ISSN: 2182-2069 / E-ISSN: 2182-2077

Assessing Cyber-Physical Security Standards and Metrics for Next-Generation Autonomous Vessels

Deepa Rajesh[1*], and Ramesh Balasubramanian[2]

[1*]Department of Amet Business School, AMET University, Kanathur, Tamil Nadu, India.
deeparajesh@ametuniv.ac.in, https://orcid.org/0009-0008-9743-4791

[2]Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India. rameshchitra2002@yahoo.co.in, https://orcid.org/0009-0009-5709-2739

Received: January 27, 2025; Revised: March 11, 2025; Accepted: April 23, 2025; Published: May 30, 2025

Abstract

The integration of autonomous technologies in maritime operations increases the need for sound cyber-physical security. Autonomous systems and Artificial Intelligence heavily depend on interconnected systems and enhanced sensors, increasing the risk from cyber-attacks and physical damage. This research examines the body of available cyber-physical security frameworks concerning the Maritime Autonomous Surface Ship (MASS) systems, assesses the existing fragmented frameworks, and analyzes the effectiveness of new emerging metrics aimed Quantify resilience and risk within the context of the proposed frameworks. Using comparative analyses of the international cyber laws governing the maritime domain, IMO and associated guidelines, ISO/IEC standards, and sectoral maritime cybersecurity frameworks, we argue the stark realities of lacking coherent, cohesive, holistic, and real-time universal security frameworks. We apply case study and threat modeling approaches to a set of scenarios to analyze claimed vulnerabilities and test the proposed metrics in a maritime setting. The study expounds the need for internationally adopted unified standards which address the operational and environmental considerations of navigating autonomous systems in maritime domains. In this regard, the study concludes with a suggestion on how to approach the governance of security and resilience in the cyber-physical ecosystem of maritime systems in the future.

Keywords: Cybersecurity, Autonomous Vessels, Maritime, Cyber-Physical Systems, Security Standards, Risk Metrics, Next-Generation Shipping.

1 Introduction

1.1 Summary of Importance in the Maritime Industry and Autonomous Vessels

The Maritime Autonomous Surface Ships (MASS), most commonly referred to as autonomous vessels, are an innovative leap in maritime transportation. These vessels use artificial intelligence (AI) along with machine learning, sensors, and other communications systems to navigate and operate autonomously, with little or no human supervision. The maritime industry is progressively integrating autonomous technologies to improve efficiency, human error reliability, and operating expenditures. Autonomous vessels stand to improve safety, emissions, and resource consumption as trade routes

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 271-284.
DOI: *10.58346/JISIS.2025.I2.019*

*Corresponding author: Department of Amet Business School, AMET University, Kanathur, Tamil Nadu, India.

become heavily utilized and the demand for faster logistics increases. Moreover, they are extremely beneficial in high danger operations such as military missions, Arctic exploration, and search-and-rescue operations where humans used to be present but now the presence is dangerous or impractical (Smihunova et al., 2024). The International Maritime Organization (IMO) and the European Maritime Safety Agency (EMSA) are currently working on regulatory policies to facilitate for the safe use of autonomous technologies (IMO, 2021; Zahedi et al., 2019; EMSA, 2020)). However, the development of MASS is still at its infancy stage for their construction, with varying autonomy degrees being observed from decision support systems to full control. Significant advances have not been made due to technical, social policy, and regulation hurdles that need to be resolved (Vasquez & Sorensen, 2025). The impact that unmanned cargo ships will have on the future of shipping logistics, as the maritime industry undergoes digitization, is immensely important.

