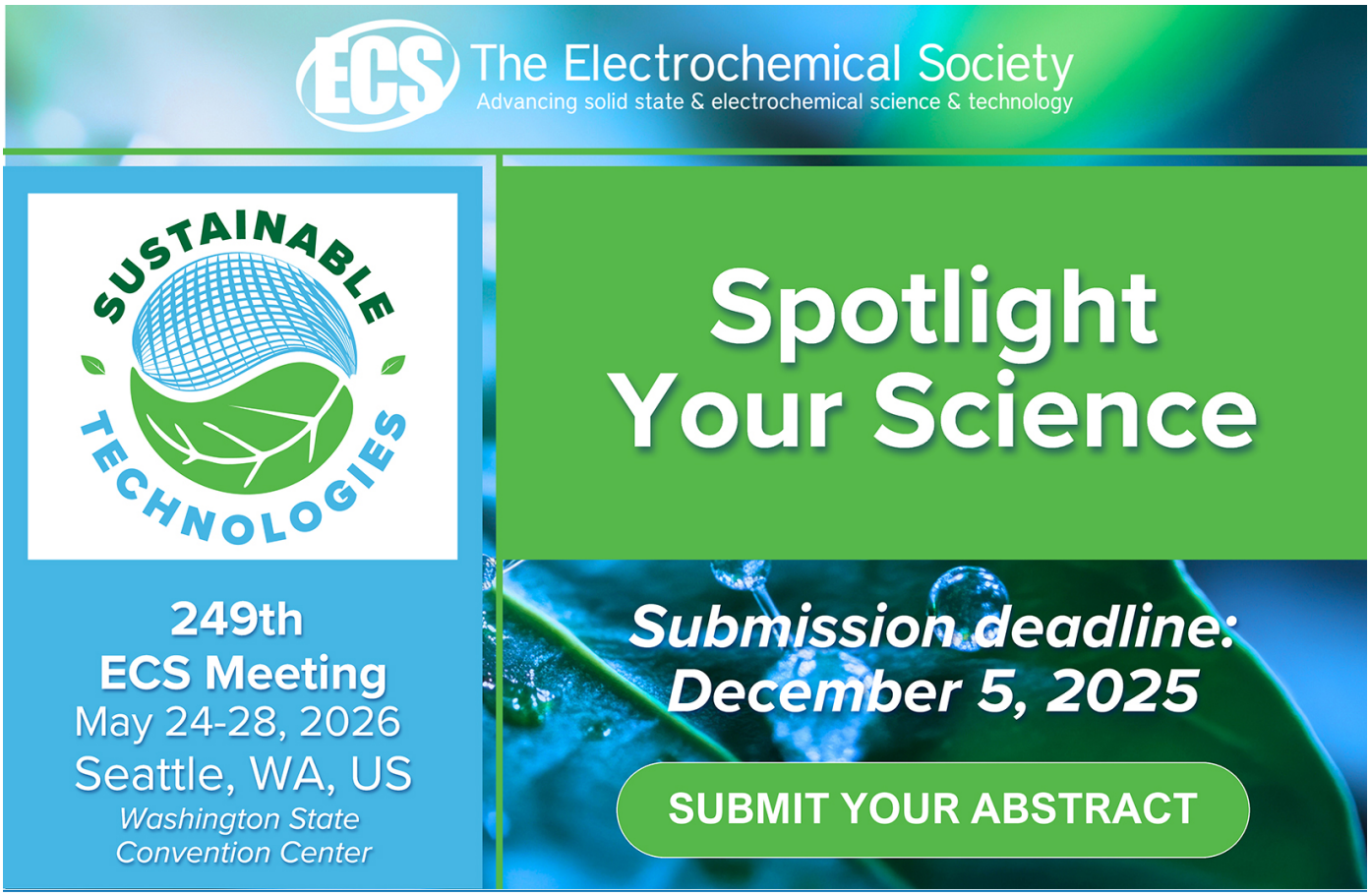
Journal of Physics:
Conference Series

PAPER • **OPEN ACCESS**

Security Challenges in Commercial off-the-shelf Equipment Integration for Small Autonomous Vessels: A Security-by-Design Approach

To cite this article: Juha Kalliovaara *et al* 2025 *J. Phys.: Conf. Ser.* **3123** 012036



Journal of Physics: Conference Series **3123** (2025) 012036 doi:10.1088/1742-6596/3123/1/012036

Security Challenges in Commercial off-the-shelf Equipment Integration for Small Autonomous Vessels: A Security-by-Design Approach

Juha Kalliovaara[1,2,*], **Juhani Hallio**[1], **Jesse Väänänen**[1], **Tero Jokela**[1]

[1]Faculty of ICT and Industrial Engineering, Turku University of Applied Sciences, 20520 Turku, Finland
[2]Department of Computing, University of Turku, 20014 Turku, Finland

E-mail: juha.kalliovaara@turkuamk.fi

Abstract. This study examines the security implications of commercial off-the-shelf (COTS) equipment used in small vessels (<25m) transitioning to autonomous operations, emphasizing a comprehensive security-by-design approach. The eM/S Salama autonomous test vessel is introduced as a representative use case, which is used to identify critical vulnerabilities in maritime technologies designed primarily for consumer markets, where usability often compromises security considerations.

Our research reveals multifaceted security challenges including communication system weaknesses, cyber-physical integration vulnerabilities, data integrity issues, inadequate cyber-attack response mechanisms, and regulatory compliance gaps. These challenges are compounded by integration difficulties in wireless technologies, cloud connectivity, and Controller Area Network (CAN) bus systems, where manufacturers' security features remain inconsistently implemented due to cost and complexity constraints typical of small vessel operations.

We propose a systematic seven-step security assessment framework encompassing asset categorization and inventory, Information Technology (IT) / Operational Technology (OT) integration requirements, physical security controls, device-level security evaluation, communication system security, human-centric security and operational resilience, and continuous monitoring and assessment. The framework provides quantitative scoring methodologies and practical implementation guidance specifically adapted for resource-constrained maritime environments, enabling systematic evaluation of COTS equipment security posture.

This security-by-design methodology addresses the fundamental challenge of maintaining robust security while enabling autonomous operations in cost-sensitive maritime environments. The framework offers assessment tools and evaluation matrices suitable for small vessel operations, bridging the gap between theoretical cybersecurity models and practical implementation in autonomous maritime systems.

1 Introduction

The maritime sector is rapidly adopting commercial off-the-shelf (COTS) technologies to enable autonomy in small vessels (<25 m). While these systems improve navigation, monitoring, and automation, they introduce significant cybersecurity risks due to a mismatch between consumer-grade design and maritime operational requirements. Unlike large ships with dedicated cybersecurity systems, small vessels often rely on cost-driven technologies [1], creating complex Information Technology (IT) / Operational Technology (OT) integration challenges and new attack surfaces [**2**]. IT refers to systems such as navigation and communication, while OT refers to systems such as propulsion and control mechanisms.

