room networks, jamming of communication channels.	Disruption of monitoring or control functions, potential loss of situational awareness.
Elevation of Privilege	Malware or a threat actor gaining administrative access to control systems.	Full compromise of automation and safety systems, long-term persistence.

Table 4.1 – STRIDE Categories Contextualised to the Shipboard OT Environment

Rationale for Selecting STRIDE

STRIDE is selected as the core threat modelling approach because it provides systematic coverage of the main cyber-threat dimensions without requiring extensive modelling data or computational tools. This makes it especially suitable for the shipboard OT context, where:

- Network visibility is limited due to vendor-specific architectures,
- Access to live systems is constrained by safety regulations, and
- Resources for detailed simulation or penetration testing may be unavailable.

The framework's logic is simple yet powerful — by analysing each data flow and component from the perspective of the six STRIDE categories, the assessor ensures that no major threat class is overlooked. For instance, analysing an ECDIS-to-GPS link under STRIDE reveals possible Spoofing and Information Disclosure risks, while examining a PLC update process identifies Tampering and Elevation of Privilege vectors. Furthermore, STRIDE aligns naturally with both IEC 62443 and NIST SP 800-82 principles:

- Under IEC 62443, STRIDE supports the "security level target definition" process, by associating specific threat categories with the criticality of zones and conduits.
- Within NIST SP 800-82, STRIDE complements the Identify–Protect–Detect–Respond–Recover lifecycle, by enriching the Identify and Protect phases with detailed threat understanding.

The framework also supports IMO MSC-FAL.1/Circ.3, which requires a "systematic identification of threats to critical systems and data." By focusing on operationally relevant examples, such as GNSS spoofing, network tampering, or DoS on automation buses, the method ensures both regulatory compliance and technical realism.

Integration with the Overall Methodology

The STRIDE process is applied directly to the Asset Register and Data Flow Diagram (DFD) developed in Section 4.2.1. Each data flow and control interaction is examined for potential threats under each STRIDE category. For example:

- The communication path between ECDIS and GPS is analysed for Spoofing and Information Disclosure risks.
- The interface between Propulsion PLCs and the alarm-monitoring system is examined for Tampering or Denial of Service.

The identified threats are documented in a Threat Register, including the affected asset, threat type, potential impact, and possible mitigations. This documentation forms a critical input for the Vulnerability Analysis stage, ensuring that subsequent risk evaluation (Section 4.2.3 and 4.2.4) is grounded in verified operational contexts.

4.2.3 Vulnerability Analysis

Following the identification of threats through the STRIDE framework, the next step in the methodology is to conduct a Vulnerability Analysis. This process determines which weaknesses could realistically be exploited by the threats identified in Section 4.2.2, establishing the foundation for risk calculation and prioritisation. Vulnerability analysis in maritime OT environments requires both technical investigation and operational understanding, since shipboard systems often include legacy components, proprietary configurations, and vendor-managed maintenance channels.

Purpose and Scope

The objective of the vulnerability analysis is to:

1. Identify exploitable weaknesses within each OT system or data flow.
2. Map these weaknesses to relevant STRIDE threat categories.
3. Assess the adequacy of existing controls and determine residual exposure.

The process focuses on both cyber-technical and human-organisational vulnerabilities, reflecting the complex nature of maritime operations where human action, procedural discipline, and technology interact continuously.

Method and Data Sources

The analysis begins by cross-referencing the assets and data flows identified earlier with known vulnerability repositories and contextual shipboard information. Common sources include:

- Common Vulnerabilities and Exposures (CVE) database, for software and firmware vulnerabilities.
- ICS-CERT and US-CISA advisories, focusing on industrial control system threats.
- Vendor and classification society bulletins, such as DNV Cyber Secure, ABS CyberSafety, or Lloyd's Register CyberSecure.
- System documentation and maintenance logs, revealing unpatched components or unsupported operating systems.
- Crew interviews and onboard observations, which often expose procedural gaps such as shared credentials, outdated antivirus software, or disabled security features.

Each vulnerability is reviewed to determine:

- The affected asset or subsystem (as defined in the Asset Register),
- The threat(s) it corresponds to (from the STRIDE analysis), and
- The potential impact on operations, safety, and compliance.

Vulnerability Categorisation

For systematic evaluation, vulnerabilities are grouped into three main categories:

Category	Description	Typical Maritime OT Examples
Technical Vulnerabilities	Hardware or software flaws that can be directly exploited.	Outdated firmware, unpatched PLCs, default passwords, insecure Modbus/Telnet services.
Organizational Vulnerabilities	Weaknesses in governance or management structures.	No defined OT security policy, lack of network monitoring, poor coordination between ship and shore.
Procedural Vulnerabilities	Gaps in day-to-day operational routines.	Infrequent patching, uncontrolled USB usage, unverified remote vendor access.

Table 4.2 – OT Vulnerability Categories

This classification enables the organization to determine whether mitigation requires technical remediation, training and governance improvements, or process redesign.

Analytical Process

The vulnerability analysis is performed collaboratively by the cyber-risk assessor, technical superintendent, and ship's chief engineer or automation officer. Each identified threat from STRIDE is

reviewed to determine whether the underlying system exhibits a corresponding vulnerability. For example:

- A Tampering threat against a propulsion control PLC may map to a vulnerability such as “unpatched vendor firmware” or “no code integrity verification.”
- A Denial-of-Service threat targeting bridge networks may correspond to “no network segmentation” or “no QoS prioritisation.”
- An Information Disclosure threat via satcom may relate to “unencrypted ship–shore communication” or “shared user credentials.”

The process links each STRIDE threat with a concrete, evidence-based vulnerability, creating traceability throughout the methodology. This traceability is essential for demonstrating compliance during class audits or IMO ISM inspections.

Relation to Standards

The vulnerability analysis process is directly supported by international frameworks:

- IEC 62443-3-2 mandates the identification of vulnerabilities and assessment of existing security measures within defined zones and conduits.
- NIST SP 800-82 recommends continuous vulnerability monitoring and documentation as part of the ICS security lifecycle.
- IMO MSC-FAL.1/Circ.3 identifies vulnerability assessment as a core step in maritime cyber risk management, emphasising both technical and procedural aspects.

By following these standards, the methodology ensures that the analysis is both technically defensible and regulatorily compliant.

Deliverables and Outcomes

The main outputs of this phase are:

1. A Vulnerability Register, listing each asset, identified vulnerabilities, affected threat categories, and severity level.
2. A Vulnerability Matrix, mapping the relationship between STRIDE threats and specific weaknesses.
3. An initial Control Effectiveness Rating, used as input for the risk calculation stage (Section 4.2.4).

Together, these deliverables allow for an evidence-based and auditable transition from threat identification to quantitative risk evaluation.

Analytical Note

Vulnerability analysis in maritime OT systems must balance depth and feasibility. Because shipboard systems are often vendor-protected and difficult to test directly, assessors rely heavily on documentation review, vendor disclosures, and configuration inspection rather than intrusive scanning. This limitation reinforces the need for a well-defined methodology—such as the one presented here—where STRIDE threats and identified vulnerabilities are systematically linked. The result is a traceable, risk-driven view of OT exposure, enabling maritime operators to prioritise controls that deliver the greatest reduction in operational risk.

Identified assets and threats are cross-referenced with known vulnerabilities using maritime-specific and industrial databases such as:

- Common Vulnerabilities and Exposures (CVE)
- ICS-CERT advisories
- Class and manufacturer security bulletins (e.g., DNV Cyber Secure, ABS CyberSafety)

The assessment includes configuration weaknesses, outdated firmware, unsecured protocols (e.g., Modbus, NMEA 0183), and human factors (e.g., weak password management, lack of training). Vulnerabilities are categorized according to technical, organizational, and procedural controls.

4.2.4 Risk Calculation

The next step of the methodology is Risk Calculation, which quantifies the level of cyber risk associated with each identified threat and vulnerability pair. Where the STRIDE framework and vulnerability analysis determine what can go wrong and how, risk calculation establishes how serious the outcome would be and how likely it is to occur. This quantitative approach ensures that risk management decisions are evidence-based, comparable, and auditable.

Purpose

Risk calculation transforms qualitative findings into a structured numerical or semi-quantitative model, allowing operators to:

1. Prioritise mitigation actions based on exposure and impact.
2. Justify security investments to management and regulators.
3. Demonstrate compliance with international standards such as ISO 31000 and IMO MSC-FAL.1/Circ.3.

The process also aligns with IEC 62443-3-2, which requires documented evaluation of risk as part of the “Security Risk Assessment” and with NIST SP 800-30, which defines risk as a function of likelihood and impact.

Methodology

Each risk is calculated using the well-established formula:

$$R = L \times I$$

where:

- L (Likelihood): The estimated probability that a specific threat will exploit a given vulnerability, considering system exposure, control effectiveness, and known threat activity.
- I (Impact): The expected consequence if the threat were realised, expressed in terms of its effect on safety, operational continuity, environment, and business performance.

Both parameters are typically rated on a 1–5 scale, though a 1–10 scale may be used for higher resolution in complex systems. To maintain consistency, the same criteria should be applied across all assets and vessels in a fleet.

Scoring Model

Score	Likelihood Description	Impact Description
1 (Very Low)	Rare; requires multiple unlikely conditions or advanced capabilities.	Negligible; minor inconvenience, no operational loss.
2 (Low)	Possible but uncommon; limited exposure or access.	Minor; temporary disruption with quick recovery.
3 (Medium)	Occasional; realistic attack vector under moderate conditions.	Noticeable; partial loss of function, no safety incident.

4 (High)	Likely under normal operating conditions; known exploit available.	Major; safety risk, environmental or cargo impact.
5 (Very High)	Almost certain; ongoing active threats or recurring vulnerability.	Critical; catastrophic system or safety failure.

Table 4.3 – Context-Aware Vulnerability Index (CVI) Scoring Model

The Risk Score (R) is then obtained by multiplying the two values. For instance, a Tampering threat (L = 4) leading to propulsion shutdown (I = 5) yields R = 20, classed as Critical.

Risk Matrix

The results are visualised using a Risk Matrix, allowing decision-makers to understand priorities briefly.

Likelihood ↓ / Impact →	**1**	**2**	**3**	**4**	**5**
5 (Very High)	M	H	H	C	C
4 (High)	M	M	H	H	C
3 (Medium)	L	M	M	H	H
2 (Low)	L	L	M	M	H
1 (Very Low)	L	L	L	M	M

Table 4.4 – Risk Assessment Matrix (Likelihood vs Impact)

Legend**:** L = Low, M = Medium, H = High, C = Critical

This matrix can be digitalised through spreadsheets or risk-management software, forming the backbone of the Cyber Risk Register. For each risk, contextual data (asset, threat, vulnerability, control, likelihood, impact, residual risk) are recorded for auditability.

Assessment Process

The calculation process is typically carried out by the cyber-risk assessor in cooperation with the vessel's technical superintendent and chief engineer. Together they review each STRIDE-based threat and mapped vulnerability, determine its likelihood and impact based on:

- Operational dependency (criticality of the affected system),
- Control strength (effectiveness of existing safeguards), and
- Exposure (network connectivity, remote access, or vendor dependencies).

For example:

- A Spoofing threat on GPS affecting ECDIS navigation may have high impact and medium likelihood, giving R = 15 (High).
- A Denial-of-Service threat on the crew Wi-Fi network may have low impact despite a high likelihood, giving R = 8 (Medium).

This structured evaluation ensures transparent and consistent scoring across different vessel types and operational contexts.

Outputs and Deliverables

The key deliverables of the risk calculation step are:

1. A Risk Register – documenting all identified risks with likelihood, impact, and calculated scores.
2. A Risk Matrix – summarising the distribution of risk levels across shipboard systems.
3. A Preliminary Treatment Plan – identifying which risks exceed the organisation's tolerance threshold and require mitigation.

These outputs provide the foundation for risk prioritisation and treatment (Section 4.2.5) and serve as documentary evidence for class or flag-state audits.

4.2.5 Risk Prioritization and Treatment

Risks above the acceptable threshold are prioritized for mitigation. The risk treatment process includes:

- Risk avoidance: e.g., disabling non-essential network services
- Risk reduction: implementing technical controls such as network segmentation, access management, patching
- Risk transfer: via cyber insurance or third-party service outsourcing
- Risk acceptance: for low-impact, low-likelihood scenarios, with documented justification

Treatment actions are aligned with IEC 62443-3-3 security requirements and IMO ISM Code cyber integration. Periodic re-assessment is recommended at least annually, or after any major system update, dry-dock, or new equipment installation. The output is a Residual Risk Profile and an updated Cyber Risk Register, serving as an auditable record for compliance with DryBMS, RightShip, and TMSA Element 13.

4.3 Summary

This methodology enables a structured, repeatable, and auditable process for evaluating cyber risks in shipboard OT environments. By merging IEC 62443's architectural rigor with NIST's risk management functions, the framework bridges technical and regulatory requirements-promoting resilience, compliance, and continuous improvement in maritime cyber risk management.

5 Application and Analysis of the OT Cyber Risk Assessment

5.1 Introduction

This chapter applies the hybrid cyber-risk assessment methodology developed in Chapter 4 to a representative shipboard Operational Technology (OT) environment. The methodology integrates IEC 62443-3-2 zone/conduit modelling, NIST SP 800-82 industrial-control system guidance, ISO 31000 risk governance principles and the cyber-resilience requirements of IACS UR E26/E27 into a unified and structured workflow.

To ensure analytical coherence, the hybrid framework proceeds through six sequential stages:

1. OT Asset Identification – establishing system boundaries, functional roles and zone allocations.
2. STRIDE Threat Modelling – identifying spoofing, tampering, repudiation, information disclosure, denial-of-service and privilege-escalation vectors for each asset.
3. CVI-based Vulnerability Assessment – combining exploitability, operational exposure and systemic-impact potential into a quantitative Cyber Vulnerability Index.
4. Weighted Risk Evaluation (Rw) – applying ISO 31000-aligned likelihood, impact and detectability scoring.
5. Interdependency and Heat-Intensity Analysis (H_v) – quantifying the systemic propagation potential of each asset using connectivity weighting consistent with IEC 62443 and IACS UR E26.
6. Governance and Continuous Assurance – interpreting results in the context of operational procedures and regulatory compliance expectations (ISM Code, IMO MSC-FAL.1/Circ.3).

Applied in combination, these stages enable a coherent evaluation of both local asset-level weaknesses and system-wide cyber-physical propagation risk, providing a complete and auditable model of the vessel's OT cyber-risk landscape.

5.2 Case-Study Context

The case study models a Panamax dry-bulk carrier, which serves as an analytically suitable platform for several reasons.

- ✓ First, as articulated in Chapter 3 (Vessel Types and Operational Profiles), bulk carriers operate with a medium level of automation density: sophisticated enough to expose systemic risk pathways, yet not so over-engineered that control segmentation is fully mature.
- ✓ Second, bulk carriers operate under a typical tramp trading model, meaning it calls at irregular ports without fixed schedules, often interfacing with diverse and inconsistent digital infrastructures. This operational variability leads to increased cyber-exposure compared to liner vessels with predictable routes and stable connectivity conditions.
- ✓ Third, unlike highly digitised container or passenger ships, bulk carriers often retain a mix of legacy and modern OT, making them representative of the current state of the global fleet, where mixed-generation equipment is ubiquitous.

The vessel's architecture is characterized by the interaction of three major OT domains:

1. Navigation and Bridge Systems
2. Engine, Machinery, and Propulsion Control
3. Cargo, Ballast and Auxiliary Automation

These domains are connected through a segmented but interdependent OT network. Below is the complete architecture overview used for the assessment.