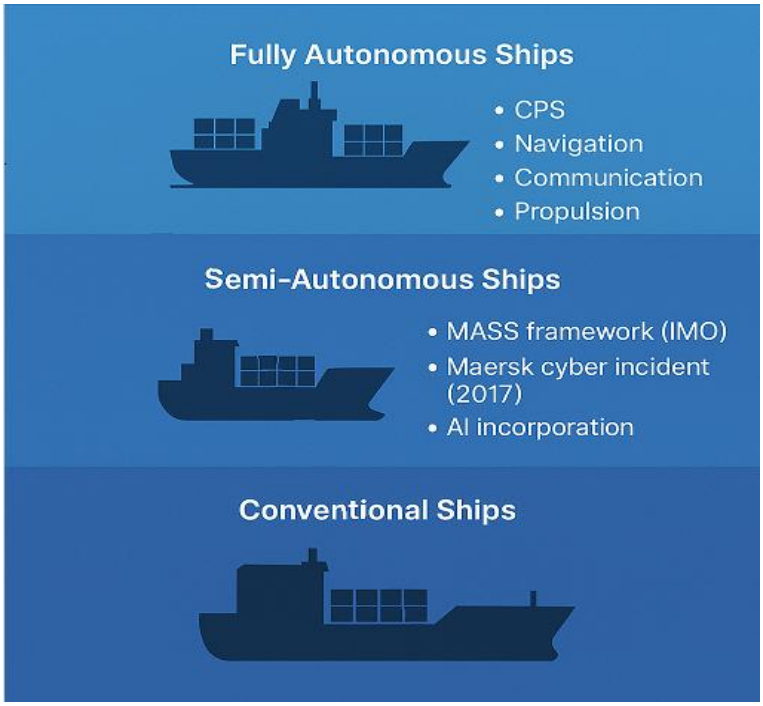

Figure 1: Evolution of Maritime Autonomy and Cyber-Physical Integration

The figure (Figure 1) depicts the stepwise progression of ships from Conventional to Semi-Autonomous and Fully Autonomous and the progression of CPS integration with each increment step. The first layer shows Conventional Ships where humans completely control all navigation, communication, and propulsion systems, with rudimentary digital assistance (Zhu et al., 2024). The middle layer marks the creation of Semi Autonomously with Ships which implement some powered automation aided by earlier CPS technologies. This step has milestones such as the IMO's international MASS framework, the 2017 Maersk cyber incident, and the first attempts to integrate Artificial Intelligence for aiding navigation and decision making (Kalita et al., 2024; Rahman & Begum, 2024). Fully Autonomous Ships reside at the top tier which is further divided in two categories with very little to no human interaction left and complete reliance on human control to sustain navigation, propulsion and communication through cyber physical systems dorsal CPS. Here, CPS take charge of all functions. This diagram emphasizes the contribution of CPS to achieving the defined degree of autonomy and demonstrates the increasing vulnerability of maritime activities to sophisticated systems of secure intelligent computing.

1.2 The Cybersecurity Threats on Autonomous Vessels and Their Expansion

The enhancement of autonomous vessels is directly linked to the employment of digital control systems, and in turn automates a large section of the operations in the vessel (Wan & Hu, 2024; Veerappan, 2024). The vessel systems on board interacts dynamically with other systems on shore by satellite communication, fuel monitoring via GPS and analysis on the cloud, a plethora of data is received in real time. So, they are vulnerable to cyber-attacks on systems for navigation, cargo control, propulsion, remote takeover of control, etc (Tam & Jones, 2019). Attacks could be mounted by threat actors on communication interfaces, software update systems, and IoT devices for the purpose of espionage or disrupting normal functioning (Jagan, 2024; El-Saadawi et al., 2024; Kumar, 2024). That type of attack can lead to devastating destruction and a multitude of issues such as loss in profit, loss of resources, exposing a nation and its motives to enemies and giving them the chance to invade on strategic passages or military installations of great import (Kessler et al., 2022; Sadulla, 2024). With the upsurge of technology, autonomous decision-making algorithms and AI powered systems are implemented, making them more hackable due to their unexplainable nature and difficulty in auditing them for security proprietary Ojaghloo & Jannesary (2015). Notably, as is also the case in many other industries, maritime has practiced very little hands-on robust cyber security measures, aiding in patchy protective measures and responding when faced with challenges (Vrhovec et al., 2022). Additionally, numerous vessels operating today use unpatched systems and obsolete software, which renders them vulnerable to contemporary threat actors (Bichou & Bell, 2020). Defensive measures for autonomous vessels should not only focus on existing IT protections, but also the real-world impacts of cyber-attacks, especially given the direct risks to life and cargo. In this regard, next-generation maritime assets will be operated more securely if integrated cyber-physical security frameworks are more widely adopted Rajan & Srinivasan (2025).