Recent findings, such as the U.S. Coast Guard Cyber Command's 2023 CTIME report [3], highlight a growing trend of sophisticated cyberattacks targeting navigation, communication, and propulsion systems. These attacks, including ransomware and advanced persistent threats, often exploit vulnerabilities in hastily integrated COTS components lacking standardized protocols and manufacturer support.

Figure 1 illustrates the interconnected nature of modern maritime systems, where IT and OT integration creates multiple attack surfaces. This complexity increases the risk of environmental hazards, safety incidents, and financial losses, especially when COTS equipment fails to maintain clear boundaries between critical and non-critical systems.

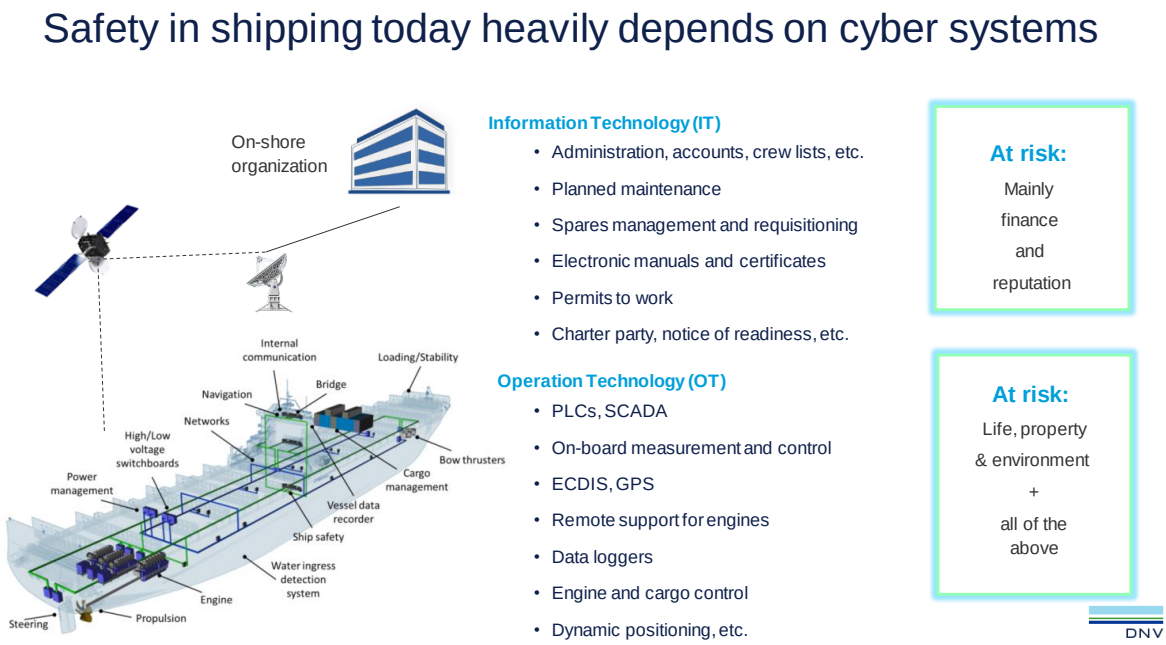


Figure 1: Smart shipping system architecture. Adapted from [4].

This study identifies critical security challenges in COTS integration, including communication system weaknesses due to insufficient encryption and authentication, cyber-physical integration vulnerabilities at IT/OT boundaries, data integrity issues across distributed systems, inadequate cyber-attack response mechanisms in resource-limited environments, and regulatory compliance gaps. These vulnerabilities are compounded by integration challenges where manufacturers' security features remain inconsistently implemented due to cost and complexity constraints typical of small vessel operations.

Using the electric motor ship (eM/S) Salama test vessel developed by Turku University of Applied Sciences [5] as a conceptual validation platform, this research identifies key security challenges and proposes a generalizable security-by-design methodology.

The systematic seven-step security assessment framework encompasses: asset categorization and inventory, IT/OT integration requirements, physical security controls, device-level security evaluation, communication system security, human-centric security and operational resilience, and continuous monitoring and assessment.

This paper contributes to the field by (1) systematically identifying and analyzing critical security challenges in COTS integration for small autonomous vessels, (2) developing a comprehensive seven-step

security evaluation framework with quantitative scoring methodologies that integrate cybersecurity, physical security, human factors, and operational resilience, and (3) providing practical assessment matrices and evaluation tools with specific implementation guidance tailored for resource-constrained maritime environments. These contributions bridge the gap between theoretical cybersecurity models and real-world implementation, offering actionable guidance for vessel developers and operators navigating the transition to autonomy.

This paper is organized as follows. Section 2 reviews literature and related work on cybersecurity in the maritime domain, identifying gaps in practical implementation guidance. Section 3 presents the eM/S Salama test platform as a case study, demonstrating real-world manifestation of identified security challenges. Section 4 introduces the proposed seven-step security evaluation framework, including detailed assessment matrices, quantitative scoring methodologies, and practical implementation guidance. Section 5 concludes the paper and outlines directions for future research.

2 Literature Review and Related Work

Cybersecurity challenges in maritime COTS integration have gained increasing attention, particularly as autonomous vessels become more prevalent. The comprehensive review by Li et al. [6] provides an extensive analysis of maritime cybersecurity challenges across multiple domains, presenting an in-depth analysis of threats in key maritime systems and exploring real-world cyber incidents.

Recent systematic reviews reveal significant methodological inconsistencies across existing frameworks. Erbas et al. (2024) [7] conducted a comprehensive systematic literature review of threat modeling and risk assessment in ship cybersecurity, highlighting the lack of standardized approaches and noting that significant inconsistencies in current approaches require standardized frameworks and tool support. Similarly, Chaal et al. (2023) identified that cybersecurity overlaps significantly with safety considerations, emphasizing the need for co-analysis methods and integrated approaches [8].

Empirical evidence of real-world maritime cybersecurity challenges comes from multiple sources. Meland et al. (2021) conducted a retrospective analysis of 46 maritime cyber security incidents from 2010-2020, demonstrating that the maritime sector typically has incidents with low frequency and high impact, which makes them hard to predict and prepare for, and there is no single solution to this problem [9]. Their analysis, combining data from open publications and insurance claims, provides crucial empirical evidence of cybersecurity vulnerabilities in operational maritime systems.

Recent research by Raymaker et al. (2025) provides unique insights from mariners' perspectives through surveys and interviews with 21 officer-level mariners, revealing systemic and human-centric issues, such as training poorly aligned with maritime needs, insufficient detection and response tools, and serious gaps in mariners' cybersecurity understanding [10]. Their study documents direct mariner experiences with shipboard cyber-attacks, including positioning system spoofing and logistics-disrupting ransomware.