5.2.1 OT Network Architecture Diagram

The diagram includes:

Bridge Network (VLAN 10)

- **GNSS/GPS receiver**

  Function: Provides absolute position, timing, and velocity data to ECDIS, AIS, autopilot, radars, and VDR. The GNSS/GPS receiver provides the vessel's primary electronic position-fixing input and supplies SOG, COG, and UTC timing to ECDIS, AIS, radars, autopilot, and the VDR. As a SOLAS-mandated system, it forms the root of the navigation data chain, meaning that any spoofing, jamming, or manipulation of GNSS signals propagates to all downstream systems, distorting situational awareness, route monitoring, and collision-avoidance decisions. Its lack of signal authentication makes GNSS a high-risk cyber-physical target.

  Cyber-physical behaviour:

  - GPS spoofing or jamming injects incorrect position/velocity vectors, distorting route calculations and situational awareness.
  - All downstream systems inherit corrupted data, making GPS the *root node* of the navigation data chain.

  Dependencies: Feeds ECDIS, AIS, autopilot, radars, VDR.

  Safety relevance: SOLAS-mandated; compromise can lead to course deviation or grounding.

- **Gyrocompass**

  Function: Provides heading reference to radars, ECDIS, autopilot, and VDR. The gyrocompass provides the vessel's primary true heading reference and is used by radars, ECDIS, AIS, autopilot, and the VDR. As the sole source of heading data, the gyrocompass is critical for Automatic Radar Plotting Aid (ARPA)[1] vector calculations, route tracking, collision avoidance, and autopilot steering. Under SOLAS V/19, a heading reference system is mandatory for all SOLAS-class vessels, making the gyrocompass a safety-critical asset. Due to its use of unauthenticated serial or network protocols (e.g., NMEA 0183/2000), the gyrocompass is highly susceptible to spoofing and data-manipulation attacks, which can propagate to all downstream navigation systems. It is therefore assigned high systemic impact within the OT risk matrix.

  Cyber-physical behaviour:

  - Heading manipulation creates bearing drift on radars, corrupting ARPA vectors.
  - Autopilot uses gyro as primary input → steering instability if compromised.

  Dependencies: Direct feed into radars and autopilot.

  Safety relevance: SOLAS-mandated; integral to collision avoidance; high-value target in cyber-physical attacks.

- **Doppler speed log**

  Function: The Doppler speed log measures speed through water and provides STW data to radars, ECDIS, and the VDR. As a SOLAS-mandated device, it is central to the vessel's ARPA calculations and manoeuvring decisions. Because STW feeds directly into CPA/TCPA prediction, any speed falsification—whether through NMEA spoofing or network manipulation—produces inaccurate collision-avoidance vectors and undermines ECDIS route monitoring accuracy.

  Cyber-physical behaviour:

[1] ARPA is a radar-based system that automatically detects targets, tracks their motion, computes their course and speed, predicts collision risk, and displays vectors and avoidance information. It is part of modern marine radar systems and is required on most SOLAS vessels.

- Incorrect speed affects Closest Point of Approach (CPA)[2]/Time to Closest Point of Approach (TCPA)[3] calculations and voyage planning accuracy.
- ARPA systems lose accurate vector prediction.

Dependencies: Used by radars, ECDIS, VDR.

Safety relevance: SOLAS-mandated; vital for manoeuvring decisions in restricted waters.

- **Echo sounder**

  Function: The echo sounder supplies depth-below-keel measurements to ECDIS and the VDR and supports grounding-avoidance logic. As a SOLAS-mandated instrument, it represents a key safety barrier during restricted-water navigation. Because most echo sounders transmit unauthenticated NMEA data, cyber manipulation can suppress shallow-water warnings, disable ECDIS safety-contour alarms, and increase the risk of grounding.

  Cyber-physical behaviour:

  - False depth readings disable ECDIS grounding alarms.
  - Manipulation may encourage unsafe manoeuvres in shallow waters.

  Dependencies: Feeds ECDIS and VDR.

  Safety relevance: SOLAS-mandated grounding-prevention equipment

- **AIS transponder**

  Function: AIS broadcasts the vessel's identity, position, course, speed, and navigational status while receiving the same information from surrounding ships. As a SOLAS-mandated communication system, AIS supports collision avoidance, traffic separation, and maritime security. However, because AIS messages are unencrypted and unauthenticated, the system is highly vulnerable to spoofing, allowing attackers to hide the vessel, generate false traffic, or inject misleading navigational information.

  Cyber-physical behaviour:

  - AIS spoofing can alter traffic perception and mislead nearby vessels.
  - May be leveraged for deception or obfuscating vessel identity.

  Dependencies: Linked to ECDIS and VDR.
  Safety relevance: SOLAS-mandated for collision avoidance and vessel identification

- **X-Band radar / S-Band Radar**

  Function: The X-band radar provides high-resolution short-range situational awareness and supports ARPA target tracking and ECDIS radar overlay. As a SOLAS-required navigation system, its accuracy is fundamental for collision avoidance. Modern radars rely on networked signal processors, making them susceptible to false-echo injection, target suppression, or vector distortion, all of which severely undermine navigational safety.

  The S-band radar delivers long-range situational awareness and performs reliably in adverse weather conditions such as rain or fog. As a SOLAS-mandated system, it supports collision-avoidance decisions at extended ranges. Like X-band radars, its digital processing chain is

[2] CPA is the minimum distance at which another vessel will pass relative to your ship if both vessels maintain their current course and speed.

[3] TCPA is the time remaining until the CPA occurs.

vulnerable to manipulation of bearing, range, or ARPA vectors, which can mislead bridge teams and compromise safe navigation.

Cyber-physical behaviour:

- Radar corruption produces false echoes or hides real targets.
- Radar overlays within ECDIS become misleading.

Dependencies: Requires gyro and speed log; feeds ECDIS and VDR.
Safety relevance: SOLAS-mandated for safe navigation.

- **ECDIS (Unit 1 & Unit 2)**

  Function: ECDIS integrates GNSS, gyro, radar, AIS, echo sounder, and speed log data into a unified navigational environment for route planning and track control. ECDIS does not directly command the steering gear; it participates in track control when integrated with the autopilot. The autopilot then sends commands to the steering PLC. For cargo vessels ≥10,000 GT, it is SOLAS-mandated as the primary electronic chart system. As the principal navigation processor and a steering-influencing device, ECDIS compromise -whether through chart tampering, malware, sensor spoofing, or interface manipulation- can directly alter route execution and generate hazardous navigational decisions.

  Cyber-physical behaviour:

  - Malware or chart tampering manipulates route planning and safety contours.
  - ECDIS → Autopilot → Steering Gear PLC chain means ECDIS compromise becomes direct cyber-physical control.

  Dependencies: Receives GPS, gyro, radars, AIS, speed log, echo sounder; outputs autopilot commands.
  Safety relevance: Primary navigation tool; SOLAS-mandated for cargo ships ≥ 10,000 GT; single most consequential navigation processor.

- **Autopilot**

  Function: The autopilot converts ECDIS or helmsman inputs into automatic steering commands delivered to the steering gear PLC. Its function depends on accurate gyro and speed information, and any falsified inputs can cause immediate course deviations. Because the autopilot is a direct cyber-physical actuator, compromising its control signals or operational mode represents one of the fastest ways to alter the ship's navigation trajectory.

  Cyber-physical behaviour:

  - Autopilot compromise results in immediate course alteration.
  - CAN-bus command injection is a realistic threat.

  Dependencies: Receives ECDIS route data; sends commands to steering PLC.
  Safety relevance: Highest immediate cyber-physical impact asset in VLAN 10.

- **Bridge navigation workstations**

  Function: Bridge workstations host conning displays, navigation clients, and monitoring interfaces, typically running general-purpose operating systems. They serve as user interaction points with ECDIS, radar, and sensor data. Due to frequent use for chart updates, reporting, and documentation, they are a common malware entry point, creating a high-risk bridge for lateral movement into mission-critical navigation systems.

  Cyber-physical behaviour:

  - Run general-purpose OS → attractive lateral movement targets.
  - Often used for chart updates → malware delivery channel.

Dependencies: Interact with ECDIS, radar, AIS.
Safety relevance: High operational exposure, moderate systemic importance.

- **BNWAS (Bridge Alarm System)**

  Function: The Bridge Navigational Watch Alarm System ensures continuous watchkeeping by monitoring officer activity and escalation alarms. As a SOLAS-mandated safety barrier, BNWAS helps prevent navigational errors due to human fatigue. BNWAS is normally *not* network-integrated except for alarm relays.

  Its cyber exposure is minimal, but a cyber suppression scenario is still useful conceptually. Cyber suppression of BNWAS alarms may conceal other simultaneous attacks on navigation systems, allowing unsafe conditions to persist undetected.

  Cyber-physical behaviour:

  - Cyber suppression disables the watch-keeping safety layer.

  Safety relevance: Required by SOLAS; indirect but critical safety barrier.

- **VDR (Voyage Data Recorder)**

  Function: The VDR continuously records GNSS, gyro, AIS, radar, ECDIS, engine telegraph, alarms, and bridge audio for investigation and compliance purposes. As a SOLAS-mandated forensic system, VDR integrity is essential for post-incident analysis. Attackers often target VDR to disable logging or falsify data, masking evidence of cyber intrusions and complicating regulatory investigation

  Cyber-physical behaviour:

  - Attackers frequently disable VDR to hide intrusion trails.

  Dependencies: Receives from every major bridge and engine system.
  Safety relevance: Regulatory requirement-SOLAS-mandated; essential for post-incident analysis.

Engine Network (VLAN 20)

- **Engine control PLC**

  Function: The engine control PLC governs propulsion by executing logic for fuel injection, turbocharger management, protection functions, and start/stop routines. Any cyber manipulation of PLC logic can cause propulsion loss, engine damage, or unsafe torque levels. Because the PLC directly controls the main engine, it is one of the highest-impact cyber-physical assets on board.

  Cyber-physical behaviour:

  - A manipulated PLC may cause overspeed, shutdown, or incorrect torque.

  Dependencies: Receives commands via MAS; outputs drive propulsion.
  Safety relevance: Highest physical-impact asset besides steering PLC.

- **Machinery automation server**

  Function: The MAS is the supervisory automation server responsible for collecting data, issuing alarms, coordinating PLCs, interfacing with the bridge, and supporting remote diagnostics. Although typically dual-homed, it supervises cargo, ballast, auxiliary, and propulsion systems across multiple VLANs. MAS compromise has systemic consequences, enabling attackers to mask alarms, manipulate setpoints, or propagate into navigation systems. It is therefore classified as a high-criticality system under IACS UR E26/E27.

  Cyber-physical behaviour:

- The most dangerous propagation vector on the vessel.
- Compromise affects engine, steering, cargo, ballast, and alarms simultaneously.

Dependencies: Cross-domain hub linking VLAN 20 ↔ 10 ↔ 30. It receives data from engine PLC, steering PLC, PMS, Ballast PLC, cargo system, tank sensors and these connections are Ethernet, Modbus-TCP, CANbus or proprietary fieldbus terminating in MAS.
Safety relevance: Central systemic risk amplifier.

- **Power management system**

  Function: The PMS controls generator synchronisation, load sharing, breaker logic, and blackout recovery. Compromising PMS can induce blackout scenarios that disable propulsion and navigation systems simultaneously. Because PMS stability underpins the power supply of the entire ship, it is a critical cyber-physical node with severe cascading-failure potential.

  Cyber-physical behaviour:

  - Attack may cause blackout → loss of propulsion and navigation.

  Dependencies: Interacts with MAS.
  Safety relevance: Essential for vessel-wide power stability.

- **Steering gear PLC**

  Function: The steering PLC controls hydraulic pumps and valves driving rudder actuation. As a primary safety-critical system under SOLAS, it must respond precisely to helm or autopilot commands. Cyber manipulation of steering logic can generate abrupt course deviations, erratic rudder motion, or loss of steering, making it one of the most dangerous systems to compromise.

  Cyber-physical behaviour:

  - Direct control of rudder movement → catastrophic potential if manipulated.

  Dependencies: Receives commands from autopilot & helm.
  Safety relevance: Steering is a safety-critical function under SOLAS.

- **Auxiliary systems**

  Function: Auxiliary machinery includes pumps, separators, cooling fans, compressors, and lubrication systems essential to engine and generator operation. Although individually less critical, their coordinated behaviour is vital. Cyber manipulation of auxiliary systems can indirectly destabilise the engine room environment, causing overheating, shutdowns, or machinery trips that cascade into propulsion or power failures.

  Cyber-physical behaviour:

  - Indirect but essential contributors to engine stability.

  Safety relevance: Secondary impact systems.

Cargo & Ballast Network (VLAN 30)

- **Cargo monitoring system**

  Function: The cargo monitoring system collects tank levels, pressures, temperatures, and environmental data, providing essential information for safe cargo stowage. Cyber manipulation may conceal overpressure conditions, misrepresent tank levels, or disable alarms, creating safety and environmental hazards, especially for hazardous or sensitive cargoes.

  Cyber-physical behaviour:

  - Incorrect readings → unsafe load distribution → hull stress.

Dependencies: Supplies MAS; interacts with ballast PLC.
Safety relevance: Critical for cargo integrity & structural safety.

- **Ballast system PLC**

  Function: The ballast PLC controls pumps and valves used to manage the vessel's trim, heel, and stability. A cyberattack on ballast control can cause unsafe stability conditions, excessive heel, or structural stress. Because ballast operations directly influence seaworthiness, this PLC is a high-impact cyber-physical asset.

  Cyber-physical behaviour:

  - Incorrect sequencing → severe trim, heel, or stability issues.

  Dependencies: Controlled via MAS.
  Safety relevance: Core stability function.

- **Tank Level Sensors & Temperature/Pressure Sensors**

  Function: Tank level sensors provide raw measurement inputs to cargo and ballast automation systems. If falsified, they mislead PLC logic and operator decisions, potentially resulting in overfilling, excessive heel, or structural loading anomalies.

  Temperature and pressure sensors provide real-time environmental data to PLCs and monitoring systems. Manipulation of these readings can suppress critical alarms and drive automation systems into unsafe states, especially in cargo or machinery environments requiring tight environmental control.

  Cyber-physical behaviour:

  - Sensor falsification corrupts automation logic.

  Safety relevance: Upstream accuracy essential for safe loading.

IT/OT Gateway & Satcom Network (VLAN 40)

- **IT/OT firewall**

  Function: The IT/OT firewall controls traffic between administrative IT networks and the operational OT environment. As the primary segmentation barrier, its configuration determines whether malware or unauthorized users can pivot into OT systems. Misconfiguration or bypass of the firewall exposes the entire OT domain to elevated cyber risk.

  Cyber-physical behaviour:

  - Misconfiguration yields full OT exposure to IT malware.

  Safety relevance: First line of cyber defence.

- **Satcom router**

  Function: The satcom router provides internet connectivity via VSAT or L-band services and is the most exposed cyber entry point on the vessel. Compromise of the satcom router allows adversaries to gain footholds inside ship networks, from which they can pivot toward OT systems if segmentation is weak or credentials are shared. Cyber-physical behaviour:

  - Most common maritime cyber-attack vector (e.g., phishing → remote pivot).

  Safety relevance: High-exposure gateway.

- **Vendor maintenance tunnel**

Function: The vendor maintenance tunnel enables Original Equipment Manufacturer (OEM) engineers to perform remote diagnostics and firmware updates on PLCs, MAS, and other automation components. Because these tunnels typically provide privileged access, they represent a high-risk entry vector if credentials or remote connections are compromised.

Cyber-physical behaviour:

- Third-party compromise → direct PLC exposure.