1.3 Importance of Establishing Security Standards and Metrics for Autonomous Vessels

The integration of autonomous vessels into the maritime domain requires the development of specific cybersecurity guidelines and performance metrics, standards that are lacking to date (Krishnan et al., 2024). Autonomous vessels, unlike conventional ships, do not carry a crew to manage emergencies which intensifies the need for fail safe, autonomous cybersecurity and safety measures. Current marine frameworks, such as the IMO's Resolution MSC.428(98), Cyber Risk Management frameworks, to some extent minimally address the issue cyber risk management, offering no guidance for autonomous operation scenarios (IMO, 2017). During vessels operations, cyber-physical engagement with the dynamic environment demands information security standards such as ISO/IEC 27001 and NIST Cybersecurity Framework need to be recontextualized into maritime domains. Additionaly, metrics such as Mean Time to Detect (MTTD) an attack and quantify the resilience of the vessel’s systems against attacks, restoration time of the system, and attack recovery time must be established for evaluating the precision of the secured defense frameworks (Caldwell et al., 2021). In the absence of such metrics, benchmarking inter-system security preparedness becomes impossible. The absence of coherent unified standards leads to fragmentation adding to compliance costs and complexities in cross-nation operations (Shaikh et al., 2020). Clear benchmarks are crucial for shipbuilders and operators to validate certify for unilaterally accepted. The clear standards and metrics along with facilitate an insurance evaluation, liability claim evaluation, and even permit approval. Hence, an amalgamation of international collaboration is required from marine regulators, cybersecurity analysts, classification societies, and tech developers to outline, manage, and modify the frameworks as autonomous vessels turn into a reality in shipping.

2 Current Cyber-Physical Security Standards for Autonomous Vessels

2.1 A Review of Standards Formed from ISO/IEC 27001 and NIST SP 800-82

ISO/IEC 27001 and NIST SP 800-82 form part of contemporary cyber–physical security frameworks. These documents offer base documents for guidance for the security of Information Systems and Industrial Control System (ICS) security as well as critical infrastructure systems. ISO/IEC 27001 outlines the need to set up, implement, operate, monitor, analyze, maintain, and improve an information security management system, with its ISMS framework focusing on risk assessment and mitigation (ISO/IEC, 2013). This standard has been implemented in various sectors, including maritime organizations that have adopted it for general IT security (Vaishnav et al., 2025). On the other hand, NIST SP 800-82 is custom made for ICS security offering detailed technical information on the security of PLCs, DCS, and SCADA systems (Stouffer et al., 2015). These components are increasingly embedded in autonomous vessels for propulsion, navigation, and monitoring. Although these standards have broad coverage, they were not developed initially with autonomous systems or maritime contexts in focus. Thus, they do not cater to varying marine operational conditions, remote control conditions, multi-party communication frameworks typical of MASS systems (Schmittner & Ma, 2018). Even so, it is appropriate and practical for shipbuilders and operators looking to adopt systematic structured cyber risk management because the standards offer a strong foundation (Kanchetti, 2021). Certain classification societies such as DNV and Lloyd's Register have begun adapting their cybersecurity certification models to these standards in order to make them more relevant to maritime settings (DNV, 2021).