This section reviews the current state of cybersecurity frameworks in maritime contexts, examining both general adaptations and maritime-specific approaches, analyzing COTS integration challenges, and identifying key implementation gaps that inform our proposed framework.

2.1 Maritime-Specific Security Approaches and Frameworks

Several frameworks specifically addressing maritime cybersecurity challenges have been developed. The concept of "cyber-seaworthiness" emphasizes the convergence of IT and OT systems as a critical vulnerability area, advocating for holistic approaches that include policy, training, and risk communication [11]. The Maritime Cyber Risk Assessment (MaCRA) framework offers dynamic risk modeling tailored to maritime contexts [12]. Kavallieratos et al. (2020) [13] applied Maritime Architecture Framework and Secure Tropos methodologies to elicit security requirements for critical maritime systems, identifying that Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), and Global Maritime Distress and Safety System (GMDSS) are particularly vulnerable [13].

Recent research demonstrates diverse methodological approaches to maritime cybersecurity. Bolbot et al. (2020) developed an enriched Cyber-Preliminary Hazard Analysis specifically adapted for autonomous vessel applications, successfully identifying critical attack scenarios in inland waterways and cargo vessels through the AUTOSHIP project [14]. Their research noted that research is scarce and non-systematic in this domain, highlighting the gap our framework addresses.

The International Maritime Organization (IMO) Resolution MSC.428(98) [15] mandates that companies operating commercial vessels over 500 gross tonnage and passenger ships engaged on international voyages must integrate cyber risk management into their Safety Management Systems (SMS) under the International Safety Management (ISM) Code framework. However, this mandate does not extend to

smaller vessels below 25 meters in length considered in this article, creating a regulatory gap that our research addresses.

2.2 General Cybersecurity Framework Applications in Maritime Context

General frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework have been widely adopted in maritime contexts due to their flexibility and industry recognition [16]. However, they often lack the maritime-specific detail needed for effective COTS integration.

Recent research has extensively applied threat modeling methods to maritime systems. Kavallieratos and Katsikas (2020) combined STRIDE, DREAD, and NIST Industrial Control Systems (ICS) overlay to propose baseline controls for cyber-physical maritime systems, reporting increased exposure to cyber risks and the need for comprehensive baseline controls [17].

Amro et al. (2020, 2022) developed sophisticated assessment approaches, first applying a six-step model with STRIDE for communication system analysis in autonomous passenger ships, then combining Failure Modes, Effects, and Criticality Analysis (FMECA) with MITRE ATT&CK framework for more granular risk assessment [18, 19]. Their research demonstrated that connectivity managers are highly susceptible to cyber threats and recommended secure protocols, incident response, and monitoring as essential mitigations.

Adaptations of the MITRE ATT&CK framework have focused on maritime-specific attack detection and situational awareness [20]. Laboratory demonstrations have validated the feasibility of sophisticated attacks, including AIS-based covert channels that exploit standard maritime protocols [21].

2.3 COTS Equipment Vulnerabilities and Integration Challenges

COTS components commonly used in small autonomous vessels—such as Raspberry Pi systems, legacy Windows installations, and unpatched embedded devices—pose significant security risks due to inconsistent patching and limited manufacturer support [22]. Communication protocol vulnerabilities, particularly in AIS, have been exploited to demonstrate command and control compromises, underscoring the need for stronger authentication and anomaly detection mechanisms.

COTS integration challenges have been addressed by Grigoriadis et al. (2021), who focused on integration and validation of maritime transport security services, identifying research and implementation gaps in integrating multiple security services including risk/threat management, system hardening, trust management, secure communications [23]. Their work highlighted the complexity of integrating diverse COTS components while maintaining security integrity.

The AUTOSHIP project, examining both Short Sea Shipping cargo vessels and Inland Waterways barges, identified regulatory gaps and essential hazards while presenting mitigation measures, though cybersecurity specifics were noted as requiring further development [24].

2.4 Implementation Challenges

Despite available frameworks, real-world maritime cybersecurity implementation faces significant barriers. A systematic review highlights the lack of empirical validation and standardization across proposed models [7], while surveys emphasize the critical need for improved cyber-security awareness community-wide [25].

Current approaches lack standardization, with studies employing different assessment methodologies without comparative validation. Most research focuses on larger commercial vessels, leaving small vessel security adaptations underexplored. Comprehensive frameworks specifically for COTS security evaluation in maritime environments are lacking. Human factors present the most critical challenge, with empirical research revealing serious gaps in mariners' cybersecurity understanding and training programs poorly aligned with maritime operational needs, particularly for small autonomous vessel operations [10, 11].

2.5 Framework Contributions

This review reveals a clear gap between theoretical frameworks and practical implementation, particularly for small vessel operations. Recent research demonstrates limited empirical validation, with different frameworks providing solid theoretical foundations but lacking adaptation to resource-constrained maritime environments with operational realities, cost constraints, and limited crew capabilities.

Our proposed seven-step security evaluation framework addresses these identified gaps by providing systematic methodology designed for small vessel constraints, comprehensive COTS-focused evaluation criteria, quantitative scoring enabling consistent assessment, and practical implementation guidance based on real-world application.

The following section demonstrates how these theoretical challenges manifest in practical autonomous vessel operations through the eM/S Salama case study.

3 Case Study: eM/S Salama Test Platform

To demonstrate the practical relevance of the identified security challenges and the applicability of our proposed framework, we examine Turku University of Applied Sciences' autonomous test vessel eM/S Salama and its associated remote operation center (ROC) [5]. This platform serves as a real-world testbed for evaluating COTS integration in small autonomous vessels.

3.1 Platform Overview and Security Context

The eM/S Salama is a 6.8-meter aluminum catamaran with electric propulsion (20 kW total power). The vessel is illustrated in Figure 2. It integrates a wide range of COTS components, making it representative of small autonomous vessels operating under cost and resource constraints. The vessel's architecture combines Ethernet-based IT systems with Controller Area Network (CAN) based National Marine Electronics Association 2000 (NMEA2000) protocols, which are typically categorized under OT. This combination illustrates the integration challenges between legacy OT protocols and modern IT infrastructure, especially in small autonomous vessels where system boundaries are often blurred.

Figure 2: Uncrewed Surface Vessel eM/S Salama.

3.2 Network Architecture and Security Implications

The vessel employs a three-network segmentation model:

- **Vessel Navigational Network:** Supports manual operations using radar, sonar, and proprietary navigation software. While mature, these systems often lack modern cybersecurity features and rely on physical isolation.
- **Remote Operation Network:** Connects the vessel to external operators via Virtual Private Network (VPN) over commercial mobile networks. This introduces dependencies on third-party infrastructure and creates a critical attack surface.
- **Sensor Network for Autonomous operations:** Includes Light Detection and Ranging (LiDAR), cameras, and Inertial Measurement Unit (IMUs) for situational awareness. These consumer-grade components are cost-effective but often lack robust security features.