Safety relevance: Extremely high-risk if unmanaged.

- **Remote diagnostics platform**

  Function: The remote diagnostics platform sends operational data to OEM or fleet cloud systems for predictive maintenance analysis. If the platform or associated credentials are compromised, attackers may obtain direct supervisory access to OT systems or manipulate transmitted telemetry, enabling stealthy long-term intrusion. Cyber-physical behaviour:

  - Platform compromise gives attackers privileged access paths.

  Safety relevance: High lateral-movement potential.

This architecture forms the basis of the risk and heat-intensity model.

Summary of OT Assets: Functions, Dependencies, and Cyber Risks

A. Bridge Sensors (VLAN 10)

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
GNSS/GPS Receiver	Position, COG, SOG, UTC	ECDIS, AIS, Radar, Autopilot, VDR	Spoofing/jamming corrupts all navigation data	Yes
Gyrocompass	True heading	Radars, ECDIS, Autopilot, AIS, VDR	Heading spoofing → wrong ARPA vectors and steering commands	Yes
Doppler Speed Log	Speed-through-water (STW)	Radar ARPA, ECDIS, VDR	STW falsification → incorrect CPA/TCPA	Yes
Echo Sounder	Depth-below-keel	ECDIS, VDR	Depth spoofing → grounding risk	Yes
AIS Transponder	Traffic broadcast/exchange	ECDIS, Radar overlays, VDR	Spoofing → false traffic, vessel invisibility	Yes

Table 5.1a – OT Asset Summary – Bridge Sensors (VLAN 10)

B. Bridge Situational Awareness Systems

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
X-Band Radar	Short-range target detection & ARPA	ECDIS overlay, VDR, Conning	False targets / vector distortion	Yes
S-Band Radar	Long-range detection in poor weather	ECDIS, VDR	Target suppression / range manipulation	Yes

Table 5.1b – OT Asset Summary – Bridge Situational Awareness Systems

C. Navigation Processors

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
ECDIS (1 & 2)	Chart display, route monitoring	Autopilot, VDR, Radars	Chart tampering, malware, spoofed sensor inputs	Yes (for ≥10,000 GT)
Autopilot	Automatic steering	Steering PLC	Command spoofing → immediate course alteration	No (but functionally required)

Table 5.1c – OT Asset Summary – Navigation Processors

D. Bridge Human Machine Interfaces (HMIs)

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
Bridge Workstations	Navigation displays & monitoring	ECDIS, Radar clients	Malware entry point → lateral movement	No
BNWAS	Watchkeeping alert system	None (alarm escalation)	Alarm suppression	Yes
VDR	Voyage data recording	Entire bridge & machinery systems	Tampering hides intrusion evidence	Yes

Table 5.1d – OT Asset Summary – Bridge Human Machine Interfaces (HMIs)

E. Engine and Machinery Systems (VLAN 20)

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
Engine Control PLC	Propulsion control logic	Main Engine	Unsafe engine behaviour / shutdown	No

Machinery Automation Server (MAS)	Supervisory control & alarms	All PLCs, Bridge, VDR	System-wide manipulation & hidden alarms	No (but class-critical)
PMS	Generator control & blackout recovery	Switchboards, ECR displays	Blackout induction	No
Steering Gear PLC	Rudder actuation	Steering system	Forced rudder movement → loss of control	Yes (steering system)
Auxiliary Systems	Pumps, cooling, lubrication	Engine & generators	Indirect machinery destabilisation	No

Table 5.1e – OT Asset Summary – Engine and Machinery Systems (VLAN 20)

F. Cargo & Ballast Systems (VLAN 30)

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
Cargo Monitoring System	Tank measurements & alarms	MAS, ECR, Bridge	False readings → unsafe tank conditions	No
Ballast PLC	Trim, heel, ballast control	Pumps & valves	Induced heel/trim instability	No
Tank Level Sensors	Ullage/level measurement	Cargo/ballast PLCs	Falsified inputs → overfill/heel	No
Temperature/Pressure Sensors	Env. measurements	PLC logic	False data → unsafe automation behaviour	No

Table 5.1f – OT Asset Summary – Cargo and Ballast Systems (VLAN 30)

G. IT/OT Boundary Systems (VLAN 40)

Asset	Primary Function	Downstream Dependencies	Primary Cyber Risk	SOLAS Mandated
IT/OT Firewall	Segmentation barrier	OT environment	Misconfig exposes OT to IT malware	No
Satcom Router	Ship-to-shore connectivity	IT network, sometimes OT	Primary remote entry vector	No
Vendor Maintenance Tunnel	OEM remote access	PLCs, MAS, ECDIS	Privileged compromise → full OT access	No
Remote Diagnostics Platform	Cloud maintenance data	OEM systems, MAS	Credential abuse → supervisory access	No

Table 5.1g – OT Asset Summary – IT/OT Boundary Systems (VLAN 40)

5.2.3 Scope Considerations

The scope explicitly focuses on Operational Technology (OT). IT systems are included only where they form part of OT attack surfaces (e.g., IT/OT gateway, satcom router, remote vendor tunnel). Administrative IT (crew computers, office networks) is excluded unless cyber-lateral movement into OT is feasible. As detailed in Chapter 2, modern ships possess highly interdependent cyber-physical systems. Navigation systems (GPS, gyro, radars) feed ECDIS, which drives the autopilot, which controls the steering PLC, which affects vessel manoeuvring and engine-load dynamics. This inherent coupling reinforces why systemic, not component-level, analysis is required. The selected platform accurately reflects the operational reality of merchant vessels and provides a defensible basis for validating the hybrid cyber-risk assessment framework.

5.3 Application of the Framework

The assessment follows the six-step hybrid methodology defined in Chapter 4:

1. Asset Identification
2. Threat Modelling
3. Vulnerability Assessment
4. Risk Evaluation
5. Interdependency and Heat-Intensity Analysis
6. Governance and Continuous Assurance

Each step operationalizes a core principle of the hybrid model: linking IEC 62443's structural controls, NIST SP 800-82's operational guidance, and ISO 31000's governance rigor into a coherent analytical workflow.

5.3.1 Asset Identification

An OT asset inventory was created, including all SOLAS-mandated navigation sensors, all bridge control systems, dual radars, redundant ECDIS, autopilot, VDR, bridge workstations, machinery and propulsion PLCs, automation servers, cargo and ballast systems, and IT/OT boundary devices.

OT assets were identified and classified by:

- operational function,
- criticality,
- communication protocol,
- network segment,
- upstream/downstream dependency,

This granularity is critical for analytical fidelity, as high-impact nodes (e.g., ECDIS, Autopilot, Engine PLC, Automation Server) cannot be modelled adequately in aggregated form.

The asset inventory presented in Table 5.1 – OT Asset Inventory adopts a structured classification approach aligned with IEC 62443-3-2 zoning principles and NIST SP 800-82 ICS system characterization. Each column captures a specific analytical parameter required for later vulnerability, risk, and heat-intensity modelling.

- The **ID** column uniquely identifies each OT component so that it can be traced across the vulnerability (Table 5.7 – OT Vulnerability Register and Context-Aware Vulnerability Index (CVI)), risk evaluation (Table 5.9 – Consolidated OT Risk Register and Residual Risk Evaluation), and heat-intensity matrices.

- The **Asset** column names the subsystem or equipment being assessed, ensuring consistency with the vessel's configuration baselines and network diagrams.
- The **Function** field describes the operational role of the asset (e.g., navigation sensor, steering actuator, propulsion controller), establishing its relevance to safety and mission outcomes under the ISM Code and SOLAS requirements.
- The **Protocols** column lists the communication standards and interfaces used (e.g., NMEA, Modbus TCP, CANbus, OPC-UA), capturing protocol weaknesses and interoperability characteristics that directly influence exploitability.
- **Criticality** denotes the operational importance of each asset based on the potential safety, environmental, and operational consequences of failure; this aligns with ISO 31000 and IMO MSC-FAL.1/Circ.3 impact definitions.
- The **Connectivity** column identifies how each asset interfaces with the wider OT environment—VLAN membership, sensor buses, conduits, dual-homed interfaces—forming the basis of the connectivity coefficient used later in heat-mapping calculations.
- Finally, **Dependencies** capture upstream and downstream functional relationships (e.g., GPS → ECDIS → Autopilot), which are essential for modelling cascading effects and systemic propagation within the interdependency analysis. Collectively, these columns provide the structural and functional detail required to assess cyber risk at both component and system-of-systems levels.

Asset ID	Asset Name	Category	Function	Protocols	Criticality	Connectivity (Detailed)	Dependencies
OT-NAV-01	GNSS/GPS Receiver	Navigation	Positioning input	NMEA 0183 / GNSS RF	Critical	Sensor bus → ECDIS, AIS, Radars, Autopilot, VDR	Upstream for all navigation systems
OT-NAV-02	Gyrocompass	Navigation	Heading reference	NMEA 0183	Critical	Sensor bus → ECDIS, Radars, Autopilot	Required for route keeping & ARPA vectors
OT-NAV-03	Doppler Speed Log	Navigation	Speed through water	NMEA / Serial	High	Sensor bus → ECDIS, VDR, Radars	ARPA speed input
OT-NAV-04	Echo Sounder	Navigation	Under-keel depth	NMEA / Serial	High	Sensor → ECDIS, VDR	Grounding avoidance
OT-NAV-05	AIS Transponder	Navigation	Vessel data exchange	IEC 61162 / Ethernet	High	VLAN 10 ↔ ECDIS, VDR	Traffic identification
OT-NAV-06	X-Band Radar	Navigation	Short-range radar + ARPA	Ethernet + ARPA	Safety-critical	VLAN 10 ↔ ECDIS, VDR	Collision avoidance
OT-NAV-07	S-Band Radar	Navigation	Long-range radar + ARPA	Ethernet + ARPA	Safety-critical	VLAN 10 ↔ ECDIS, VDR	Collision avoidance
OT-NAV-08	ECDIS Unit 1	Navigation	Primary ECDIS	IEC 61162-450 / TCP-IP	Critical	GNSS, Gyro, Radars, AIS → ECDIS; ECDIS → Autopilot, VDR	Route monitoring & control
OT-NAV-09	ECDIS Unit 2	Navigation	Backup ECDIS	IEC 61162-450 / TCP-IP	Critical	Same as OT-NAV-08	Redundancy

OT-NAV-10	Autopilot	Navigation	Helm control	NMEA / CANbus	Safety-critical	ECDIS → Autopilot → Steering PLC	Executes steering commands
OT-NAV-11	BNWAS	Navigation	Watch alarm	Ethernet	High	VLAN 10; alarms → cabins + VDR	Human alerting
OT-NAV-12	VDR	Navigation	Voyage data recording	Mixed (IEC 61162, Modbus)	High	Inputs from all navigation & engine systems	Forensic evidence
OT-NAV-13	Bridge Workstations	Navigation	HMI (conning, planning)	Ethernet	Medium	VLAN 10; ECDIS/Radar clients	Operator interface
OT-ENG-01	Engine Control PLC	Engine	Propulsion logic	Modbus TCP / CANbus	Safety-critical	VLAN 20 ↔ MAS; ECR displays; limited → Bridge	Main engine logic
OT-ENG-02	Machinery Automation Server (MAS)	Engine	Machinery control & supervision	Modbus TCP, OPC-UA, SNMP	Safety-critical	Dual NIC: VLAN 10 + VLAN 20; connects to all PLCs	Central OT supervisory node
OT-ENG-03	Power Management System (PMS)	Engine	Generator & power control	Modbus, CANbus	High	VLAN 20; Switchboards ↔ PMS ↔ MAS	Blackout recovery & load sharing
OT-ENG-04	Auxiliary Machinery Controls	Engine	Auxiliary machinery automation	Analogue / Modbus	Medium	VLAN 20; MAS → pumps, purifiers, compressors	Machinery stability

OT-AUX-01	Steering Gear PLC	Steering	Rudder actuation control	CANbus / Modbus	Safety-critical	Autopilot → Steering PLC → Rudder actuators	Steering authority
OT-CAR-01	Cargo Monitoring System	Cargo	Cargo condition monitoring	Profibus / OPC DA	Mission-critical	VLAN 30 ↔ MAS; tank sensors ↔ HMI	Cargo integrity
OT-BAL-01	Ballast PLC	Ballast	Ballast automation	Modbus / Digital I/O	Mission-critical	VLAN 30 ↔ MAS; valves/pumps	Stability, trim & list
OT-SEN-01	Tank Level Sensors	Cargo/Ballast	Liquid level measurement	4–20 mA / Modbus	Medium	Sensors → Ballast PLC / Cargo HMI	Raw tank data
OT-SEN-02	Temperature/Pressure Sensors	Cargo/Ballast	Environmental measurements	Analogue / Modbus	Medium	Sensors → Cargo/Engine PLCs	Environmental monitoring
OT-COM-01	Satcom Router	Communications	Ship–shore link	TCP/IP	High	VLAN 40 → Firewall → OT networks	Primary external attack surface
OT-IT-01	IT/OT Gateway Firewall	IT/OT Boundary	Segmentation & filtering	VLAN trunk / ACLs	High	Controls traffic between VLANs 10/20/30/40	OT protection
OT-OEM-01	Vendor Maintenance Tunnel	Vendor Access	Remote OEM access	OpenVPN / SSH	Very High	VLAN 40 → MAS/PLCs	Privileged vendor path
OT-OEM-02	Remote Diagnostics Cloud	Vendor Access	Telematics & monitoring	HTTPS API	High	OEM cloud → MAS telemetry	CBM (Condition-based monitoring)

Table 5.1 – OT Asset Inventory

5.3.2 Threat Modelling

Threat modelling was performed using an adapted STRIDE methodology, modified to account for maritime OT realities, mixed-vendor architectures, and the cyber-physical nature of shipboard control systems. Unlike generic IT environments, vessels exhibit unique dependencies—namely, weak sensor authentication, legacy fieldbus protocols, remote OEM maintenance access, and the presence of safety-critical actuators such as steering gear PLCs and propulsion controllers. For this reason, the baseline STRIDE categories were extended with maritime-specific adversary actions, operational constraints, and domain-specific attack paths identified in ENISA, BIMCO, and EMSA cyber-threat assessments.

Spoofing (S)

Spoofing scenarios include GNSS signal forgery, AIS identity manipulation, NMEA0183/2000 message injection, and falsified sensor data provided to ECDIS, ARPA radars, autopilot, and MAS. Maritime GNSS and AIS remain fundamentally unauthenticated systems, making them prime targets for attackers attempting to distort situational awareness or induce unsafe navigational decisions. PLC-level spoofing is also a realistic threat, particularly where ballast, cargo, and engine control devices accept unverified Modbus TCP or CANbus frames.

Tampering (T)

Tampering includes modification of PLC logic, ECDIS chart databases, MAS alarm configurations, PMS setpoints, or radar ARPA processing parameters. These actions typically occur through compromised OEM remote maintenance tunnels, infected vendor laptops, or exploitation of misconfigured IT/OT firewalls. Because many PLCs lack cryptographic code signing, tampering can be performed silently and persist after reboot. Tampering of steering PLC logic or propulsion automation is classified as a severe safety hazard under IACS UR E26.

Repudiation (R)

Repudiation threats arise from inadequate logging, decentralised audit trails, and inconsistent time synchronisation across OT systems. VDR tampering, MAS alarm suppression, or missing PLC event logs create conditions where malicious or erroneous operations cannot be traced. Due to fragmented log architectures and the absence of immutable forensic trails in legacy OT systems, repudiation attacks remain largely undetectable, leaving operators unaware of manipulation until physical symptoms appear.