2.2 Examining the Application of Autonomous Vessel Standards

There is contextual effort needed to apply existing cyber-physical security standards to autonomous vessels. ISO/IEC 27001 strips an organization of its information assets, policies, and governance frameworks which are pertinent to the shoreside control of an autonomous system, yet is deficient in operational integrity of real-time, systems autonomy, and submerged decision-making logic within MASS technologies (Gupta & Quamara, 2018). With equal measure, NIST SP 800-82 delineates protecitons for ICS in a manner that is complete, but does not encompass mobility, remote connection, and multi-vendor systems on autonomous vessels (Humayed et al., 2017; Ahani, 2019). These standards need to be broadened to account for maritime specific systems such as ECDIS, AIS, and integrated bridge systems (Anand, 2024). Furthermore, autonomous vessels navigate open, and often hostile terrains where satellite communication acts as the only data conduit, a consideration that the original standards did not plan or provide for (Ahmad et al., 2021). Such lines of communication are susceptible to spoofing, jamming, and interception, which accentuates the need for the expansion of existing standards to include maritime focused threat and defense mechanism models (Karimov & Bobur, 2024). Some modifications have surfaced like DNV's "Cyber Secure" class notations and BIMCO's guidelines for shipboard cybersecurity, which integrate parts of ISO and NIST standards but adapt them for maritime operations (DNV, 2021; BIMCO, 2020). In spite of these efforts, the swift development of MASS technologies needs a more dynamic, hybrid style across IT and operational technology (OT) domains to safeguard vessel autonomy and safety more fully (Veerappan, 2023).

2.3 Finding Deficiencies in Existing Standards Governing Autonomous Vessels

Even with existing foundational documents, cyber-physical security standards that attempt to address the vulnerabilities of autonomous maritime vessel vessels are still lacking (Shetty & Kapoor, 2024). One

shortfall is the focus on autonomy related concerns such as AI navigational algorithm spoofing, adversarial sensor inputs, or decision manipulation (Sharma et al. 2021). Most standards still deal with the relative security of static systems and human-controlled infrastructures, whereas autonomous vessels require unattended operation, real-time systems, and failure response standards. Moreover, remote command-and-control ownership authenticity clearly lacks standards due to possible scenarios of satellite communication delay signals and jamming (Vimal & Muthukkumarasamy 2022). The integration of autonomous vessels into port and ship traffic management systems add another layer of difficulty which is unconsidered by the ISO/IEC 27001 and NIST frameworks. In addition, there is no consensus in the area of certifying and testing cybersecurity of militarized autonomous systems under the sea for criteria based on penetration testing, twin-simulation validation, or resilience scoring (Boehmer & Eling 2021). Current technical standards, framed for functioning AI technologies, omit crucial policies regarding AI responsibility and automated processes but are needed to ensure compliance with legislation and regulation Latha & Chandran (2025). Consequently, the IMO and classification societies, as the responsible parties, are now compelled to formulate security frameworks pertinent to MASS, whether as supplements to existing ones or entirely new ones (Sengupta & Deshmukh, 2024). The gaps associated provide a unique opportunity for collaborative international standards to be developed in a manner that strikes a tactical balance between safety, operational efficiency, and innovation.

3 Proposed Cyber-Physical Security Standards and Metrics for Autonomous Vessels

3.1 Creating Guidelines for Cyber-Digital Security in Autonomous Maritime Technology

The evolution of maritime cyber automation technology requires specific cyber-physical security standards custom for autonomous vessels' attributes. Existing security paradigms, which capture some relevance to autonomous vessel security, are primarily for scarce resources networks with human operated ma rout platforms or system, thereby overlooking autonomous vessel environments. Standards addressing the autonomy continuum, including navigation, communication, propulsion, and self-aware environmental systems interfaces, require definition for minimal human supervision. Above that, these new standards should include secure over the air software update protocols, automated incident response, and self-diagnosing state awareness tools for optimal situational surveillance and grid resilience. Moreover, they should defend against spoofed sensors, dangling command controls, dynamic environmental uncertainties, sensors, and unsanctioned data commands. Such customize standards should not only provide modular features, but also achieve flexible measurability with inflexible legacy systems capturing shifting technological parameters. The craft design must underline modular flexibility, real-time corroboration, encrypting data vessels watermark transits, secured anomaly spotting borders, and encrypted communications between land controlling stations and the board vessels. In addition, such standards need to provide rigid escape boundaries from captures of loss, diminished functionality, and isolation from strikes. To ensure that the standards are both technically sound and internationally accepted, collaborative development from maritime authorities, shipbuilders, cybersecurity specialists, and classification societies will be necessary. In the end, all autonomous vessels globally will rely on such devoted standards for their safe, secure, and trustworthy operation.