These networks are separated and only remote operation network is accessible through the VPN tunnel.

3.3 Control System Architecture and Vulnerabilities

The vessel's control system includes manual, remote, and autonomous modes. Manual systems (e.g., hydraulic steering) offer minimal cyber exposure. The remote and autonomous architectures are built around a distributed Dynamic Control Unit (DCU) system:

- **DCU Commander:** Interfaces with the ROC, handling external communications and acting as the primary attack surface.
- **DCU Motor:** Controls propulsion. A compromise could lead to unauthorized speed changes or propulsion loss.
- **DCU Rudder:** Manages steering and autopilot. Attacks here could cause course deviation or navigation failure.

The DCU components are all in-house products that enable controlling the steering and propulsion systems of the boat via control commands from ROC as IP messages. They convert IP traffic into proprietary signals (analog and digital) that drive traditional marine equipment.

This distributed architecture increases flexibility but also the attack surface. Secure inter-unit communication, authentication, and encryption are essential to prevent spoofing or unauthorized control. The lack of strict separation between critical and non-critical systems can enable lateral movement once access is gained.

3.4 Physical Security Implementation

The vessel demonstrates varying levels of physical security:

- **High-security compartments** (e.g., battery and motor controllers) are sealed and difficult to access.
- **Medium-security areas** (e.g., navigation computers) are protected by standard marine locks.
- **Low-security components** (e.g., external sensors) are exposed and vulnerable to tampering.

3.5 Communication Security Challenges

The communication architecture reveals several vulnerabilities:

- **Commercial network reliance** introduces third-party risks and potential single points of failure.
- **VPN implementation** requires robust key management and monitoring, which are often lacking in COTS setups.

3.6 COTS Integration Security Lessons

The eM/S Salama platform highlights key lessons:

- **Consumer-grade vulnerabilities** are prevalent in sensors and computing components.
- **IT/OT convergence** introduces integration complexity and new attack surfaces.
- **Remote operation** expands the threat landscape by introducing an extra attack vector through communication channels. The VPN needs to be configured in a robust way. Furthermore, proper key management and continuous monitoring is needed to secure the connection.
- **Resource constraints** limit the feasibility of comprehensive security implementations.

This case study confirms that the security challenges identified in the literature are not only theoretical but manifest in real-world autonomous vessel operations. The eM/S Salama platform provides empirical grounding for the development of our security evaluation framework, demonstrating the need for structured, resource-aware approaches to COTS integration in small maritime systems.

4 Security Evaluation Framework for COTS Integration in Autonomous Maritime Systems

To address the multifaceted security challenges associated with integrating COTS components into small autonomous vessels, this chapter presents a structured evaluation framework tailored to maritime environments.

4.1 Framework Overview and Process Flow

The security evaluation framework presented here is informed by the eM/S Salama case study but designed as a generalized methodology applicable to any small autonomous vessel integrating COTS components. The assessment matrices, risk scoring methodologies, and evaluation criteria represent tools that can be applied across diverse vessel types, operational contexts, and equipment configurations, with specific lessons from the Salama implementation demonstrating practical application where relevant.

The cyber-physical security and operational resilience framework presented in Figure 3 provides a systematic approach to evaluating and enhancing security in small autonomous maritime vessels integrating COTS components. This framework addresses the gap identified in our literature review, where existing cybersecurity frameworks often lack maritime-specific considerations or practical implementation guidance for resource-constrained environments.

The framework, inspired by ISO/IEC 27005:2022 standard [26] for information security risk management, has been specifically adapted to address the unique challenges of COTS integration in autonomous maritime systems. The framework is guided by four key principles: adaptation to harsh maritime environments, recognition of resource constraints, focus on COTS-specific integration challenges, and prioritization of operational continuity during incidents. The framework follows a structured seven-step process, each building on the previous to ensure both immediate protection and long-term resilience. The cyclical nature of the framework, as illustrated in Figure 3, reflects the need for continuous security assessment and improvement, where the final step of continuous monitoring and assessment feeds back into the initial asset categorization to account for new threats, equipment changes, and lessons learned from operational experience. The steps are:

1. **Asset Categorization and Inventory**
   - Identify all onboard systems and components.
   - Assess criticality, dependencies, and vulnerabilities.
   - *Output:* Asset register with risk scores.
2. **IT/OT Integration Requirements**
   - Define secure interfaces between IT (e.g., navigation) and OT (e.g., propulsion).
   - Address differing update cycles and failure tolerances.
   - *Output:* Integration security requirements and protection specifications.
3. **Physical Security Controls**
   - Evaluate access control and environmental protection.
   - Classify equipment by access level (restricted, controlled, public).
   - *Output:* Physical security matrix and mitigation strategies.
4. **Device-Level Security Evaluation**
   - Score each COTS component across domains like encryption, authentication, and updates.
   - *Output:* Security scorecard and remediation priorities.
5. **Communication System Security**
   - Assess vulnerabilities in Very High Frequency (VHF), AIS, cellular, satellite, and Wi-Fi.
   - Recommend encryption, monitoring, and fallback procedures.
   - *Output:* Communication security plan and incident response protocols.
6. **Human-Centric Security and Operational Resilience**
   - Integrate crew training, secure workflows, and emergency procedures.
   - *Output:* Training programs, operating procedures, and incident response roles.
7. **Continuous Monitoring and Assessment**
   - Implement real-time monitoring, periodic reviews, and threat intelligence updates.

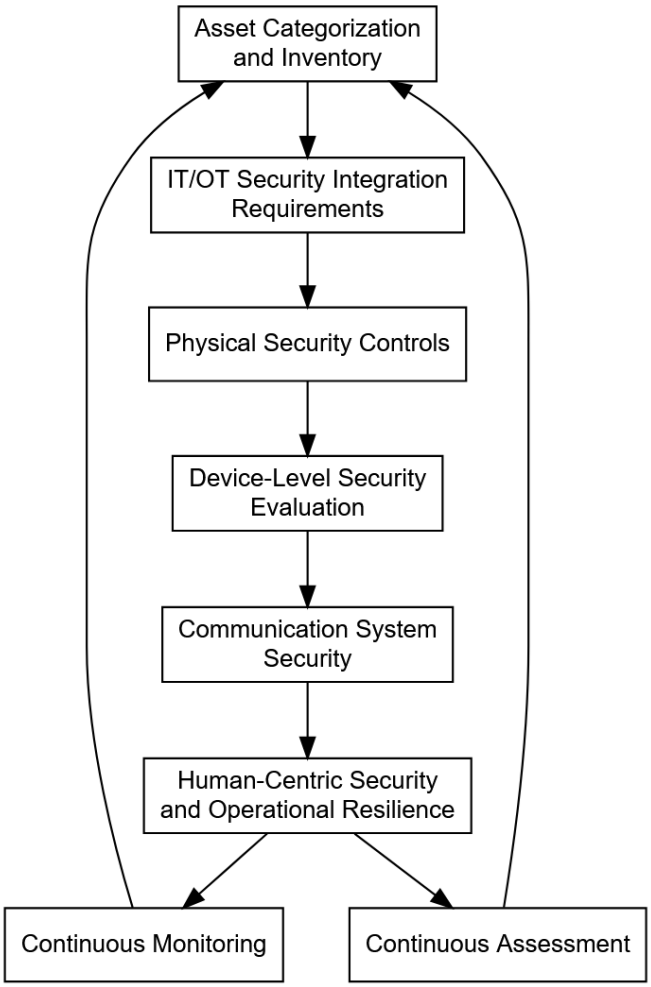


Figure 3: The structured process flow for the cyber-physical security and operational resilience framework for small maritime vessels.