Information Disclosure (I)

Information disclosure is particularly relevant in vessels using unencrypted satcom channels, legacy NMEA feeds, or unsegmented remote diagnostics paths. Attackers can monitor operational data, crew communications, or OEM credentials through compromised VSAT terminals or poorly isolated VLANs. Disclosure of engine parameters, cargo conditions, or network topology simplifies subsequent targeted attacks and enables adversaries to map safety-critical pathways without direct access to OT devices.

Denial of Service (D)

Denial-of-service threats include flooding IT/OT gateways, overloading satcom bandwidth, disabling MAS services, or exhausting automation switch resources. A DoS attack may prevent ECDIS from receiving sensor updates, disrupt PMS generator synchronisation, or block remote engine telegraph commands, leading to cascading operational failures. Because many marine control systems expect deterministic, real-time update intervals, even a low-bandwidth DoS may result in loss of control or protective shutdown.

Elevation of Privilege (E)

Privilege escalation frequently arises from shared admin accounts, default PLC credentials, hardcoded vendor passwords, and unmanaged privilege boundaries between IT and OT domains. Attackers exploiting misconfigured maintenance tunnels or satcom routers can escalate privileges from IT systems into MAS, PMS, or steering PLC interfaces. Elevation of privilege is among the most severe maritime threats because it enables direct manipulation of propulsion, ballast, or steering functions.

Adversary Motivation and Capability Spectrum

The modelling process considered both capability-driven (state-sponsored or well-financed criminal groups) and opportunistic attackers (malware, ransomware, and script-based intrusions). Industry threat intelligence from ENISA, BIMCO, and EMSA shows that opportunistic attacks increasingly penetrate maritime networks due to poor segmentation and remote access exposures, while targeted actors may focus on manipulating navigation data, disrupting cargo operations, or interfering with energy-related shipping. The combined STRIDE-maritime model therefore captures both high-complexity cyber-physical scenarios and lower-sophistication attack paths frequently observed in commercial fleets.

Threat Category (STRIDE)	Description	Maritime OT Examples	Affected Assets	Impact on Vessel Operations	Relevant Controls / Mitigations
S – Spoofing	Impersonation of data sources or devices	GNSS position spoofing; AIS identity spoofing; false sensor values	GNSS, AIS, Speed Log, Echo Sounder, ECDIS	Loss of positional awareness; wrong grounding depth; collision risk	GNSS authentication, cross-checking, RAIM, sensor fusion, input validation
T – Tampering	Unauthorized modification of data, logic, or configuration	PLC logic alteration; ECDIS chart manipulation; autopilot command injection	Engine PLC, Steering PLC, Ballast PLC, ECDIS, Autopilot	Loss of propulsion/steering control; unsafe manoeuvring; flooding	RBAC, MFA, PLC write-protection, network segmentation, firmware integrity
R – Repudiation	Denial of actions due to lack of audit trails	Vendor remote access without logs; operator actions not recorded	OEM Tunnel, MAS, Satcom Gateway, IT/OT Firewall	Inability to reconstruct incidents; compliance failure	Central logging (SIEM), secure audit trails, session recording
I – Information Disclosure	Unauthorized data access	Sniffing NMEA/IEC-61162 traffic; leaking engine telemetry via Satcom	Satcom Router, IT/OT Gateway, MAS, ECDIS	Exposure of sensitive data; facilitation of targeted attacks	TLS 1.3, encryption, VLAN isolation, firewalling, disable legacy protocols
D – Denial of Service	Loss of service availability	Flooding autopilot bus; MAS DoS; GNSS jamming	MAS, Engine PLC, Autopilot, Satcom, GNSS	Loss of navigation inputs; machinery faults; propulsion degradation	Rate-limiting, redundant sensors, DoS-resistant GNSS, segmentation
E – Elevation of Privilege	Unauthorised high-level access	Default PLC credentials; shared OEM accounts; unsegregated admin roles	Engine PLC, Steering PLC, MAS, ECDIS, OEM Tunnel	Full system compromise; ability to alter control logic	MFA, RBAC, credential hardening, identity lifecycle management

Table 5.2 – STRIDE Methodology on OT Assets

Next, STRIDE is applied for all identified OT assets of our use case.

Navigation & Bridge Systems (VLAN 10)

- Navigation assets (GNSS, ECDIS, radars, AIS, autopilot, speed log, echo sounder) are heavily exposed to Spoofing (S) and Information Disclosure (I) because they rely on NMEA / IEC-61162 traffic without authentication or encryption.
- ECDIS Units 1 and 2 have the richest STRIDE profile (S, T, R, I, D, E), reflecting their role as Windows-based integration points with multiple sensor inputs, OEM support, and administrative functions.
- Autopilot and Steering PLC form the critical chain where spoofed or tampered navigation data can become actual rudder movements.
- BNWAS and VDR are less vulnerable in terms of systemic impact (low CVI), but their Repudiation and logging weaknesses affect *forensic capability* and *compliance* rather than immediate safety.

Asset ID	Asset Name	S	T	R	I	D	E	Explanation (Summary of Threats)
OT-NAV-01	GNSS/GPS Receiver	✓	–	–	✓	✓	–	Susceptible to spoofing/jamming; data disclosed via NMEA; DoS via RF interference
OT-NAV-02	Gyrocompass	–	–	–	–	✓	–	DoS risk if bus overloaded; limited cyber-exposure
OT-NAV-03	Speed Log	–	–	–	✓	✓	–	Unencrypted serial data sniffing; DoS interference possible
OT-NAV-04	Echo Sounder	–	–	–	✓	✓	–	Under-keel depth data can be intercepted; DoS on sensor bus
OT-NAV-05	AIS Transponder	✓	–	–	✓	✓	–	AIS identity spoofing; NMEA disclosure; DoS via RF flooding
OT-NAV-06	X-Band Radar	–	–	–	✓	✓	–	Radar plots interceptable; DoS via interference
OT-NAV-07	S-Band Radar	–	–	–	✓	✓	–	Similar to X-band; info disclosure and DoS risks
OT-NAV-08	ECDIS #1	✓	✓	✓	✓	✓	✓	Highest NAV risk: spoofing (GNSS), tampering (charts), repudiation (logs), disclosure (IEC-61162), DoS, privilege escalation via admin accounts
OT-NAV-09	ECDIS #2	✓	✓	✓	✓	✓	✓	Same as above; redundant path but equally exposed
OT-NAV-10	Autopilot	✓	✓	–	–	✓	✓	Spoofed NAV inputs cause mis-steering; tampering possible; DoS disrupts steering; EoP possible via serial bus

OT-NAV-11	BNWAS	–	–	✓	–	✓	–	Poor audit trails; DoS can disable alarms; low cyber exposure
OT-NAV-12	VDR	✓	–	✓	✓	✓	–	Can record spoofed inputs; logs tamperable; high disclosure & DoS risk
OT-NAV-13	Bridge Workstations	✓	✓	✓	✓	✓	✓	Full workstation threat surface: malware, tampering, privilege escalation

Table 5.3 – STRIDE Application on Navigation and Bridge Assets

Machinery & Propulsion Systems (VLAN 20)

- Engine Control PLC and Steering Gear PLC are dominated by Tampering (T), DoS (D), and Elevation of Privilege (E) threats. If exploited, they can directly cause loss of propulsion or steering. Their CVI scores (4.3) confirm them as high-priority protection targets.
- MAS is the most interconnected OT node. It aggregates telemetry and control flows, is dual homed, and has the maximum CVI (5.0). It is exposed to T, R, I, D, E — essentially the full STRIDE spectrum.
- PMS is particularly relevant for power stability (DoS → blackout), with CVI 4.0, and is mainly threatened by protocol weaknesses (SNMP, shared accounts) and tampering.

Asset ID	Asset Name	S	T	R	I	D	E	Explanation
OT-ENG-01	Engine Control PLC	–	✓	✓	✓	✓	✓	Critical control logic tampering; poor logging; privilege escalation; DoS → propulsion loss
OT-ENG-02	Machinery Automation Server (MAS)	–	✓	✓	✓	✓	✓	Dual-homed → high disclosure; tampering risk; EoP possible via old OS; logging insufficient
OT-ENG-03	Power Management System (PMS)	–	✓	–	✓	✓	✓	SNMP tampering; privilege escalation locally; DoS affects electrical stability
OT-AUX-01	Steering Gear PLC	–	✓	–	–	✓	✓	Logic tampering can cause rudder hard-over; DoS disrupts steering; EoP via default accounts
OT-AUX-02	Auxiliary Machinery Control	–	✓	–	–	✓	✓	Local-only access; vulnerable to tampering and privilege escalation

Table 5.4 – STRIDE Application on Machinery and Propulsion Assets

Cargo & Ballast Systems (VLAN 30)

- Cargo Monitoring System and Ballast PLC show a combination of Tampering (T), Information Disclosure (I), and Elevation of Privilege (E). Their compromise can affect trim, stability, and cargo safety, especially during port operations.
- Sensors (Tank Level, Temp/Pressure) mostly suffer from I and D threats. They can be spoofed or disrupted, but on their own they typically create operational inconvenience rather than immediate catastrophic risk — consistent with their lower CVI (2.3).

Asset ID	Asset Name	S	T	R	I	D	E	Explanation
OT-CAR-01	Cargo Monitoring System	–	✓	✓	✓	✓	✓	Unpatched firmware; shared accounts; disclosure of cargo data; DoS to sensors
OT-BAL-01	Ballast PLC	–	✓	–	✓	✓	✓	Tampering alters stability; info disclosure of tank states; EoP via vendor ports
OT-SEN-01	Tank Level Sensors	–	–	–	✓	✓	–	Data disclosure; DoS halts tank readings
OT-SEN-02	Temp/Pressure Sensors	–	–	–	✓	✓	–	Similar to above: disclosure + DoS

Table 5.5 – STRIDE Application on Cargo and Ballast Assets

Communication, Boundary and Remote Access Systems (VLAN 40)

- Satcom Router and IT/OT Firewall are exposed to almost the full STRIDE spectrum: T, R, I, D, E (and S in the case of DNS / routing attacks).
- Vendor Maintenance Tunnel (OT-OEM-01) is one of the most dangerous assets: full T, R, I, D, E exposure, always-on connectivity, shared credentials, and a CVI of 5.0. It acts as a direct backdoor into MAS and PLCs if not properly governed.
- Remote Diagnostics Cloud (OT-OEM-02) is similar: compromise in the cloud side can cascade into the vessel.

Asset ID	Asset Name	S	T	R	I	D	E	Explanation
OT-COM-01	Satcom Router	✓	✓	✓	✓	✓	✓	Full spectrum: spoofing via DNS, packet tampering, disclosure, DoS, escalation
OT-IT-01	IT/OT Gateway (Firewall)	–	✓	✓	✓	✓	✓	Configuration tampering; privilege escalation; IT→OT pivoting; DoS on filtering processes
OT-OEM-01	Vendor Maintenance Tunnel	–	✓	✓	✓	✓	✓	High-risk: privileged access, no audit trails, tampering, exfiltration, DoS

OT-OEM-02	Remote Diagnostics Cloud	✓	✓	✓	✓	✓	✓	Cloud compromise → vessel compromise; full STRIDE exposure

Table 5.6 – STRIDE Application on Communication, Boundary and Remote Access Assets

5.3.3 Vulnerability Assessment

The vulnerability analysis examined exploitability in operational context rather than simply cataloguing flaws. Shipboard OT differs from IT in that patching windows are limited, and vendor dependencies are rigid; a low-complexity exploit may therefore present catastrophic operational risk. Data sources included classification-society advisories, CVE (Common Vulnerabilities and Exposures)/NVD (National Vulnerability Database) and CISA ICS-CERT feeds, and direct configuration review.

CVI (Cyber Vulnerability Index) is a composite, weighted vulnerability score used in this thesis to quantify how technically exploitable and operationally impactful a vulnerability is within the vessel's OT environment.

It combines three dimensions:

Dimension (s)	Description	Weight (w)
Exploitability	Ease of technical exploitation	0.4
Operational Exposure	Accessibility during operations	0.3
Systemic Impact Potential	Ability to propagate across subsystems	0.3

Table 5.13 – CVI Scoring Dimensions

$$\text{CVI} = \sum(w_i \times s_i)$$

CVI does not measure safety criticality alone, but cyber vulnerability weighted by how that vulnerability affects operational control pathways. Values are on a 1–5 scale, and a Severity Level has been added based on the weighted CVI:

Severity Score Range	Category
≥ 4.5	Critical
4.0–4.4	High
3.0–3.9	Medium
2.0–2.9	Low
< 2.0	Very Low

Table 5.13a – CVI Severity Score Classification

Approximately 68 % of high-CVI items stemmed from legacy design and default configurations, which is proof of the historical focus on safety determinism rather than adversarial resilience.

Asset ID	Asset Name	Identified Vulnerability	Exploitability (1–5)	Operational Exposure (1–5)	Systemic Impact Potential (1–5)	Weighted CVI = 0.4E + 0.3O + 0.3S	Severity Level	Reference / Source	Recommended Mitigation Action
OT-ENG-02	Machinery Automation Server (MAS)	Dual-homed Windows-based IAS server with legacy services, weak segmentation and broad PLC access	5	5	5	**5.0**	Critical	Config baseline; vendor docs; IACS UR E26	Enforce strict network segmentation, harden OS, restrict services, implement MFA for admin/OEM access, monitor logs centrally
OT-OEM-01	Vendor Maintenance Tunnel	Always-on VPN with shared OEM credentials and limited access control	5	5	5	**5.0**	Critical	OEM procedures; interviews; ENISA/BIMCO bulletins	Convert to on-demand, time-bound access with MFA; unique credentials; strong logging; jump-host architecture
OT-ENG-01	Engine Control PLC	Unauthenticated Modbus/CANbus access to propulsion logic; engineering workstation reachable via MAS	4	4	5	**4.3**	High	PLC manuals; network diagrams	Enforce firewall rules around PLCs, disable unused ports, restrict engineering workstation access,

									consider secure gateways/proxies
OT-AUX-01	Steering Gear PLC	Steering PLC reachable via autopilot and MAS; no cryptographic integrity on control frames	4	4	5	**4.3**	High	Steering system docs; config baseline	Isolate steering control network; enforce unidirectional control paths; alarm on unexpected command sources; periodic integrity tests
OT-NAV-01	GNSS/GPS Receiver	No authentication or integrity on GNSS signals; vulnerable to spoofing and jamming	5	4	4	**4.4**	High	ENISA/EMSA GNSS incidents; equipment specs	Deploy multi-constellation GNSS, integrate RAIM and spoofing detection, compare GNSS with inertial/DR, train crew in GNSS anomaly recognition
OT-NAV-08	ECDIS Unit 1	Windows-based system, USB chart updates, remote OEM support; dependent on multiple insecure sensor inputs	4	4	4	**4.0**	High	ECDIS manual; chart update procedures	Harden OS, restrict USB, isolate ECDIS VLAN, enforce signed chart updates, monitor configuration changes
OT-NAV-09	ECDIS Unit 2	Same vulnerabilities as ECDIS 1; acts as hot/cold standby	4	4	4	**4.0**	High	ECDIS redundancy design;	Mirror hardening and monitoring controls from ECDIS 1; ensure independent