3.2 Blending Risk Assessment with Threat Modeling and Security Metrics

When creating cyber-physical security metrics for autonomous vessels, sophisticated risk assessment and threat modeling needs to be incorporated. Autonomous ships are more susceptible to dynamic cyber threats because they require independent real-time data processing and action implementation. Addressing this issue necessitates the development of security metrics grounded in exhaustive threat models that mimic physical and logical attack vectors. Such models would account for GPS spoofing, AI-induced exploitation, control system DoS, and data wiping communication channels. Assessment frameworks should determine not only the likelihood of assault scenario execution but also their influence on safety, mission persistence, and environmental impact. Systems agility could also be measured using TLI, ISS, and RTO baselines. Moreover, scoring telemetry and health monitoring would enable the constant renewal of threat profiles along with automated defensive measures. Additionally, the need to quantify redundancy, backup responses, time interval for intrusion detection, and maintenance of operational capability during hostile attacks influenced these metrics. The integration of these indicators into design and operational processes allows for proactive risk management, builds trust amongst stakeholders, and aids in compliance with regulations. Furthermore, these metrics suggest standards needed to assess emerging technologies and enhancements ensuring that cyber-physical security is a focal aspect of the vessel's functionality rather than an ancillary consideration. The maritime industry can incorporate threat modeling into metric design to enhance adaptability and resiliency within frameworks for autonomous operations.

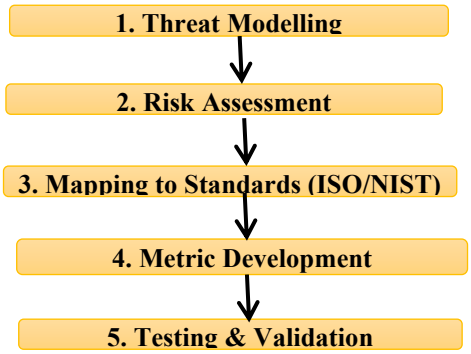

Figure 2: Cyber-Physical Security Evaluation Framework

Figure 2 depicts the approach framework for assessing and improving the cybersecurity posture of autonomous vessels. The flowchart begins with Threat Modeling, which identifies cyber-physical risks: potential threats to the vessel, whether it is mechanical, electronic, or software related. After modeling the threats comes the Risk Assessment, where the possibility and impact of these risks are gauged. Next, these results are mapped to guidelines and standards such as ISO/IEC 27001 or the NIST frameworks, ensuring compliance with industry best practices. After alignment, predetermined standards of security performance are set which are known as Metric Development. These metrics can then be used to quantitively assess an organization's security performance. Finally, through real-world simulations or digital twin environments where the vessel is virtually represented, Testing and Validation is done to check if the proposed measures will be trustworthy and effective. Following this process allows for tailored autonomous maritime systems that have robust and practical cybersecurity measures.

3.3 Taking into Account International Standards and Policies Applicable to Autonomous Vessels

For autonomous vessels to comply and be operational on a global scale, their cyber-physical security standards and metrics must conform to international laws. The maritime industry is global;

heterogeneous security requirements can increase operational friction, raise costs, and expose systems to inconsistent risk levels. For these reasons, all recommended standards should be instruments of cooperation and systems integration, bolstowing the IMO's framework on autonomous surface vessels, SOLAS, and the ISPS Code. Integration of these regional standards will ensure autonomous vessels' certification and operation will be feasible in various regions without extensive retrofitting or compliance restructuring. Additionally, compliance with regional standards will improve collaboration between regulators, shipbuilders, technology vendors, and classification societies. Appendices must consider jurisdictional over regulatory protective measures, including data protection legislation, cyber incident reporting, and liability law. With the gradual adoption of technology in different regions, a tiered and/or modular approach to standards permitting vessels to achieve minimum baseline security and advance with more sophisticated requirements where necessary may be helpful. Moreover, collective international efforts can foster the establishment of common certification and audit procedures which minimize overlapping work while guaranteeing uniform application. After all, the integration of universal norms and control mechanisms is crucial for the development of a balanced international security architecture designed to enable the safe and dependable operational deployment of autonomous ships on a global scale.