- *Output:* Monitoring schedules, KPIs, and improvement plans.

The framework emphasizes that maritime security cannot be achieved through isolated technical measures but requires holistic integration of physical, cyber, and human elements tailored to the unique constraints and requirements of autonomous vessel operations.

Having established this comprehensive framework overview, the following subsections detail each evaluation step, beginning with the foundational asset categorization and inventory process that forms the basis for all subsequent security assessments.

4.2 Asset Categorization and Inventory

Assets are systematically categorized into primary groups based on their criticality and security requirements:

- Propulsion and navigation systems including vessel control mechanisms and positioning systems.
- Communication systems encompassing data transmission and network infrastructure.
- Sensor networks for environmental monitoring and operational awareness.
- Cargo and payload systems varying based on mission requirements.

- Operational data including navigation logs, mission records, and system telemetry.
- Software and intellectual property, containing control algorithms, configuration data, and proprietary systems.
- Environmental safety.

The comprehensive asset inventory process requires systematic documentation of each component including manufacturer information, version details, configuration specifics, and integration dependencies. This documentation forms the baseline for ongoing security assessment and provides essential information for vulnerability management and incident response planning.

Table 1 presents the comprehensive asset risk assessment matrix incorporating threat levels, vulnerability assessments, and impact analysis specifically adapted for maritime autonomous systems. The numeric values presented in this table serve as illustrative examples for demonstration purposes and should be adapted to each individual case.

Table 1: Asset Risk Assessment Matrix for Maritime Autonomous Systems

Asset Category	**Threat Level**	**Vulnerability**	**Impact**	**Risk Score**	**Priority**	**Key Protection Requirements**
Propulsion & Navigation	8	5	9	7.3	2	Physical isolation, access controls
Communication Systems	8	8	8	8.0	1	Encryption, authentication, monitoring
Sensor Networks	5	8	8	7.0	2	Tamper detection, data validation
Cargo & Payload	4	5	4	4.3	3	Mission-specific protection
Operational Data	8	5	8	7.0	2	Encryption, access controls, backup
Software & IP	5	8	8	7.0	2	Code signing, version control
Environmental Safety	8	3	9	6.7	2	Redundancy, fail-safe mechanisms

Risk scoring methodology incorporates quantitative assessment across multiple dimensions to ensure consistent and comprehensive evaluation. Threat Level Assessment evaluates likelihood of attack based on asset attractiveness to adversaries, accessibility for exploitation, and historical incident data from maritime cybersecurity databases, scored 1-10 with 10 representing highest threat probability. Vulnerability Assessment examines technical weaknesses including unpatched systems, configuration issues, and inherent design limitations, scored 1-10 with 10 representing most vulnerable systems requiring immediate attention. Impact Assessment quantifies potential consequences including direct financial losses, operational disruption costs, regulatory violations and penalties, and safety implications including environmental damage, scored 1-10 with 10 representing catastrophic impact.

The composite risk score calculation follows the mathematical framework:

Composite Risk Score:

$$R = \frac{T + V + I}{3} \tag{1}$$

where T, V, and I represent Threat Level, Vulnerability, and Impact assessments respectively (each scored 1-10), providing standardized risk rankings enabling consistent prioritization across diverse asset categories.

Priority Classification:

- **Priority 1:** $R \geq 8.0$ – Immediate attention requiring emergency response capabilities and rapid remediation
- **Priority 2:** $5.0 \leq R < 8.0$ – Systematic improvement within 3-6 months through planned security enhancements
- **Priority 3:** $R < 5.0$ – Routine maintenance and monitoring through standard operational procedures

Having established a comprehensive asset inventory and risk baseline, the framework next addresses the critical integration challenges between information technology and operational technology systems, which represent one of the most significant vulnerability areas in modern autonomous vessels.

4.3 IT/OT Security Integration Requirements

To ensure secure and reliable integration between information technology (IT) and operational technology (OT) systems aboard autonomous maritime vessels, it is essential to address their distinct operational priorities, update strategies, and security requirements. Table 2 presents a comprehensive overview of these integration requirements, highlighting the primary concerns, maintenance approaches, and emergency procedures associated with each system type. This structured comparison supports the development of tailored security strategies that respect the unique constraints and performance expectations of both IT and OT domains in maritime environments.

Table 2: IT/OT Security Integration Requirements

System Type	**Primary Concern**	**Update Strategy**	**Security Measures**	**Emergency Procedures**
Navigation IT	Data integrity	Scheduled maintenance	Encryption, access controls	Backup navigation systems
Communication IT	Availability	Real-time updates	VPN, monitoring	Alternative communication
Propulsion OT	Continuous operation	Planned maintenance	Physical isolation	Manual override
Safety OT	Reliability	Manufacturer schedule	Redundancy, fail-safe	Emergency shutdown
Sensor OT	Real-time response	Minimal disruption	Data validation	Sensor redundancy
Control OT	Predictable behavior	Change control	Access logging	Manual control

4.4 Physical Security Controls

Physical security assessment addresses the unique challenges of maritime environments where vessels operate in uncontrolled spaces with varying access control capabilities. Table 3 provides the comprehensive physical security assessment matrix incorporating environmental factors specific to maritime operations. The Access Level and Environmental Protection values in the table serve as illustrative examples for demonstration purposes and should be adapted to each individual case.