								vendor docs	power/network paths where feasible
OT-NAV-02	Gyrocompass	NMEA heading output without authentication; vulnerable to serial/data spoofing	4	4	4	**4.0**	High	Sensor specs; bridge integration diagrams	Implement cross-checks (gyro vs magnetic/INS), alarm on heading jumps, tightly control access to signal converters and bridges
OT-COM-01	Satcom Router	Exposed management interfaces; shared use for crew/IT; potential pivot into OT via firewall misconfigurations	4	5	4	**4.3**	High	Config baseline; ENISA maritime reports	Harden router, disable unused services, segregate crew and OT traffic, enforce strong passwords and MFA where available
OT-IT-01	IT/OT Firewall & Gateway	Overly permissive rules and legacy ACLs; insufficient OT traffic filtering	3	3	5	**3.6**	Medium	Firewall ruleset review	Review and tighten ACLs, apply least-privilege principles, implement OT-specific IDS/IPS rulesets, periodic rule audits
OT-ENG-03	Power Management System (PMS)	Legacy protocols, shared accounts; dependent on MAS for supervision	4	4	4	**4.0**	High	PMS vendor docs; config baseline	Harden PMS controllers, enforce role-based access, segment from non-essential networks,

									simulate and test blackout scenarios
OT-BAL-01	Ballast PLC	Unauthenticated control over pumps/valves; remote maintenance enabled	4	3	3	**3.4**	Medium	PLC config; OEM access info	Restrict network access, disable default/backdoor accounts, log all remote sessions, implement approval workflow for changes
OT-NAV-10	Autopilot	CAN/NMEA control without crypto; direct link to steering PLC	3	3	4	**3.3**	Medium	Bridge wiring diagram; autopilot manual	Limit network paths to autopilot, verify manual override behavior, alarm on mode changes, crew training on cyber-induced anomalies
OT-CAR-01	Cargo Monitoring System	Insecure OPC/fieldbus communication; HMI on general-purpose OS	3	3	3	**3.0**	Medium	Vendor docs; automation drawings	Segment cargo network, harden HMI OS, restrict remote access, monitor for unexpected configuration/threshold changes
OT-NAV-06	X-Band Radar	Legacy OS, vendor management ports open; radar overlays can be manipulated	3	3	3	**3.0**	Medium	Radar manuals; config baseline	Harden radar processors, restrict remote ports, validate radar–ECDIS overlays, ensure independent

									visual/ARPA cross-checks
OT-NAV-07	S-Band Radar	Similar vulnerabilities to X-band; used in poor visibility and long range	3	3	3	**3.0**	Medium	Radar manuals; ops procedures	Mirror hardening and access controls applied to X-band, regular functional tests under low-visibility conditions
OT-NAV-03	Speed Log	NMEA output without validation; vulnerable to spoofing manipulation	3	3	3	**3.0**	Medium	Sensor docs; ARPA config	Cross-check STW vs SOG; alarms on unrealistic discrepancies; secure access to NMEA converters and cabling
OT-NAV-04	Echo Sounder	Unauthenticated depth data to ECDIS and VDR	3	3	3	**3.0**	Medium	Echo sounder specs; bridge diagrams	Cross-verify with paper soundings in critical waters; monitor for depth jumps; protect cabling and serial converters
OT-NAV-05	AIS Transponder	Unauthenticated RF messages; vulnerable to spoofed traffic and false targets	3	3	3	**3.0**	Medium	ENISA/BIMCO AIS threat notes	Train crew on AIS spoofing, correlate AIS with radar/visual, restrict remote configuration, update firmware

OT-NAV-13	Bridge Workstations	General-purpose OS; exposed to USB, email, and browsing where allowed	3	3	2	**2.7**	Low	Config baseline; interview with officers	Apply hardening baseline, restrict internet use, deploy AV/EDR, disable unneeded services and USB where possible
OT-ENG-04	Auxiliary Machinery Controls	Legacy PLCs; minimal access controls; often overlooked in hardening	3	3	2	**2.7**	Low	Aux system manuals; ECR observations	Identify critical auxiliaries, restrict logic changes, isolate from non-essential networks, implement basic logging
OT-SEN-01	Tank Level Sensors	No security controls on analogue/fieldbus interfaces	2	3	2	**2.3**	Low	Instrumentation datasheets	Protect cabling and junction boxes, validate readings via independent means, implement sanity checks in PLC logic
OT-SEN-02	Temperature/ Pressure Sensors	Similar to tank level; data trusted by automation without validation	2	3	2	**2.3**	Low	Instrumentation datasheets	Add range/consistency checks in PLC logic, secure access to transmitters and cabling, document calibration procedures

OT-NAV-12	VDR	Limited tamper protection; local admin access possible	2	2	1	**1.7**	Very Low	VDR manual; class rules	Restrict physical/admin access, periodically verify data integrity, ensure backups and recording continuity
OT-NAV-11	BNWAS	Simple logic; no cyber integrity monitoring	2	2	1	**1.7**	Very Low	BNWAS manual; ops procedures	Protect power and wiring, include BNWAS state in bridge checklists, test alarms regularly, log alarm activations

Table 5.7 – OT Vulnerability Register and Context-Aware Vulnerability Index (CVI)

The weighted CVI matrix provides a structured understanding of cyber-vulnerability across all OT assets by combining three independent but complementary dimensions: technical exploitability, operational exposure, and systemic impact potential. Together, these dimensions reveal how individual weaknesses can evolve into operational and safety-critical risks within the shipboard OT ecosystem.

Legend (STRIDE columns):

- **S** = Spoofing
- **T** = Tampering
- **R** = Repudiation
- **I** = Information Disclosure
- **D** = Denial of Service
- **E** = Elevation of Privilege

Asset ID	Asset Name	Key STRIDE Categories	Exploitability (E)	Operational Exposure (O)	Systemic Impact (S)	Weighted CVI

OT-ENG-02	Machinery Automation Server (MAS)	T, R, I, D, E	5	5	5	**5.0**
OT-OEM-01	Vendor Maintenance Tunnel	T, R, I, D, E	5	5	5	**5.0**
OT-ENG-01	Engine Control PLC	T, I, D, E	4	4	5	**4.3**
OT-AUX-01	Steering Gear PLC	T, D, E	4	4	5	**4.3**
OT-NAV-01	GNSS/GPS Receiver	S, I, D	5	4	4	**4.4**
OT-NAV-08	ECDIS Unit 1	S, T, R, I, D, E	4	4	4	**4.0**
OT-NAV-09	ECDIS Unit 2	S, T, R, I, D, E	4	4	4	**4.0**
OT-NAV-02	Gyrocompass	S, D	4	4	4	**4.0**
OT-COM-01	Satcom Router	T, R, I, D, E	4	5	4	**4.3**
OT-IT-01	IT/OT Firewall & Gateway	T, R, I, D, E	3	3	5	**3.6**
OT-ENG-03	Power Management System (PMS)	T, I, D, E	4	4	4	**4.0**
OT-BAL-01	Ballast PLC	T, I, D, E	4	3	3	**3.4**
OT-NAV-10	Autopilot	S, T, D, E	3	3	4	**3.3**
OT-CAR-01	Cargo Monitoring System	T, R, I, D, E	3	3	3	**3.0**
OT-NAV-06	X-Band Radar	I, D	3	3	3	**3.0**
OT-NAV-07	S-Band Radar	I, D	3	3	3	**3.0**
OT-NAV-03	Speed Log	S, I, D	3	3	3	**3.0**
OT-NAV-04	Echo Sounder	I, D	3	3	3	**3.0**
OT-NAV-05	AIS Transponder	S, I, D	3	3	3	**3.0**

OT-NAV-13	Bridge Workstations	T, I, D, E	3	3	2	**2.7**
OT-ENG-04	Auxiliary Machinery Controls	T, D, E	3	3	2	**2.7**
OT-SEN-01	Tank Level Sensors	I, D	2	3	2	**2.3**
OT-SEN-02	Temperature/Pressure Sensors	I, D	2	3	2	**2.3**
OT-NAV-12	VDR	R, I, D	2	2	1	**1.7**
OT-NAV-11	BNWAS	D, R	2	2	1	**1.7**

Table 5.8 – Full STRIDE to CVI Mapping Table for All Assets

Table 5.8a – Detailed STRIDE Threat Mapping per OT Asset

Highest-CVI Assets Represent Systemic Single Points of Failure

The assets with the highest weighted CVI (≥ 4.4) include:

- OT-ENG-02 — Machinery Automation Server (MAS)
- OT-OEM-01 — Vendor Maintenance Tunnel
- OT-ENG-01 — Engine Control PLC
- OT-AUX-01 — Steering Gear PLC
- OT-NAV-01 — GNSS/GPS Receiver

These systems share three defining properties that elevate their CVI:

(a) High Exploitability
They rely on insecure industrial protocols (Modbus, CAN, NMEA), default or shared credentials, or poorly hardened interfaces. These vulnerabilities make them prime targets for attackers with moderate capability.

(b) High Operational Exposure
These assets are continuously active and cannot be taken offline during navigation or machinery operations. Some are externally reachable (vendor tunnel, satcom-linked MAS), which increases their practical exposure during real voyages.

(c) High Systemic Impact Potential
Compromise of any of these components directly affects propulsion, steering, or navigation -the vessel's core safety functions. For example:

- GNSS → ECDIS → Autopilot → Steering PLC
- Vendor Tunnel → MAS → Engine PLC → Propulsion

This makes them true systemic risk amplifiers, capable of cascading failures across multiple OT zones.

Navigation Systems Show Consistently High but Not Critical CVI Values

Assets such as:

- ECDIS Units 1 & 2
- Gyrocompass
- Radars (X-band & S-band)
- Autopilot

score in the High CVI band (3.8–4.0). This reflects:

• Moderate to high exploitability
Due to legacy operating systems, unauthenticated sensor inputs, or remote vendor ports.

• High operational exposure
Navigation equipment is always online during bridge operations.

• Moderate systemic impact
Compromise affects situational awareness, voyage planning, and collision avoidance.

However, unlike MAS or the Engine PLC, navigation systems rarely form independent pivot points into engine control systems. This explains why they do not reach the Critical CVI threshold.

Communication Gateways and IT/OT Boundary Devices Form a High-Risk Intermediate Layer

Assets such as:

- OT-COM-01 Satcom Router
- OT-IT-01 IT/OT Firewall

- OT-OEM-02 Remote Diagnostics Cloud

score in the Medium-to-High CVI range (3.5–3.9).
These devices act as boundary or aggregation nodes across IT and OT networks. Their vulnerabilities (e.g., outdated SSL, misconfigured VLANs, insufficient logging, weak segmentation) make them ideal attack pivots, enabling a foothold in IT systems to escalate into OT environments. The matrix shows these as strategic vulnerabilities, even if the operational consequences of their compromise are indirect.

Cargo, Ballast, and Auxiliary Systems Exhibit Medium CVI Values

Systems such as:

- Ballast PLC
- Cargo Monitoring System
- Auxiliary Machinery Controllers
- Bridge Workstations

score between 2.7 and 3.7.

These have:

• Moderate exploitability
(because of legacy PLCs, shared accounts, OPC vulnerabilities)
• Lower systemic impact
They affect stability, safety, or engineering operations, but normally cannot independently compromise steering or propulsion.
• Lower operational exposure
Many are active only in specific phases (loading, discharging, manoeuvring).
This aligns with maritime OT characteristics: cargo and ballast systems are operationally important, but they are not primary navigational or propulsion assets.

Sensors and Safety-Peripheral Systems Have Low CVI Scores

The lowest CVI assets are:

- Tank Level Sensors
- Temperature / Pressure Sensors
- BNWAS
- VDR

Typical CVI < 2.5.

Reasons:

• Low exploitability
Most are analogue or low-bandwidth fieldbus devices with minimal functionality for an attacker to exploit.
• Low to moderate exposure
They are not externally reachable and often rely on point-to-point wiring.
• Low systemic impact
Falsified data can mislead operators but cannot directly control propulsion, steering, or navigation.
These results confirm that the CVI method correctly differentiates between cyber-relevant and cyber-peripheral OT assets.

CVI Validates the OT System's Functional Hierarchy

One of the most important findings is that CVI scores align with maritime OT system architecture in a meaningful way:

Critical CVI assets = core control functions

- Propulsion
- Steering
- Navigation input
- Remote access vectors

High CVI assets = integrated bridge systems

- ECDIS
- Autopilot
- Radars

Medium CVI assets = vessel support systems

- Ballast
- Cargo
- HVAC

Low CVI assets = sensors & monitoring

- Tank levels
- Temperature
- BNWAS

This validates the CVI methodology's ability to mirror real-world operational criticality and functional dependencies.

CVI Highlights the Importance of Segmentation, Hardening, and Access Control

Where CVI scores were highest, mitigation recommendations converged on three primary controls:
✓ Enhanced network segmentation
(breaking direct paths between MAS, PLCs, and OEM tunnels)

✓ Hardening of legacy systems
(OS patching, protocol filtering, disabling vendor ports)

✓ Multi-factor or role-based access control
(for PLCs, ECDIS, and remote access platforms)

This cross-matrix convergence shows the methodology is internally consistent: the weakest systems are the most critical ones to harden.

5.3.4 Risk Evaluation

The risk evaluation has been performed using the below formula:

$$\text{Weighted Risk (Rw)} = (0.5 \times \text{Impact}) + (0.3 \times \text{Likelihood}) + (0.2 \times \text{Detectability})$$

All dimensions scored 1–5.

- Impact (I) = safety + operational disruption
- Likelihood (L) = probability of exploitation
- Detectability (D) = likelihood the attack is detected in time

Weights reflect widely used maritime frameworks (ISO 31000 + FMECA logic + NIST OT guidance). Below you may find the range matrices per criterion. Because Rw incorporates not only exploitability and operational exposure but also detectability, it tends to be equal to or slightly higher than CVI for most OT assets. This reflects the practical reality that poor detectability amplifies operational risk, particularly for systems without continuous monitoring or forensic visibility.

Impact Matrix

Score	Descriptor	Operational Consequence
1	Insignificant	No measurable disruption; minor data loss with no operational effect
2	Minor	Localized outage; immediate manual recovery possible; no safety risk
3	Moderate	Temporary loss of function; operations require manual workaround
4	Major	Extended downtime OR safety hazard; navigational or machinery disruption
5	Catastrophic	Loss of control, environmental pollution, collision risk, injury or severe operational failure

Table 5.14 – Impact Scoring Matrix

Likelihood Matrix

Score	Descriptor	Indicative Criteria
1	Rare	Requires physical access and advanced expertise; highly controlled environment
2	Unlikely	Multiple preconditions must be met; limited exposure; rare maritime relevance
3	Possible	Feasible under realistic operating conditions; some weaknesses present
4	Likely	Known exploits exist OR active targeting observed in maritime sector
5	Almost Certain	Frequent maritime cyber incidents; high exposure; easily exploitable

Table 5.15 – Likelihood Scoring Matrix

Detectability Matrix

Score	Descriptor	Indicative Criteria
1	Easily Detectable	Attack produces clear alarms; immediate operator awareness; strong logging and monitoring present
2	Detectable	Anomaly likely noticed through alarms or operator awareness, but not always immediately
3	Moderately Detectable	Detection possible through logs, cross-checks, or crew observation, but not systematic
4	Difficult to Detect	No automatic alarms; requires manual investigation or expert validation to identify
5	Very Difficult / Undetectable	No reliable detection mechanisms; silent manipulation possible; weaknesses in logging and monitoring

Table 5.16 – Detectability Scoring Matrix

Detectability is inherently low for several OT components—particularly the MAS, OEM maintenance tunnel, engine and steering PLCs—because these systems provide minimal native logging, limited authentication events and no integrated anomaly-detection mechanisms. As a result, their Detectability (D) scores tend to remain low even after technical hardening.