4 Case Studies and Examples

4.1 Analysis of the Latest Cyber-Attacks Directed Toward Autonomous Vessels

An increasing number of cyber-attacks have been recorded against maritime systems, including cyber-attacks against autonomous and semi-autonomous vessels in the last few years. One notable case includes the hacking of an autonomous steering system through GPS spoofing, where the vessel was misled into sailing on a default course without human intervention. Similarly, an Integrated Bridge System of a container ship was hacked, resulting in the navigation charts being altered and in the absence of manual overrides, had the potential to exhibit collision course information. These kinds of cyber-attacks illustrate the greater challenges posed to systems that make critical decisions based on sensor data within a network. Also of greater concern are cyber-attacks that sever satellite communications or remote-control links, effectively disconnecting the ship from shore control. With the rise of autonomous vessels operating without crews, such incidents pose severe risks not only to the vessels and cargo, but also to marine life and coastal infrastructure. These examples underscore that malign actors are actively striving to exploit vulnerabilities in sophisticated technologies used in shipping industries, alongside attesting that security measures currently in place are inadequate for unilateral operations.

4.2 Assessment of How Defense Protocols Would Have Altered the Outcomes of Attacks

A number of autonomous vessel cyber incidents could have been evaded or at least less damaging had cyber-physical security standards been adopted. For instance, the irony of GPS spoofing attack could have been easier detection with redundancy like positioning systems, anomaly detection and integration algorithms within the vessel navigation suite. Access to systems onboard could be regulated through multilayered authentication systems. This would prevent unsanctioned control of ship-bridge control tampering. Moreover, protocols regarding messages exchanged between the ship and control centers also have a bearing on sat elit communication linkk hijacking and, as such, need to be fortified. Such standards focused on a given premise would slow down or soften the soft spots in burst style vessel systems that would under normal circumstances free an exploit. Security policies that demand regular vulnerability assessments and penetration testing are known to delay exploitation. If a standard required

real time check of the vessel components for attacks indeed some of the mentioned actions might resort to placing the system within detach from the unparalleled man manner. A few supported examples outline a tremendous shift that needs to be done from remedial to more advanced security that focus on prevention – So, actions done before the attack. The structure in itself of such a measure would heavily decrease risks of autonomous vessels neglecting operational stand stilles, enduring response scenarios where conflict fits and non conflict frameworks endure so called while within duress.

4.3 Fostering Dialogue on The Risks of Failure to Continuously Adapt Security Improvement and Monitoring Protocols

Updating security protocols regularly, including onshore maritime property pertaining to diagnosing cyber threats, is a must in the field of maritime autonomy. We acknowledge that cyber risks are enduring, and today's innovations are likely to be tomorrow's vulnerabilities. The intricate cyber risks industries face today rendering the remote control, sensor amalgamation, and AI utilized in autonomous vessels susceptible to cyber risks. Continuous monitoring means tracking real-time system metrics, behavior, performance, and communications to determine whether anomalies indicative of cyber intrusions exist. Monitoring helps detect breaches at their earlier stages and mitigates their impact. Moreover, autonomous systems must enable reliable vulnerability exploitation without manual labor via control-free software over-the-air system updates. Autonomous systems devoid of regular updated protocols are bound to open loopholes to known exploits and loss of faith is inevitable. Having security informed feedback mechanisms will make the ecosystem more proactive against attacks. Civil security revalidation audits coupled with new threat intel fuel modern cyber frameworks. In a maritime context, continuous monitoring and updating is not just a best practice but the norm—an industry requirement.