Table 3: Physical Security Assessment Matrix for Maritime Equipment

Equipment Category	**Access Level Required**	**Environmental Protection**	**Vulnerabilities**	**Mitigations**
Propulsion Batteries	Restricted	Sealed Hull	Electrical hazards limit access	Tamper seals, monitoring
Motor Controllers	Restricted	Enclosed	Specialized tools required	Access logging, cameras
Navigation Computers	Controlled	Cabin	Standard marine locks	Biometric locks, alarms
Network Equipment	Controlled	Enclosed	Tool access required	Tamper detection, logging
Communication Antennas	Public	Exposed	Deck mounted, accessible	Tamper detection, redundancy
External Sensors	Public	Exposed	Easy physical access	Tamper evidence, monitoring
Power Distribution	Controlled	Enclosed	Panel access required	Locking panels, monitoring
Emergency Systems	Emergency	Accessible	Emergency access required	Secure emergency procedures

Access control implementation considers maritime operational requirements including emergency response procedures, maintenance accessibility, and crew safety considerations. Restricted Access requires specialized tools and procedures with comprehensive logging and monitoring, suitable for critical systems where unauthorized access poses significant safety or security risks. Controlled Access implements standard security measures including locks, access cards, or biometric systems with routine monitoring, balancing security with operational accessibility. Public Access acknowledges operational necessity for accessibility while implementing tamper detection and evidence collection capabilities, recognizing that some systems must remain accessible for safety or operational reasons.

Environmental protection assessment addresses salt water corrosion effects on security hardware, extreme weather impact on access controls, and temperature variations affecting electronic security systems. Security hardware selection prioritizes marine-grade components with appropriate Ingress Protection (IP) ratings, corrosion resistance, and operational temperature ranges suitable for maritime environments, ensuring long-term reliability and effectiveness.

4.5 Device-Level Security Evaluation

Comprehensive security evaluation requires systematic analysis of each COTS component using evaluation criteria that address the specific integration challenges identified in maritime environments. Table 4 presents the comprehensive device security scorecard providing quantitative assessment across all critical security domains. The Max Score values and Assessment Guidelines numerical thresholds can be adjusted according to the specific operational priorities and risk tolerance of the vessel in question.

Table 4: Comprehensive Device Security Scorecard

Security Domain	Evaluation Criteria	Max Score	Assessment Guidelines	COTS Considerations
Physical Security	Enclosure, mounting, tamper detection	15	Secured (15), Partial (10), None (0)	Marine environment compatibility
Authentication	Access control, device auth, keys	15	Strong (15), Moderate (9), None (0)	Default credential management
Encryption	Data protection, key management	20	Full (20), Partial (12), None (0)	Consumer vs. enterprise grade
Configuration	Hardening, documentation	15	Complete (15), Partial (10), Default (0)	Maritime-specific settings
Updates	Mechanism, frequency, testing	15	Automated (15), Manual (10), None (0)	Manufacturer support lifecycle
Monitoring	Logging, alerting, anomaly detection	10	Comprehensive (10), Basic (6), None (0)	Integration with vessel systems
Network Security	Protocols, filtering, segmentation	10	Implemented (10), Partial (5), None (0)	Maritime protocol compatibility
Total Security Risk Level			**High (<60), Medium (60-79), Low (≥80)**	

Physical Security Assessment (15 points) evaluates enclosure integrity, mounting security, and tamper detection in maritime environments. Secured implementation (15 points) requires marine-grade enclosures with IP67+ ratings, vibration-resistant mounting, and comprehensive tamper detection. Partial implementation (10 points) includes basic weather protection and standard mounting with limited tamper evidence. No implementation (0 points) represents consumer-grade devices requiring comprehensive physical security upgrades. Marine environment compatibility demands specialized consideration of salt water corrosion, temperature variations, and UV exposure affecting standard security measures.

Authentication Assessment (15 points) has a critical role in preventing unauthorized access. Strong authentication (15 points) implements multi-factor authentication with hardware security modules, certificate-based device authentication, and robust key management with secure generation, distribution, and rotation. Moderate authentication (9 points) includes password-based access control, basic device authentication using shared secrets, and manual key management. No authentication (0 points) encompasses default credentials, no device authentication, or hardcoded mechanisms requiring immediate remediation. Default credential management challenges require systematic inventory and updates during COTS installation.

Encryption Assessment (20 points) addresses data confidentiality and integrity throughout vessel communications. Full encryption (20 points) could implement e.g. AES-256 for data at rest and in transit, hardware-based key management, and end-to-end encryption for critical communications. Partial encryption (12 points) could include e.g. AES-128 for sensitive data, software-based key management, and selective encryption. No encryption (0 points) represents plaintext transmission, unprotected storage, or deprecated algorithms requiring external encryption systems. Consumer versus enterprise-grade capabilities often determine COTS suitability for maritime applications.

Configuration Security Assessment (15 points) addresses system hardening, documentation, and maritime-specific customization. Complete configuration (15 points) requires comprehensive hardening following maritime baselines, complete documentation, and maritime-specific optimization. Partial configuration (10 points) includes basic hardening with disabled unnecessary services and limited documentation. Default configuration (0 points) encompasses manufacturer defaults without hardening, creating vulnerabilities requiring systematic remediation. Maritime requirements often differ from standard IT environments, addressing power management, environmental conditions, and specialized protocol integration.

Update Management Assessment (15 points) impacts long-term security through vulnerability remediation. Automated updates (15 points) provide secure, verified automatic updates with rollback capabilities and maritime change management integration. Manual updates (10 points) include systematic procedures, periodic vulnerability assessment, and documented testing. No updates (0 points) encompasses devices without mechanisms, discontinued support, or operationally risky procedures requiring replacement planning. Manufacturer support lifecycle evaluation must consider extended maritime operational requirements beyond typical consumer lifecycles.

Monitoring Assessment (10 points) enables incident detection and forensic analysis. Comprehensive monitoring (10 points) implements detailed security logging, real-time anomaly detection with alerting, and vessel-wide system integration. Basic monitoring (6 points) includes essential logging, periodic review procedures, and basic alerting. No monitoring (0 points) prevents effective incident response and compliance demonstration. Integration requires consideration of data aggregation, storage limitations, and crew workload without overwhelming resources.

Network Security Assessment (10 points) addresses protocol security, filtering, and segmentation. Implemented security (10 points) includes secure protocols with certificate validation, firewall capabilities, and segmentation support. Partial security (5 points) encompasses basic protocol security and simple filtering. No security (0 points) represents insecure protocols requiring external measures. Maritime protocol compatibility often determines feasibility, as specialized protocols may not support

advanced security features.

Scoring Methodology and Rationale

The maximum scores presented in Table 4 represent expert-derived heuristics based on systematic analysis of the relative criticality of each security domain in maritime COTS environments.

The scoring methodology assigns different maximum points to reflect the relative importance of each security domain in maritime operations. These values can be modified according to the specific operational priorities, risk tolerance, and security requirements of individual vessels under assessment. The different point allocations for Full/Partial/None implementation levels within each category reflect the varying complexity and security impact of implementing these controls in maritime environments. The gaps between implementation levels (e.g., Encryption: Full 20, Partial 12, None 0) represent the significant security differences between comprehensive implementations and basic or absent controls. These thresholds can be adjusted based on specific vessel requirements and operational contexts.