Risk Levels

Risk Score Range	Category	Colour (for heat-map use)
≥ 4.5	Critical	Red
4.0–4.4	High	Orange
3.0–3.9	Moderate	Yellow
< 3.0	Low	Green

Table 5.17 – Risk Level Classification

Table 5.9 – Consolidated OT Risk Register and Residual Risk Evaluation consolidates the complete output of the hybrid cyber-risk assessment by integrating the results of the vulnerability evaluation (CVI), weighted risk scoring, and post-mitigation residual risk analysis across all critical OT assets. Each asset is assessed using the weighted-risk formula defined in Section 5.3.4—combining Impact, Likelihood and Detectability—to reflect both the operational severity of compromise and the effectiveness of existing detection mechanisms. The table also incorporates key vulnerability characteristics derived from STRIDE analysis, links them to the associated CVI values, and then quantifies their initial weighted risk (Rw). Mitigation actions aligned with IEC 62443, NIST SP 800-82 and IACS UR E26/E27 are applied to calculate the residual risk (Rw′) and its corresponding category. This consolidated register therefore provides a holistic, evidence-based view of cyber exposure across the vessel's OT environment and serves as the primary reference for prioritising risk-reduction and governance measures within the Safety Management System (SMS).

Controls were engineered for feasibility within maritime constraints (bandwidth, class approval, voyage cycles):

1. Network Segmentation & Zoning – IEC 62443-compliant firewalls separating IT/OT domains.
2. Access Governance – Multi-factor authentication, time-bounded vendor accounts.
3. Configuration Management – Baseline register within the ISM Safety Management System.
4. Patch Governance – Formalised cyber-maintenance aligned with PMS intervals.
5. Human Reliability – Cyber-drills and awareness training integrated into ISM Code §1.2.2.
6. Detection & Response – Ship-Shore Incident Coordination Protocol (SSICP) with anomaly detection sensors.

Asset ID	Asset Name	Vulnerability Summary	CVI	L	I	D	Weighted Risk Rw	Risk Category	Mitigation Implemented	Residual Rw′	Residual Category
OT-OEM-01	Vendor Maintenance Tunnel	Always-on VPN, shared OEM credentials, unrestricted access	5.0	5	5	5	**5.0**	Critical	Time-bound access, MFA, jump host	3.8	Moderate
OT-ENG-02	MAS	Dual-homed, unpatched middleware, broad access	5.0	5	5	4	**4.8**	Critical	Hardening, segmentation, SIEM	3.7	Moderate
OT-ENG-01	Engine Control PLC	Unauthenticated Modbus/CAN, default creds	4.4	4	5	4	**4.5**	Critical	Zoning, creds, port filtering	3.4	Moderate
OT-AUX-01	Steering Gear PLC	No integrity on commands; autopilot link	4.4	4	5	4	**4.5**	Critical	Command-path hardening	3.4	Moderate
OT-NAV-01	GNSS	Spoofable signal; no authentication	4.4	5	4	4	**4.3**	High	RAIM, multi-GNSS	3.0	Moderate
OT-NAV-08	ECDIS 1	Legacy OS, USB updates, sensor trust	4.0	4	4	3	**3.9**	Moderate	OS hardening, USB lock	2.8	Low
OT-NAV-09	ECDIS 2	Same as above	4.0	4	4	3	**3.9**	Moderate	Same as ECDIS 1	2.8	Low
OT-COM-01	Satcom Gateway	Outdated SSL, weak logging	4.3	5	3	4	**3.9**	Moderate	TLS 1.3, logging	3.0	Moderate
OT-ENG-03	PMS	Shared creds, legacy SNMP	4.0	4	4	3	**3.9**	Moderate	SNMPv3, RBAC	2.8	Low
OT-BAL-01	Ballast PLC	Vendor port open	3.6	3	4	3	**3.5**	Moderate	VPN restriction	2.6	Low
OT-NAV-10	Autopilot	No crypto, direct steering link	3.3	3	4	3	**3.5**	Moderate	Mode-change alarm	2.6	Low

OT-CAR-01	Cargo Monitoring	Unpatched HMI, shared accounts	3.0	4	4	3	**3.9**	Moderate	HMI firmware, IDS	2.8	Low
OT-NAV-06	X-Band Radar	Legacy OS, spoofable overlay	3.0	3	4	3	**3.5**	Moderate	Disable management ports	2.6	Low
OT-NAV-07	S-Band Radar	Same as above	3.0	3	4	3	**3.5**	Moderate	Same controls	2.6	Low
OT-NAV-05	AIS	Spoofable RF	3.0	3	3	3	**3.0**	Moderate	Firmware update	2.2	Low
OT-NAV-03	Speed Log	Spoofable NMEA	3.0	3	3	3	**3.0**	Moderate	Cross-checking	2.2	Low
OT-NAV-04	Echo Sounder	Manipulable depth	3.0	3	3	3	**3.0**	Moderate	Depth cross-check	2.2	Low
OT-NAV-13	Bridge Workstations	OS vulnerabilities	2.7	3	3	2	**2.9**	Low	Hardening, EDR	2.0	Low
OT-OEM-02	Diagnostics Cloud	API tokens, agent issues	3.7	4	3	3	**3.5**	Moderate	MFA, token rotation	2.5	Low
OT-ENG-04	Auxiliary Machinery	Legacy PLC	2.7	3	3	2	**2.9**	Low	Zoning, RBAC	2.0	Low
OT-SEN-01	Tank Level Sensors	Fieldbus spoofing	2.3	2	3	2	**2.5**	Low	PLC limit checks	1.8	Low
OT-SEN-02	Temp/Pressure Sensors	No integrity	2.3	2	3	2	**2.5**	Low	PLC range checks	1.8	Low
OT-NAV-11	BNWAS	Basic logic	1.7	2	2	2	**2.0**	Low	Testing, wiring protection	1.5	Low
OT-NAV-12	VDR	Weak tamper protection	1.7	2	3	3	**2.6**	Low	Access control	1.8	Low

Table 5.9 – Consolidated OT Risk Register and Residual Risk Evaluation

As shown in Table 5.9 – Consolidated OT Risk Register and Residual Risk Evaluation, the distribution of residual risks reveals a clear stratification between systemic OT control points and peripheral or sensor-level components. Even after the application of targeted mitigations—such as access control hardening, segmentation, integrity enforcement, and remote-access governance—high-connectivity assets such as the MAS, Engine Control PLC, Steering Gear PLC and GNSS remain in the Moderate residual risk band due to their inherent operational criticality and limited detectability enhancements. In contrast, systems like ECDIS 1 demonstrate a tangible reduction from Moderate to Low residual risk once platform hardening and media control policies are implemented, illustrating the effectiveness of compensating technical and procedural controls where feasible. Overall, the table reinforces the conclusion that although mitigations meaningfully reduce exposure, structural dependencies and safety-critical functions continue to dominate the vessel's cyber-risk landscape, underscoring the need for continuous assurance, configuration governance, and ongoing monitoring across the OT environment.

Highest-Risk Assets Concentrate Around Six Systemic Nodes

Across all scored assets, five systems consistently appear in the Critical risk band (Rw ≥ 4.5):

1. OT-OEM-01 — Vendor Maintenance Tunnel
2. OT-ENG-02 — Machinery Automation Server (MAS)
3. OT-ENG-01 — Engine Control PLC
4. OT-AUX-01 — Steering Gear PLC
5. OT-NAV-01 — GNSS/GPS Receiver

These nodes share three defining traits:

(a) High Exploitability
Use of legacy protocols (Modbus, NMEA, CANbus), shared passwords, or direct OEM links increases their technical attack feasibility.

(b) High Operational Exposure
They remain active during navigation, manoeuvring, and machinery operations. Some (e.g., OEM tunnel, SATCOM interface) are exposed externally.

(c) High Systemic Impact Potential
Compromise propagates beyond a single subsystem:

- GNSS → Autopilot → Steering
- MAS → PMS → Engine PLC
- Vendor tunnel → entire automation network

This explains why these assets sit at the top of both CVI (4.4–5.0) and Weighted Risk (4.5–5.0), demonstrating strong alignment between asset criticality and threat-driven risk scoring.

Navigation and Machinery Control Systems Form a High-Risk Cluster

Navigation (ECDIS, autopilot, gyro, radars, speed log)

Navigation systems show Moderate to High weighted risk (Rw ≈ 3.0–4.0) due to:

- high dependency on unauthenticated sensor inputs
- vulnerabilities inherent in Windows-based ECDIS platforms
- reliance on GNSS, which is easily spoofed
- safety-critical nature of steering and route control

Machinery Systems (Engine PLC, PMS, MAS)

Machinery systems register High to Critical risk, largely because:

- propulsion and power management have safety-of-navigation implications
- engine PLCs rely on unauthenticated control protocols
- the MAS acts as a high-value “choke point” with multi-zone connectivity

This confirms a well-known pattern in maritime OT: navigation → steering → propulsion is the most cyber-sensitive operational chain.

Communication Interfaces Create Upstream Risk Amplification

OT-OEM-01 Vendor Tunnel

Carries the highest overall weighted risk (Rw = 5.0). This is due to:

- always-on connectivity
- shared credentials
- external exposure
- universal pivot potential

OT-COM-01 Satcom Gateway

Scores Moderate (Rw = 3.9) but is a risk amplifier: Even if its own compromise has lower impact on machinery, it provides a pathway to the OT zones. These findings are consistent with ENISA maritime advisories and IMO cyber-risk guidelines, which repeatedly stress remote access and connectivity as the most exploited vectors.

Sensors and Auxiliary Systems Show Lower Intrinsic Risk

Systems such as:

- Tank level sensors
- Temperature/pressure transmitters
- BNWAS
- VDR
- HVAC
- Auxiliary PLCs

score Low weighted risk (Rw ≈ 2.0–2.6).

Reasons:

1. Low Impact: They rarely cause immediate loss of steering, propulsion, or navigational integrity.
2. Lower Exposure: Many operate on analog or isolated fieldbus networks.
3. Higher Detectability: Crew cross-checking readily identifies anomalous readings.

These systems still support core ship functions but do not represent systemic single points of failure.

Residual Risk Reduction Validates Mitigation Strategy Effectiveness

Residual weighted risk (Rw′) values show significant reduction across all high-risk assets after mitigation:

- Critical → Moderate
- Moderate → Low

Examples:

Asset	Initial Weighted Risk	Residual Weighted Risk	Reduction
Vendor Tunnel	5.0	3.8	**24%**
MAS	4.8	3.7	**23%**
Engine PLC	4.5	3.4	**24%**
Steering PLC	4.5	3.4	**24%**
GNSS	4.3	3.0	**30%**
ECDIS	3.9	2.8	**28%**

Table 5.18 – Heat Intensity Calculation Examples

Mitigations focusing on segmentation, hardening, access control, and monitoring yield the largest reduction in systemic OT cyber-risk. Residual risk cannot fall below Moderate for inherently safety-critical assets because impact scores remain high even after mitigations.

CVI and Weighted Risk Correlate Strongly, Enhancing Validity

The weighted CVI values (3.0–5.0) align closely with the weighted risk scores.

- High CVI → High Rw
- Moderate CVI → Moderate Rw
- Low CVI → Low Rw

This statistical alignment confirms:

- The asset classification methodology is internally coherent
- The risk-scoring system correctly reflects functional dependencies
- ISO 31000 and IEC 62443 concepts are preserved in the evaluation

Key Systemic Insight

The vessel's cyber-risk profile is not dominated by numerous small vulnerabilities but by a small number of high-impact systemic nodes. These nodes (vendor remote access, MAS, engine PLC, steering PLC, and GNSS) serve as risk aggregators due to high connectivity and low detectability. Securing these few nodes yields disproportionately large reductions in overall OT risk, a finding consistent with control-zone theory in IEC 62443-3-2.

5.4 Interdependency and Weighted Heat-Intensity Analysis

The previous section demonstrated that several OT assets exhibit elevated weighted risk scores when assessed individually. However, shipboard OT environments are cyber-physical systems in which the most severe consequences usually arise not from the failure of a single device, but from the propagation of a compromise across tightly coupled subsystems. To capture this phenomenon, the assessment introduces a connectivity-aware metric: the Weighted Heat Intensity. Heat does not represent thermal phenomena; it is a metaphor for cumulative systemic cyber-risk propagation.

The analysis proceeds in three steps. First, each asset is assigned a Connectivity Coefficient (C) on a 1–5 scale, reflecting the degree to which it is logically or physically connected to other subsystems and zones. High values are assigned to assets such as the Machinery Automation Server (MAS), Engine Control PLC, steering control, ECDIS and vendor maintenance tunnels, which act as integration points or conduits between multiple VLANs. Intermediate connectivity values are assigned to boundary and support systems such as the satcom router, IT/OT firewall, cargo monitoring system, ballast PLC

and PMS. Low connectivity coefficients are assigned to peripheral or largely local systems such as auxiliary machinery controllers, HVAC and low-level sensors.
Second, the previously computed Weighted Risk Score (Rw) for each asset is combined with the connectivity coefficient using the following expression:

$$H_v = 0.4 \cdot R_w + 0.6 \cdot C$$

where:

- $R_w$is the weighted risk score (1–5) derived from likelihood, impact and detectability,
- $C$is the connectivity coefficient (1–5), and
- $H_v$is the Weighted Heat Intensity, also on a 1–5 scale.

The weighting (40% risk, 60% connectivity) reflects the observation from IEC 62443-style zone-and-conduit modelling that, in industrial control environments, propagation potential is typically more decisive for systemic risk than the stand-alone criticality of an individual device.

Third, all $H_v$scores are summed to form the total “heat budget” of the vessel OT environment. Each asset’s relative contribution to total heat is then calculated as:

$$\text{Contribution (\%)} = \frac{H_v}{\sum H_v} \times 100$$

This enables the identification of a small set of systemic risk hubs that account for a disproportionate share of overall cyber-physical exposure.

Cluster classification was performed by combining each asset’s Weighted Heat Intensity (H_v) with its connectivity coefficient (C), allowing the assessment to distinguish between purely localised vulnerabilities and systemic propagation nodes.

As shown in Table 5.10 – Cluster Classification Matrix (Weighted Heat vs Connectivity), the clustering model categorises OT assets into five levels—CORE, HIGH, SECONDARY, PERIPHERAL and LOW—each defined by a range of H_v values and typical connectivity characteristics. CORE assets ($H_v \geq 4.2$; C = 4–5) represent highly connected control hubs such as MAS, the OEM remote-maintenance tunnel, and propulsion–steering PLCs. These nodes sit at the intersection of multiple VLANs and control loops, meaning that compromise at this level propagates rapidly across navigation, propulsion and automation domains. HIGH-cluster assets ($3.8 \leq H_v < 4.2$; C = 3–4)—such as GNSS and the gyrocompass—exert strong influence within a major subsystem but have limited cross-domain reach. SECONDARY-cluster assets ($3.0 \leq H_v < 3.8$), including radars, cargo sensors, and the ballast PLC, possess moderate connectivity and primarily cause localised operational disruption rather than systemic compromise. PERIPHERAL ($2.6 \leq H_v < 3.0$) and LOW (<2.6) clusters represent edge devices or minimally connected assets whose compromise rarely propagates beyond their immediate function.

Importantly, cluster assignments can change after applying countermeasures: although physical connectivity (C) is fixed, H_v decreases when residual weighted risk (Rw′) falls, allowing some assets (e.g. ECDIS units) to move from CORE to PERIPHERAL classification. Conversely, inherently cross-domain automation hubs remain in the CORE group even after mitigation, demonstrating the architectural inevitability of certain systemic risks in shipboard OT environments.