5 Implementation Challenges and Recommendations

5.1 Finding Issues in Applying Security Protocols to Autonomous Boats

The implementation of cyber-physical security measures for autonomous vessels systems faces challenges associated with technology, regulation, and maritime operations. One of the main difficulties autonomous ships face is the lack of standardized maritime autonomous shipping protocols on a national and international level. There is a divergent approach between countries and organizations working within the same industry which creates divergence in protocols followed. Furthermore, factors such as AI, machine learning technology, and IoT devices pose threats in areas older maritime systems were not designed to tackle. The conservative maritime industry tends to be slow in technological investment, particularly those requiring heavy capital outlay, opposed to integrating new revolutionary tools. Many operators range of skills which enables them to thoroughly analyze the implementation and maintenance of dynamic cybersecurity frameworks. Perhaps the most significant hurdle is styling ill defined uniform frameworks for assessing environments and certifying vessels for compliant cybersecurity infrastructure. Use of multiple vendor components creates interoperability gaps and divides security responsibility resulting in shattered defense architectures. The fragmented security leads to vessels being constructed without regard to tailored bespoke deformation. Retrofitting vessels with newer cybersecurity frameworks poses a challenge both in aspect of technical pragmatism and fiscal responsibility. These issues underscore the necessity of a unified, staged approach that balances different degrees of technological advancement while still moving the sector towards a safe autonomous future.

5.2 The Challenges and Suggested Solutions

Combining stringent security standards for autonomous vessels with existing technologies poses numerous challenges that are better addressed with a comprehensive approach. For starters, the creation of adaptable, modular standards that are easier to implement and more affordable across various types of vessels and technologies would go a long way. The regulation implementation cooperation among the industry, classification societies, and other stakeholders needs to provide clear instructions alongside certification frameworks and roadmaps detailing cyber security specifications needed for new builds and retrofitted vessels. Shipbuilders and operators should be able to pre-evaluate the security measure deployment effectiveness through simulation environments or digital twins, which could further assist in cybersecurity measure evaluation. Providing financial assistance with tax incentives or grants for cybersecurity enhancement could increase adoption industry wide. Moreover, maritime personnel deployed onboard or onshore need to be trained in cyber awareness and response skills to ensure that any potential responses to a cyber threat are adequately addressed. The establishment of centralized threat intelligence dissemination hubs would enable stakeholders to adjust their defenses against emerging attack vectors and new vulnerabilities. Standards have to be kept in check with technology changes and new threats in order to ensure relevancy, therefore there is a need for developers, regulators, and end users to have continuous feedback sessions. In addressing these gaps, focusing on education, providing practicality, and regulatory transparency would allow the industry to gradually overcome the barriers set in place and enhance the cyber resilience in autonomous vessels. The graph (Figure 3) depicts the distribution of the key problems that stakeholders encounter while trying to apply cybersecurity standards to autonomous vessels. The greatest concern, impacting 68% of stakeholders, is the absence of specific autonomous maritime system frameworks. This points to the fact that there is an absence of authoritative unified guidelines across industries. The next problem of concern, high implementation costs, is critical to 60% of stakeholders – primarily the smaller operators who usually have limited budgets. Another important problem is the scant availability of Maritime Cybersecurity experts in the industry, impacting 55% of respondents. Also, retrofitting existing vessels to incorporate advanced cybersecurity infrastructure poses challenges for 48% of stakeholders, while issues relating to interoperability among multi-vendor systems constrict 45% of stakeholders. All these statistics in unison, strengthen the case for modular scalable solutions, support driven phenomena, and increased support from the industries.