Risk Level Determination and Total Score Calculation

The total device security score is calculated by summing all individual category scores:

$$\text{Total Score} = \sum_{i=1}^{7} S_i \tag{2}$$

where S_i represents the score for each of the seven security domains (Physical Security, Authentication, Encryption, Configuration, Updates, Monitoring, Network Security), with a maximum possible total score of 100 points.

Risk level determination provides quantitative assessment for systematic prioritization: High Risk (Total Score < 60) indicates immediate attention required, with devices potentially unsuitable for safety-critical applications without significant additional security measures. Medium Risk (Total Score 60-79) represents acceptable security posture requiring systematic improvement planning and enhanced monitoring. Low Risk (Total Score ≥ 80) indicates robust security suitable for safety-critical applications with minimal additional security requirements.

Vessel operators should adapt the scoring thresholds and category weightings based on their specific operational requirements, regulatory compliance needs, and risk tolerance levels.

4.6 Communication System Security

Communication systems represent primary attack vectors for remote exploitation and require comprehensive security evaluation addressing the full spectrum of maritime communication technologies. Table 5 provides detailed security assessment for each communication method commonly used in autonomous vessel operations.

Table 5: Communication Security Assessment Matrix

Communication Method	**Security Features Available**	**Primary Vulnerabilities**	**Recommended Mitigations**	**Emergency Procedures**
VHF Radio	None (plain text)	Interception, spoofing	Traffic monitoring, protocols	Coast Guard channels
AIS	None (standard)	Position spoofing, Denial of Service (DoS)	Anomaly detection, backup	Emergency position beacons
Cellular/4G/5G	Carrier encryption	Network dependency	VPN, traffic analysis	Satellite backup
Satellite	Link encryption	High latency, cost	Prioritization, compression	Emergency channels
Wi-Fi	WPA2/3 available	Range, interference	Enterprise security	Secure guest networks
Bluetooth	Pairing encryption	Limited range, attacks	Device controls, monitoring	Disable during emergencies

Maritime communication protocols present unique security challenges due to historical emphasis on interoperability and reliability over security. VHF and AIS systems operate as standardized protocols without encryption or authentication by design - autonomous vessels must comply with these standards to participate in maritime traffic management and safety systems. The security approach for these systems focuses on monitoring and anomaly detection rather than protocol modification, including detection of spoofing attempts, identification of jamming attacks, and validation of received data against other sensor inputs. Recent research demonstrates the feasibility of AIS-based covert channels for command and control attacks, highlighting the need for enhanced monitoring and anomaly detection capabilities [21].

Cellular networks, while providing carrier-level encryption, introduce dependency on terrestrial infrastructure that may be unavailable in remote maritime areas, necessitating additional VPN layers and traffic analysis for enhanced security. Satellite communications offer global coverage with link-level encryption but face challenges from high latency. Wi-Fi systems, despite supporting robust WPA2/3 encryption

standards, present significant security risks due to their broadcast nature and susceptibility to interference in maritime environments, demanding enterprise-grade security configurations and careful network segmentation. Bluetooth connections, while offering convenient short-range connectivity for maintenance and configuration, introduce attack vectors through pairing vulnerabilities and limited authentication mechanisms, requiring strict device access controls and continuous monitoring protocols.

4.7 Human-Centric Security and Operational Resilience

Effective cybersecurity in transition towards autonomous maritime operations must account for the human element, particularly in environments characterized by isolation, limited crew, and high operational stress. Human factors integration addresses these realities by focusing on the roles, responsibilities, and limitations of onboard personnel in maintaining security.

Small vessel crews often operate with minimal external support and must manage multiple responsibilities, including cybersecurity tasks for which they may have limited training. In such contexts, security procedures are at risk of being overlooked—especially during high-pressure situations such as emergencies or system failures. To mitigate this, tailored training programs are essential. These should include maritime-specific cybersecurity awareness, recognition of common attack vectors (e.g., phishing, spoofing), social engineering defenses, and secure operational practices that align with existing safety protocols.

Operational security must also be embedded into routine procedures. This includes analyzing standard workflows for potential vulnerabilities, identifying maintenance activities that may temporarily weaken security postures, and ensuring that emergency protocols do not inadvertently bypass critical safeguards. Port operations, where vessels are physically accessible to unauthorized individuals, require particular attention to access control and tamper detection.

Incident response and recovery planning must reflect the unique challenges of maritime environments. These include limited communication capabilities during emergencies, constrained response resources in remote areas, and jurisdictional complexities when incidents occur in international waters. Additionally, environmental safety considerations may necessitate immediate action, even before full security assessments can be completed.

A structured incident classification system should cover scenarios such as navigation system compromise, communication disruption, propulsion interference, and physical breaches. Response protocols must prioritize safety and environmental protection while ensuring coordination with maritime authorities. Clear roles and responsibilities should be defined for both onboard and shore-based personnel, supported by reliable communication channels and decision-making hierarchies.

Finally, evidence collection procedures must be adapted to maritime conditions, ensuring forensic integrity while balancing operational demands. This includes secure data logging, chain-of-custody protocols, and coordination with law enforcement when necessary.

4.8 Continuous Monitoring and Assessment

Continuous Monitoring and Assessment could provide e.g. ongoing security evaluation through real-time monitoring capabilities including network traffic analysis for anomalous patterns, system performance monitoring to detect security-related degradation, anomaly detection algorithms adapted for maritime operational patterns, and threat intelligence integration incorporating maritime-specific threat information.

Key performance indicators for maritime cybersecurity effectiveness could include e.g. incident detection time measured from initial compromise to detection, response time to security events from detection to containment, system availability during security operations ensuring safety systems remain functional, and training completion rates ensuring crew competency in security procedures.

Periodic assessment schedules balance comprehensive security evaluation with operational requirements through daily automated monitoring with minimal crew intervention, weekly comprehensive log review by designated security personnel, monthly detailed security posture assessment including vulnerability scanning, and annual framework evaluation incorporating lessons learned and threat landscape changes.

Threat intelligence integration could address maritime-specific threat information from government sources, industry security bulletins from maritime organizations, regulatory updates affecting cybersecurity requirements, and emerging attack methodologies targeting maritime systems.

5 Conclusion

This study presents a security-by-design framework for integrating COTS equipment into small autonomous vessels. Using the eM/S Salama test platform, we demonstrate how theoretical cybersecurity challenges manifest as practical risks in real-world maritime operations.

The case study reveals critical vulnerability issues stemming from the inherent trade-offs in consumer-grade technologies prioritizing usability and cost over security. To address these issues, we propose a seven-step evaluation framework encompassing asset categorization, IT/OT integration, physical and device-level security, communication system assessment, human-centric resilience, and continuous monitoring. The framework's modular design and quantitative scoring enable tailored implementation across diverse vessel types and operational contexts. This security-by-design methodology provides robust foundations for safe autonomous maritime operations. By offering assessment tools, quantitative evaluation methodologies, and practical implementation guidance, the research enables small vessel operators to navigate autonomy transitions with confidence in their cybersecurity postures.