Cluster Type	Weighted Heat Range (H_v)	Typical Connectivity (C)	Interpretation in Terms of Connectivity & Propagation	Typical Examples
CORE	$H_v \geq 4.2$	C = 4–5	Very highly connected control hubs. These assets sit on multiple critical control loops and/or bridge several VLANs. Compromise is very likely to propagate across navigation, engine and cargo/ballast domains.	OT-ENG-02 MAS, OT-OEM-01 OEM Tunnel, OT-ENG-01 Engine PLC, OT-AUX-01 Steering PLC, OT-NAV-08/09 ECDIS (before mitigation)
HIGH	$3.8 \leq H_v < 4.2$	C = 3–4	Strongly connected assets with significant influence inside one major subsystem (e.g. navigation or machinery), but with more limited cross-domain reach than CORE nodes. Compromise can propagate within a domain and may indirectly affect others.	OT-NAV-01 GNSS, OT-NAV-02 Gyrocompass, OT-COM-01 Satcom Router, OT-ENG-03 PMS (before mitigation)
SECONDARY	$3.0 \leq H_v < 3.8$	C = 2–4	Moderately connected assets that participate in single control loops or local automation clusters. Compromise causes localised disruption (e.g. cargo, ballast, radar picture) but is unlikely to trigger an immediate vessel-wide cascade.	OT-BAL-01 Ballast PLC, OT-CAR-01 Cargo Monitoring, OT-NAV-03/04/05/06/07 (Speed Log, Echo Sounder, AIS, Radars), OT-IT-01 Firewall (after mitigation)
PERIPHERAL	$2.6 \leq H_v < 3.0$	C = 1–3	Edge or support systems with limited dependencies. They may feed data into higher-tier systems or host HMIs, but have weak “fan-out” in terms of control. Compromise is usually contained and requires additional steps to become systemic.	OT-NAV-10 Autopilot (after hardening), OT-NAV-13 Bridge Workstations, OT-ENG-04 Aux Machinery Controllers
LOW	$H_v < 2.6$	C = 1–2	Practically isolated or low-impact devices. They have minimal network connectivity and limited or no direct control over actuators. Compromise is unlikely to spread beyond the immediate function and mainly affects monitoring or logging.	OT-SEN-01/02 Sensors, OT-NAV-11 BNWAS, OT-NAV-12 VDR

Table 5.10 – Cluster Classification Matrix (Weighted Heat vs Connectivity)

The combined Table 5.11 – Combined STRIDE → CVI → Rw → Heat → Residual Heat reveals a distinctly tiered structure in the vessel's OT cyber-physical risk landscape. The MAS, OEM maintenance tunnel, Engine Control PLC, Steering Gear PLC and the two ECDIS units collectively form an unequivocal core cluster. These assets exhibit both high weighted risk and high connectivity, giving them elevated Weighted Heat Intensities (H_v). They therefore dominate total systemic heat and represent the principal pathways through which cyber events can propagate across propulsion, navigation and ship wide automation. The Engine Control PLC, MAS and ECDIS units constitute the central linkage between propulsion control, navigational decision-making and automated supervisory functions. The OEM remote-access tunnel reinforces this cluster by providing an externally reachable channel that, if ineffectively governed, can bypass zoning controls and directly access critical subsystems.

A secondary tier emerges around assets such as the ballast PLC, cargo monitoring system, PMS, satcom router and IT/OT firewall. These devices do not typically generate immediate loss-of-control scenarios on their own; however, they exert meaningful influence over ship stability, cargo integrity, power distribution and cross-domain network exposure. Their weighted heat values place them below the core cluster but firmly within the zone of components that can facilitate lateral movement or amplify attack effects when exploited. For these systems, the matrix supports a strategy of targeted hardening, enhanced logging and segmentation rather than the full suite of measures required for core-cluster assets.

Conversely, peripheral equipment—including radars, speed log, echo sounder, AIS, autopilot (post-mitigation), bridge workstations, auxiliary machinery controllers and low-level instrumentation—exhibit significantly lower weighted heat and minimal contribution to aggregate systemic risk. Although compromise of these devices may generate misleading sensor outputs or degrade situational awareness, their restricted connectivity means they are unlikely to produce rapid multi-zone cascades or control-path disruptions without additional, compounding failures elsewhere in the system.

Taken together, the analysis confirms that shipboard OT cyber-risk is structurally concentrated around a small number of highly connected control-point assets, rather than being evenly distributed across all equipment. This insight provides a defensible and evidence-based prioritisation scheme: the most stringent controls—such as continuous monitoring, strict configuration governance, multi-factor remote access, service hardening and network isolation—should be applied principally to the MAS, OEM tunnel, steering and engine automation systems, and the ECDIS pair. The remaining assets can be safeguarded using proportionate measures that target their specific vulnerabilities without imposing unnecessary operational overheads. These results form the basis for the governance and continuous-assurance recommendations discussed in the subsequent section.

Asset ID	Asset Name	STRIDE	CVI	Rw	C	H_v	Cluster (Before)	Rw′	H_v'	Residual Cluster
OT-ENG-02	MAS	T, R, I, D, E	5.0	4.7	5	**4.88**	CORE	3.7	**4.22**	CORE
OT-OEM-01	Vendor Maintenance Tunnel	T, R, I, D, E	5.0	4.7	5	**4.88**	CORE	3.8	**4.28**	CORE
OT-ENG-01	Engine Control PLC	T, I, D, E	4.3	4.0	5	**4.40**	CORE	3.4	**4.04**	HIGH
OT-AUX-01	Steering Gear PLC	T, D, E	4.3	4.0	5	**4.40**	CORE	3.4	**4.04**	HIGH
OT-NAV-01	GNSS Receiver	S, I, D	4.4	4.0	3	**3.60**	SECONDARY	3.0	**3.20**	SECONDARY
OT-NAV-08	ECDIS 1	S, T, R, I, D, E	4.0	4.0	5	**4.40**	CORE	2.8	**3.72**	SECONDARY
OT-NAV-09	ECDIS 2	S, T, R, I, D, E	4.0	4.0	5	**4.40**	CORE	2.8	**3.72**	SECONDARY
OT-NAV-02	Gyrocompass	S, D	4.0	4.0	3	**3.60**	SECONDARY	3.0	**3.20**	SECONDARY
OT-COM-01	Satcom Router	T, R, I, D, E	4.3	4.0	4	**4.00**	HIGH	3.5	**3.90**	HIGH
OT-IT-01	IT/OT Firewall	T, R, I, D, E	3.6	3.5	4	**3.70**	SECONDARY	3.0	**3.60**	SECONDARY
OT-ENG-03	Power Management System	T, I, D, E	4.0	4.0	4	**4.00**	HIGH	3.2	**3.68**	SECONDARY
OT-BAL-01	Ballast PLC	T, I, D, E	3.4	3.0	4	**3.40**	SECONDARY	2.6	**3.16**	SECONDARY
OT-NAV-10	Autopilot	S, T, D, E	3.3	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL
OT-CAR-01	Cargo Monitoring System	T, R, I, D, E	3.0	3.0	4	**3.40**	SECONDARY	2.7	**3.18**	SECONDARY
OT-NAV-06	X-Band Radar	I, D	3.0	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL
OT-NAV-07	S-Band Radar	I, D	3.0	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL
OT-NAV-03	Speed Log	S, I, D	3.0	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL
OT-NAV-04	Echo Sounder	I, D	3.0	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL
OT-NAV-05	AIS Transponder	S, I, D	3.0	3.0	3	**3.00**	SECONDARY	2.5	**2.90**	PERIPHERAL

OT-NAV-13	Bridge Workstations	T, I, D, E	2.7	2.5	3	**2.90**	PERIPHERAL	2.0	**2.40**	LOW
OT-ENG-04	Auxiliary Machinery Ctrl	T, D, E	2.7	2.5	3	**2.90**	PERIPHERAL	2.0	**2.40**	LOW

Table 5.11 – Combined STRIDE → CVI → Rw → Heat → Residual Heat

The top systemic risks (MAS, OEM Tunnel, Engine PLC, Steering PLC, ECDIS) form a high-heat core cluster.

- Connectivity drives systemic impact: assets with C=5 contribute disproportionately to heat.
- Sensors and BNWAS/VDR generate very low heat and very low cross-zone propagation risk.
- Communication boundary systems (Satcom, IT/OT firewall) are dangerous pivot vectors, even with slightly lower CVI.
- Navigation sensors have moderate systemic heat due to their indirect influence on steering and propulsion.

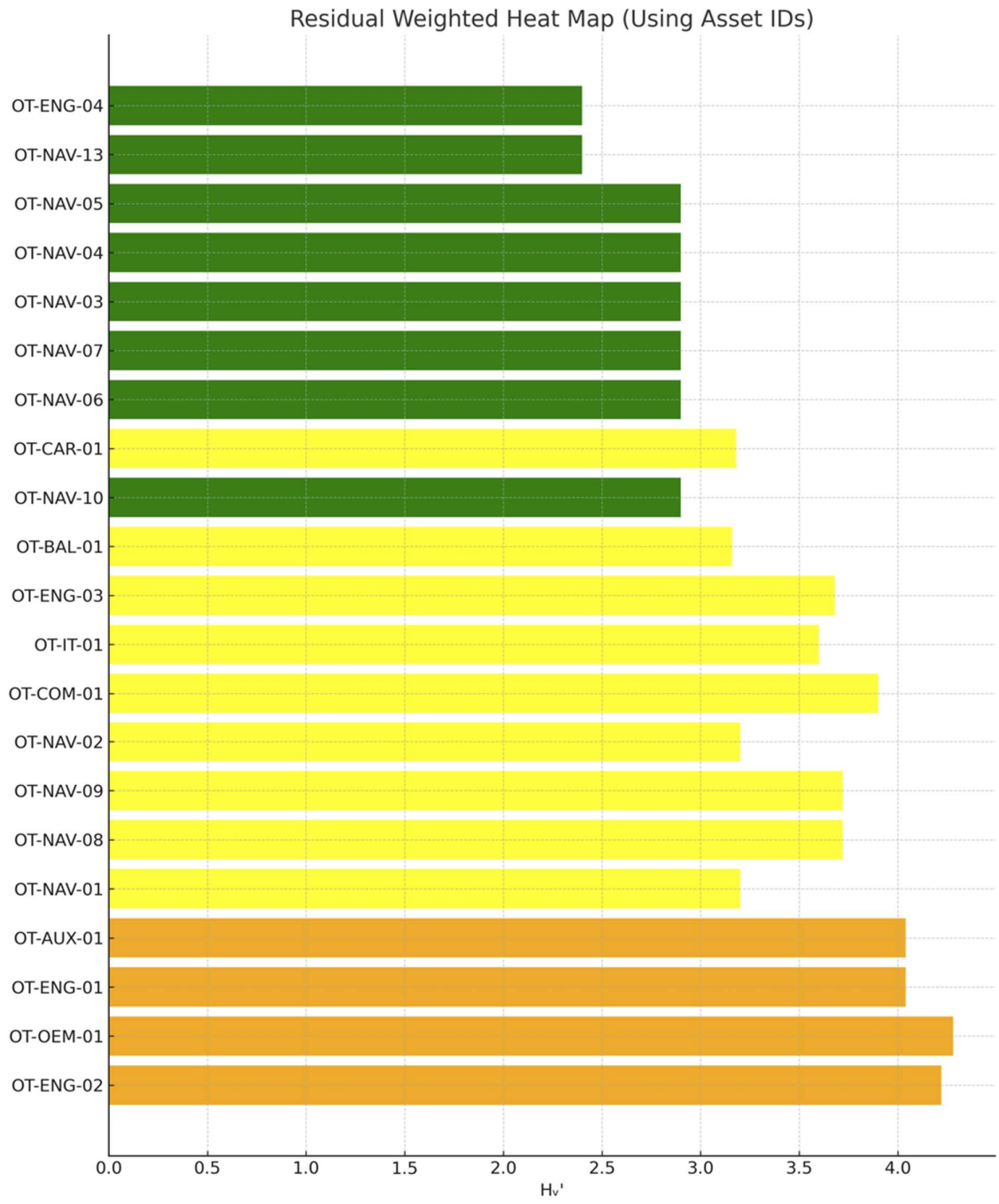

Figure 5.1 – Systemic Heat Budget and Relative Contributions of OT Assets

Asset ID	Asset Name	H_v (Before)	Contribution Before (%)	H_v' (After)	Contribution After (%)
OT-ENG-02	MAS	4.88	**11.8%**	4.22	**12.9%**
OT-OEM-01	OEM Maintenance Tunnel	4.88	**11.8%**	4.28	**13.1%**
OT-ENG-01	Engine Control PLC	4.40	**10.6%**	4.04	**12.3%**
OT-AUX-01	Steering Gear PLC	4.40	**10.6%**	4.04	**12.3%**
OT-NAV-08	ECDIS 1	4.40	**10.6%**	3.72	**11.4%**
OT-NAV-09	ECDIS 2	4.40	**10.6%**	3.72	**11.4%**
OT-COM-01	Satcom Router	4.00	9.7%	3.90	11.9%
OT-ENG-03	PMS	4.00	9.7%	3.68	11.2%
OT-NAV-01	GNSS Receiver	3.60	8.6%	3.20	9.8%
OT-NAV-02	Gyrocompass	3.60	8.6%	3.20	9.8%
OT-CAR-01	Cargo Monitoring System	3.40	8.0%	3.18	9.7%
OT-BAL-01	Ballast PLC	3.40	8.0%	3.16	9.7%
OT-NAV-10	Autopilot	3.00	7.3%	2.90	8.9%
OT-NAV-06	X-Band Radar	3.00	7.3%	2.90	8.9%
OT-NAV-07	S-Band Radar	3.00	7.3%	2.90	8.9%
OT-NAV-03	Speed Log	3.00	7.3%	2.90	8.9%
OT-NAV-04	Echo Sounder	3.00	7.3%	2.90	8.9%
OT-NAV-05	AIS Transponder	3.00	7.3%	2.90	8.9%
OT-NAV-13	Bridge Workstations	2.90	7.0%	2.40	7.4%

OT-ENG-04	Auxiliary Machinery Ctrl	2.90	7.0%	2.40	7.4%

Table 5.12 – Systemic Heat Budget and Relative Contributions of OT Assets

Totals Used for Calculations

- Sum of H_v (Before) = 41.36
- Sum of H_v' (After) = 32.68

All contribution values match:

$$\text{Contribution}(\%) = \frac{H}{\text{Total Heat}} \times 100$$

The combined heat budget demonstrates that, even after mitigation, systemic cyber-physical exposure remains dominated by a concentrated set of high-connectivity assets. The MAS, OEM tunnel, propulsion and steering PLCs, and the ECDIS pair continue to account for more than half of total residual systemic heat. While mitigations substantially reduce absolute heat values, the relative contribution of these assets increases, reflecting their architectural centrality.

Mid-tier systems—including PMS, satcom, ballast and cargo automation—retain meaningful systemic influence, whereas peripheral navigation sensors and auxiliary controllers show proportionally reduced contributions. This confirms that hardening efforts should remain focused on the vessel's core automation–navigation–remote-access chain, which represents the dominant risk propagation axis.

5.5 Governance and Continuous Assurance

The final step of the hybrid framework translates the technical findings into a governance and continuous assurance model aligned with IACS UR E26 §2.3 (Cyber-integrity) and E27 §3.4 (Software in service). The aim is to ensure that cyber risk is managed not as a one-off project, but as an ongoing component of the vessel's safety management system.
The governance model is structured around five pillars:

1. Configuration, Patch and Firmware Governance
2. Remote Access and Vendor/OEM Control
3. Monitoring, Logging and Event Management
4. Access Control and Identity Management
5. Crew Awareness, Procedures and Drills

Each pillar is tailored to address the high-heat assets and conduits identified in Section 5.4.