Future research should address the evolution of autonomous systems incorporating artificial intelligence (AI) and machine learning, requiring AI-specific security evaluation modules including adversarial robustness testing and secure model validation procedures. Integration of automated security monitoring tools represents significant opportunity for enhancing real-time threat detection while reducing crew workload. Long-term research directions should examine COTS equipment security evolution and integration with emerging maritime technologies, including advanced wireless communications, edge computing platforms, and next-generation satellite networks. Collaboration with regulatory bodies will be essential to ensure consistent cybersecurity standards for autonomous vessels.

References

[1] F. Martínez, et al., (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 23, 1429–1457. Available: `https://link.springer.com/article/10.1007/s10207-023-00800-0`

[2] R. R. Negenborn, et al., (2023). Autonomous ships are on the horizon: here's what we need to know. *Nature*. Available: `https://www.nature.com/articles/d41586-023-00557-5`

[3] U.S. Coast Guard Cyber Command, *2023 Cyber Trends and Insights in the Marine Environment (CTIME) Report*, United States Coast Guard, 2024. `https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf`

[4] G. Hatzivasilis, et al., *Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees*. Applied Sciences, vol. 10, no. 16, article 5702, 2020. Available: `https://doi.org/10.3390/app10165702`

[5] J. Kalliovaara, et al., *Deep Learning Test Platform for Maritime Applications: Development of the eM/S Salama Unmanned Surface Vessel and Its Remote Operations Center for Sensor Data Collection and Algorithm Development*, Remote Sensing, vol. 16, no. 9, p. 1545, 2024, Available: `doi:10.3390/rs16091545`

[6] M. Li, et al., "Maritime Cybersecurity: A Comprehensive Review," arXiv preprint arXiv:2409.11417v2, 2024. Available: `https://arxiv.org/html/2409.11417v2`

[7] M. Erbas, S. M. Khalil, and L. Tsiopoulos, "Systematic Literature Review of Threat Modeling and Risk Assessment in Ship Cybersecurity," *Ocean Engineering*, vol. 295, article 116785, 2024. Available: `http://dx.doi.org/10.1016/j.oceaneng.2024.118059`

[8] M. Chaal, X. Ren, A. Bahootoroody, S. Basnet, V. Bolbot, O. V. Banda, and P. van Gelder, "Research on Risk, Safety, and Reliability of Autonomous Ships: A Bibliometric Review," *Safety Science*, 2023. Available: `http://dx.doi.org/10.1016/j.ssci.2023.106256`

[9] P.H. Meland, et al., (2021). *A Retrospective Analysis of Maritime Cyber Security Incidents*. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 15(3), 519–526. Available: `https://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html`

[10] A. Raymaker, et al, (2025). *A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners*. arXiv preprint. Available: `https://arxiv.org/abs/2506.15842`

[11] O. Schinas and D. Metzger, "Cyber-Seaworthiness: A Critical Review of the Literature," *Marine Policy*, vol. 148, article 105441, 2023. Available: https://doi.org/10.1016/j.marpol.2023.105592

[12] K. Tam and K. Jones, "Cyber-Risk Assessment for Autonomous Ships," in *Proc. International Conference on Cyber Security And Protection Of Digital Services*, 2018. Available: http://dx.doi.org/10.1109/CyberSecPODS.2018.8560690

[13] G. Kavallieratos, V. Diamantopoulou, and S. Katsikas, "Shipping 4.0: Security Requirements for the Cyber-Enabled Ship," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6617–6625, 2020. Available: http://dx.doi.org/10.1109/TII.2020.2976840

[14] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A Novel Cyber-Risk Assessment Method for Ship Systems," *Safety Science*, 2020. Available: http://dx.doi.org/10.1016/j.ssci.2020.104908

[15] International Maritime Organization. "Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems," IMO, London, June 2017.

[16] P. McGillivary, "Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed," *Marine Technology Society Journal*, vol. 52, no. 5, pp. 48–57, 2018. Available: http://dx.doi.org/10.4031/MTSJ.52.5.11

[17] G. Kavallieratos and S. Katsikas, "Managing Cyber Security Risks of the Cyber-Enabled Ship," *Journal of Marine Science and Engineering*, 2020. Available: http://dx.doi.org/10.3390/jmse8100768

[18] A. Amro, G. Kavallieratos, K. Louzis, and C. Thieme, "Impact of Cyber Risk on the Safety of the MilliAmpere2 Autonomous Passenger Ship," *IOP Conference Series: Materials Science and Engineering*, 2020. Available: http://dx.doi.org/10.1088/1757-899X/929/1/012018

[19] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework," *ACM Transactions on Privacy and Security*, 2022. Available: http://dx.doi.org/10.1145/3571733

[20] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime Cyber Threats Detection Framework: Building Capabilities," in *Proc. WISE*, 2022. Available: http://dx.doi.org/10.1007/978-3-031-08172-9_8

[21] A. Amro and V. Gkioulos, "From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks," in *Proc. European Symposium on Research in Computer Security*, 2022. Available: http://dx.doi.org/10.1007/978-3-031-17143-7_26

[22] R. Zăgan, G. Raicu, and A. Sabau, "Studies and Research Regarding Vulnerabilities of Marine Autonomous Surface Systems (MASS) and Remotely Operated Vessels (ROVs) from Point of View of Cybersecurity," *International Journal of Modern Manufacturing Technologies*, 2022. Available: https://doi.org/10.54684/ijmmt.2022.14.3.310

[23] C. Grigoriadis, S. Papastergiou, P. Kotzanikolaou, C. Douligeris, A. Dionysiou, E. Athanasopoulos, K. Bernsmed, P. H. Meland, and L. Kamm, "Integrating and Validating Maritime Transport Security Services: Initial Results from the CS4EU Demonstrator," *International Conference on Contemporary Computing*, 2021. Available: http://dx.doi.org/10.1145/3474124.3474213

[24] V. Bolbot, G. Theotokatos, E. Boulougouris, L. Wennersberg, H. Nordahl, Ø. Rødseth, J. Faivre, and M. Colella, "Paving the Way Toward Autonomous Shipping Development for European Waters – The AUTOSHIP Project," 2020. Available: https://www.researchgate.net/publication/342833933_Paving_the_way_towards_autonomous_shipping_development_for_European_Waters_-_The_AUTOSHIP_project

[25] M. A. Ben Farah, E. A. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information*, vol. 13, no. 1, article 22, 2022. Available: https://doi.org/10.3390/info13010022

[26] International Organization for Standardization. (2022). *ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (4th ed.).