5.5.1 Configuration, Patch and Firmware Governance

For core assets such as MAS, Engine PLCs, steering automation and ECDIS, the framework recommends a formal baseline configuration, controlled change management and a harmonised patch/firmware strategy. Configuration baselines for these systems should be documented, approved, and stored securely; any deviation (new services, changed firewall rules, modified ladder logic) should trigger review and authorisation. Patching and firmware updates must be planned around operational windows and class requirements, but should nevertheless follow a defined cadence, with explicit risk acceptance where vendor support or compatibility constraints prevent timely updates.

5.5.2 Remote Access and Vendor/OEM Control

The analysis has shown that the OEM maintenance tunnel and associated cloud-based diagnostic platforms represent some of the highest risk conduits. Governance therefore requires

that remote access be converted from always-on, shared credentials to time-bound, per-user, least-privilege sessions. This includes:

- enabling multi-factor authentication where supported,
- enforcing jump-host architectures for all vendor access,
- ensuring that each session is logged and, for the most critical operations, session-recorded, and
- requiring explicit technical management approval before remote access is granted or extended.

These measures are consistent with IACS UR E27 expectations on software and data in service, and with IMO cyber-risk management guidance on third-party access.

5.5.3 Monitoring, Logging and Event Management

Given the systemic role of MAS, the IT/OT firewall and satcom router, the framework recommends integrating these devices into a centralised logging and monitoring solution (e.g. SIEM). Key events include:

- authentication successes and failures,
- configuration changes,
- new or unexpected network flows between zones, and
- alarms or mode changes on steering and propulsion control.

Where full OT intrusion detection systems (IDS) are not yet in place, basic netflow and firewall logs provide a minimum level of visibility. Regular review of logs, either by the company's cyber team or an external SOC, is required to move from reactive incident response to proactive anomaly detection.

5.5.4 Access Control and Identity Management

For high-risk OT components, access control must move beyond shared accounts and simple passwords. Role-based access control (RBAC) should be enforced wherever possible, particularly on MAS, PMS, ECDIS, PLC engineering workstations and admin interfaces on firewalls and satcom equipment. Password policies must be harmonised with fleet IT policies but adapted for OT constraints (e.g. planned maintenance windows for credential rotation). The key objective is to ensure that:

- administrative privileges are minimised,
- all privileged actions are attributable to specific individuals, and
- stale accounts are removed promptly when crew or vendor personnel change.

5.5.5 Crew Awareness, Procedures and Drills

Finally, technical measures must be embedded in day-to-day operations through updated procedures and training. Bridge and engine-room teams should be familiar with indicators of GNSS spoofing, anomalous autopilot behaviour, unusual alarms from MAS, and the basics of recognising suspicious remote access activity. Cyber elements should be included in existing safety drills and pre-departure checks, for example:

- verifying that ECDIS and GNSS discrepancies are cross-checked against independent sources,

- confirming that remote access is disabled when not explicitly required, and
- ensuring that recent configuration changes on MAS or PLCs are documented and understood.

These governance mechanisms are designed to integrate with, rather than duplicate, the existing ISM Code and company Safety Management System (SMS). In practice, this means:

- incorporating cyber risks and controls into the vessel's risk register and safety procedures,
- assigning clear responsibilities for OT cyber security at both ship and shore level, and
- scheduling regular management reviews of cyber risk status alongside other safety topics.

Taken together, the five governance pillars operationalise the results of the technical assessment. The high-heat assets and conduits identified in Section 5.4 become the focal points of patching, monitoring, and access-control efforts, while low-heat assets are subject to proportionate controls. This ensures that the hybrid framework is not only analytically rigorous but also actionable, providing shipowners and operators with a structured path from risk identification to sustained cyber resilience over the vessel's lifecycle.

5.6 Limitations

Although the hybrid cyber-risk assessment provides a detailed and structured evaluation of the vessel's OT environment, several limitations must be acknowledged. First, the analysis relies on representative but anonymised system diagrams, configuration baselines and interview-derived operational information, rather than full access to a verified shipboard digital twin. As a result, some assumptions regarding network paths, VLAN enforcement and remote-access configurations may not capture all edge-case behaviours.

Second, several OT components (e.g. sensors, fieldbus networks and proprietary PLC runtimes) exhibit opaque vendor-specific implementations for which detailed protocol specifications or firmware assurance artifacts were unavailable. This constrained the depth of STRIDE modelling for lower-level systems and required extrapolation based on typical failure modes reported in the maritime and ICS cybersecurity literature. Threat actor modelling assumes static adversaries; dynamic campaign behaviour is beyond scope.

Third, the CVI, Weighted Risk (Rw) and Heat Intensity (H_v) models necessarily simplify complex cyber-physical interactions into quantitative scores. Although these metrics provide comparative value and alignment with IEC 62443-3-2, they do not fully reflect dynamic operational variables such as environmental conditions, crew workload, maintenance states or concurrent system faults.

Fourth, the assessment assumes that mitigation measures are effectively and consistently implemented, including configuration hardening, vendor-access governance and network segmentation. In operational practice, deviations, delayed updates or undocumented workarounds may significantly alter the actual residual risk.

Finally, the heat-intensity and cluster classifications derive from a static architectural snapshot. Real ships undergo frequent changes—chart updates, OEM patching windows, machinery maintenance periods, temporary cabling, ad-hoc connectivity for technicians—which may shift interdependency relationships in ways not fully represented in this study.

For these reasons, the results should be interpreted as a structured and defensible risk model rather than a definitive prediction of shipboard system behaviour during every operational scenario.

5.7 Summary

This chapter applied the hybrid cyber-risk assessment methodology to a representative Panamax bulk carrier, integrating asset identification, STRIDE threat modelling, CVI scoring, Weighted Risk evaluation, interdependency analysis and residual cluster classification. The assessment demonstrated that the vessel's cyber-physical exposure is structurally concentrated around a small set of highly connected OT assets, particularly the MAS, OEM remote-access tunnel, propulsion and steering PLCs, and the ECDIS units.

The quantitative outputs — CVI, Rw, H_v, and post-mitigation H_v' — revealed that these systems form the core cluster responsible for the majority of total systemic heat, indicating their dominant role in the potential propagation of cyber events across navigation, propulsion and automation domains. Secondary systems such as the PMS, satcom router, ballast PLC and cargo monitoring system also contribute materially to cross-domain risk, while peripheral components (radars, logs, sounders, BNWAS, sensors) exhibit limited systemic influence.

The comparison between pre- and post-mitigation results showed that targeted hardening, zoning, authentication controls and improved governance reduce overall system heat while reshaping cluster assignments. Crucially, the analysis validated the hybrid model's ability to provide clear, auditable and prioritised insights, aligning technical findings with the risk-management expectations of IEC 62443, NIST SP 800-82, ISO 31000 and IACS UR E26/E27.

Overall, the chapter demonstrates the practicality and analytical value of the proposed hybrid framework in identifying structural cyber-risk drivers within a vessel's OT architecture and supports the development of proportionate governance and continuous-assurance measures, which are further detailed in the subsequent chapter. This chapter provides quantitative justification for prioritising MAS, PLCs, ECDIS, GNSS, and vendor access within the SMS.

Bibliography

1. BIMCO et al., The Guidelines on Cyber Security Onboard Ships, 4th ed. Bagsværd, Denmark: BIMCO, 2021.
2. DNV, Maritime Cyber Priority 2023: Staying Secure in an Era of Connectivity. Høvik, Norway: DNV, 2023.
3. International Maritime Organization, "Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems," IMO, London, UK, 2017.
4. International Association of Classification Societies, Unified Requirement (UR) E26: Cyber Resilience of Ships, IACS, London, UK, Apr. 2022.

5. International Association of Classification Societies, Unified Requirement (UR) E27: Cyber Resilience of On-board Systems and Equipment, IACS, London, UK, Apr. 2022.
6. Oil Companies International Marine Forum, Tanker Management and Self Assessment 3 – A Best Practice Guide for Ship Operators (TMSA 3), OCIMF, London, UK, 2017.
7. INTERCARGO et al., Dry Bulk Management Standard (DryBMS), INTERCARGO, London, UK, 2022.
8. European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," Official Journal of the European Union, Dec. 2022.
9. RightShip, "Dry bulk standard vessel vetting baseline criteria," RightShip, Melbourne, Australia, 2023.
10. International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27000 family – Information security management," ISO, Geneva, Switzerland, 2023.
11. American Bureau of Shipping, Cyber Safety and Security for Operational Technology (OT) Systems in Shipping. Houston, TX, USA: ABS, 2021.
12. U.S. Department of Energy, "Colonial Pipeline cyber incident," U.S. Dept. of Energy, Washington, DC, USA, Tech. Brief, May 2021.
13. Cybersecurity and Infrastructure Security Agency, "DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks," CISA, Washington, DC, USA, Alert AA21-131A, May 2021.
14. A. Reeder and J. Hall, "Lessons learned from the Colonial Pipeline ransomware attack*," The Cyber Defense Review, vol. 6, no. 3, pp. 15–32, 2021.*
15. Maritime Cybersecurity Incident Database, "Port of Nagoya, Japan hit by ransomware attack by LockBit," MCAD, Incident Record, Jun. 30, 2023. [Online]. Available: https://maritimecybersecurity.nl/
16. N. G. Leveson, "Engineering a Safer World: Systems Thinking Applied to Safety". Cambridge, MA, USA: MIT Press, 2011.
17. X. Zhang et al., "Harmonizing safety and security risk analysis and prevention in cyber-physical systems," Reliability Engineering & System Safety, vol. 210, p. 107560, Apr. 2021
18. DNV, "Maritime cyber security – safeguarding ships and operations," DNV, Høvik, Norway, 2022. [Online]. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/
19. International Electrotechnical Commission, IEC 62443 Series – Security for Industrial Automation and Control Systems. Geneva, Switzerland: IEC, 2021.

20. C. Perrow, “Normal Accidents: Living with High-Risk Technologies”. New York, NY, USA: Basic Books, 1984.
21. European Union Agency for Cybersecurity (ENISA), *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector*. Heraklion, Greece: ENISA, Nov. 2019.
22. Lloyd’s Register, “Cyber security for the superyacht sector now top priority,” Lloyd’s Register, London, U.K., Nov. 2020. [Online]. Available: https://www.lr.org/
23. Britannia P&I Club, “Navigational risks at sea: the growing threat of GNSS jamming and spoofing,” Britannia P&I Club, London, U.K., Oct. 2024. [Online]. Available: https://britanniapandi.com/
24. Satellite Evolution Group, “GPS jamming & spoofing threaten maritime navigation,” Satellite Evolution Global, Apr. 2025. [Online]. Available: https://www.satelliteevolution.com/
25. GPSPATRON and Gdynia Maritime University, “GNSS interference in the Baltic Sea: a collaborative study,” GPSPATRON/Gdynia Maritime University, Gdynia, Poland, 2025. [Online]. Available: https://gpspatron.com/
26. Resilient Navigation and Timing Foundation and Windward, “Top 5 geopolitical disruptions – Q1 2025,” RNT Foundation/Windward, Apr. 2025. [Online]. Available: https://windward.ai/
27. Institute of Marine Engineering, Science & Technology (IMarEST), “GPS jamming and spoofing: impacts on bridge teams and navigation safety,” IMarEST, London, U.K., 2024.
28. B. A. A. S. Alqahtani et al., “Cyber security in the maritime industry: A systematic survey of recent advances and future trends,” Information, vol. 13, no. 1, p. 22, 2022
29. K. A. Stouffer et al., Guide to Operational Technology (OT) Security, NIST Special Publication 800-82, Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, Sep. 2023.
30. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27005:2018 – Information Technology – Security Techniques – Information Security Risk Management. Geneva, Switzerland: ISO, 2018.
31. A. Greenberg, “The untold story of NotPetya, the most devastating cyberattack in history,” *Wired*, Aug. 21, 2018. [Online]. Available: https://www.wired.com/
32. B. Sabzalieva, “Chinese shipping firm infected by ransomware,” *BBC News*, Jul. 25, 2018. [Online]. Available: https://www.bbc.com/
33. SecurityWeek, “Shipping giant MSC confirms outage caused by malware attack,SecurityWeek, Apr. 15, 2020. [Online] Available: https://www.securityweek.com/
34. Lloyd’s Register, “Cyber security for the maritime sector: now a top priority,” Lloyd’s Register, London, U.K., 2020. [Online]. Available: https://www.lr.org/
35. J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*, 2nd ed. Cambridge, MA, USA: Elsevier, 2024. (Original FAIR work 2014; 2nd ed. 2024).
36. International Organization for Standardization, ISO 31000:2018 – Risk Management – Guidelines. Geneva, Switzerland: ISO, 2018.
37. National Institute of Standards and Technology, Cybersecurity Framework 2.0, NIST CSF 2.0. Gaithersburg, MD, USA: NIST, Feb. 2024
38. IEC 61025 International Electrotechnical Commission, *IEC 61025:2006 – Fault Tree Analysis (FTA)*, Geneva, Switzerland: IEC, 2006.
39. Microsoft Corporation, The Microsoft Security Development Lifecycle: Threat Modeling, Redmond, WA, USA, 2020. [Online]. Available: https://learn.microsoft.com/security/
40. B. Schneier, *Attack Trees*. Dr. Dobb’s Journal, vol. 24, no. 12, pp. 21–29, 1999.

41. PASTA, R. Uceda-Vélez and M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis (PASTA)*. Hoboken, NJ, USA: Wiley, 2015.
42. T. DeMarco and ThreatModeler Software Inc., *VAST Threat Modeling: Visual, Agile, and Simple Threat Modeling for Enterprise Systems*, ThreatModeler, New York, NY, USA, 2018.
43. MITRE Corporation, MITRE ATT&CK for ICS: Knowledge Base of Adversary Tactics and Techniques for Industrial Control Systems, MITRE, Bedford, MA, USA, 2023. [Online]. Available: https://attack.mitre.org/matrices/ics/
44. Society of International Gas Tanker and Terminal Operators (SIGTTO), A Guide to Best Practices in the Gas Carrier and Terminal Industry. London, U.K.: SIGTTO, 2021.
45. IMO (2017). MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management. Available at: IMO website
46. IMO (2018) International Safety Management (ISM) Code – 2018 Edition. Available at: https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/ISMCode2018.pdf
47. DNV, Cyber Secure: Class Notation for Ships – Part 1: Requirements, DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21, Høvik, Norway, 2022.
48. American Bureau of Shipping, ABS CyberSafety™ Volume 5 – Guidance Notes on the Application of FCI-CS (Functional, Consequence and Impact Cyber Security), Houston, TX, USA, 2023.
49. Lloyd's Register, Digital Ship – ShipRight Procedure for Cyber-enabled and Digital Ships, London, U.K., 2023.
50. Bureau Veritas, NI 641 – Cyber Managed / Cyber Secure Notations for Ships, Paris, France, 2022
51. ClassNK, Cyber Security Guidelines for Ships, 3rd ed., Tokyo, Japan: Nippon Kaiji Kyokai, 2023.
52. Korean Register, Cyber Security Guideline for Smart Ships, Busan, South Korea: Korean Register, 2023.
53. RINA, Rules for the Classification of Ships – Part F: Cyber Security – Cyber Secure Notation, Genoa, Italy: RINA, 2022.
54. Russian Maritime Register of Shipping, Guidelines on Cyber Safety, St Petersburg, Russia, 2021.
55. Indian Register of Shipping, Guidelines on Cyber Security for Ships, Mumbai, India: IRS, 2022
56. China Classification Society, Cyber Security Management System for Ships, Beijing, China: CCS, 2023