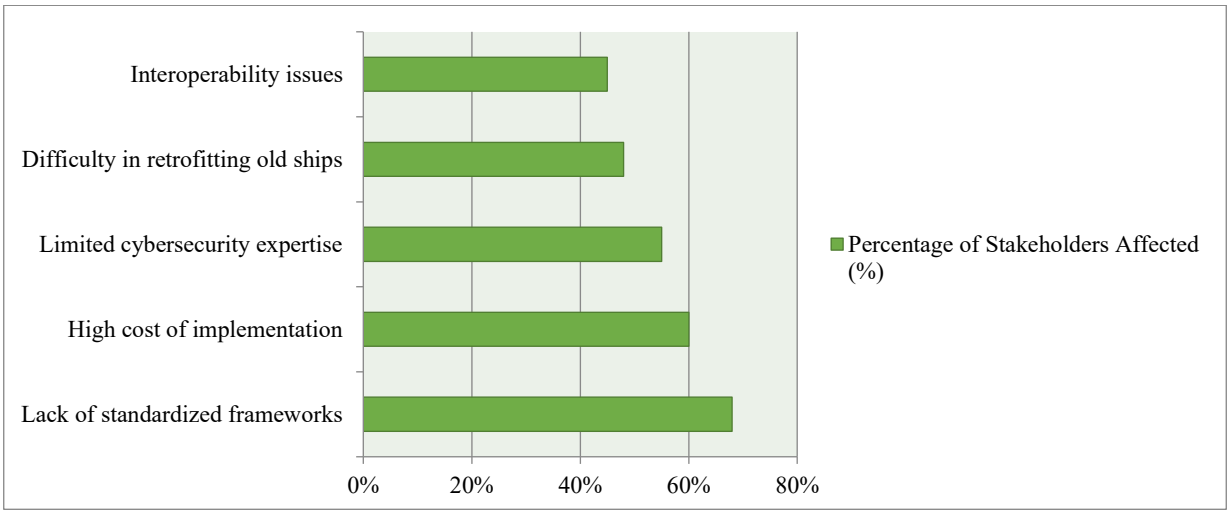

Figure 3: Key Challenges in Implementing Security Standards for Autonomous Vessels

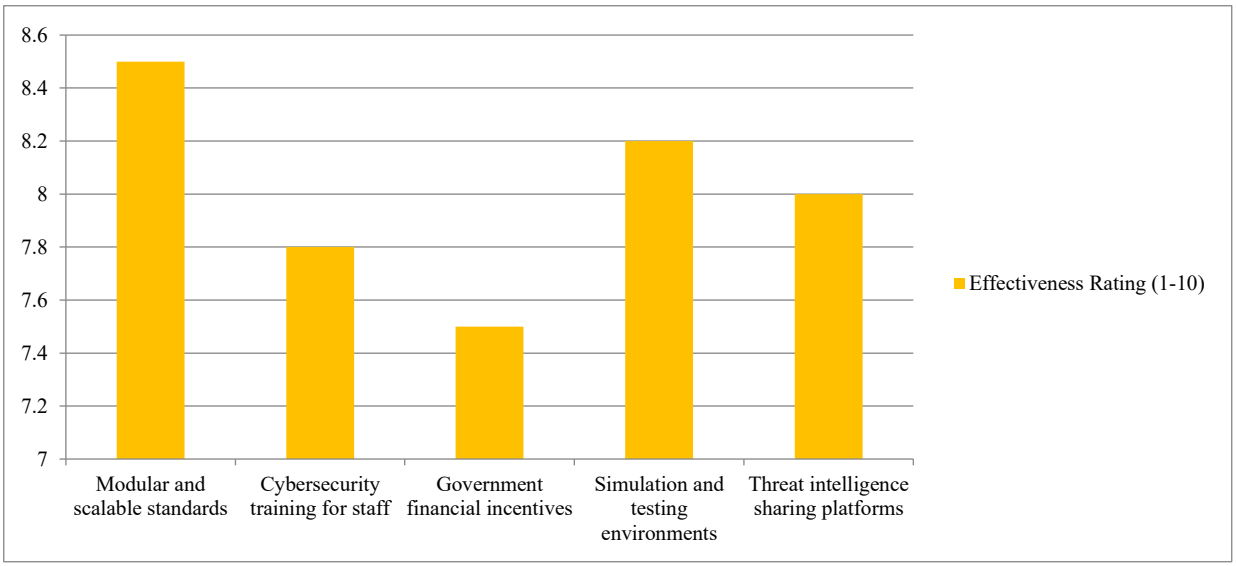

Figure 4: Effectiveness of Recommendations to Overcome Implementation Barriers

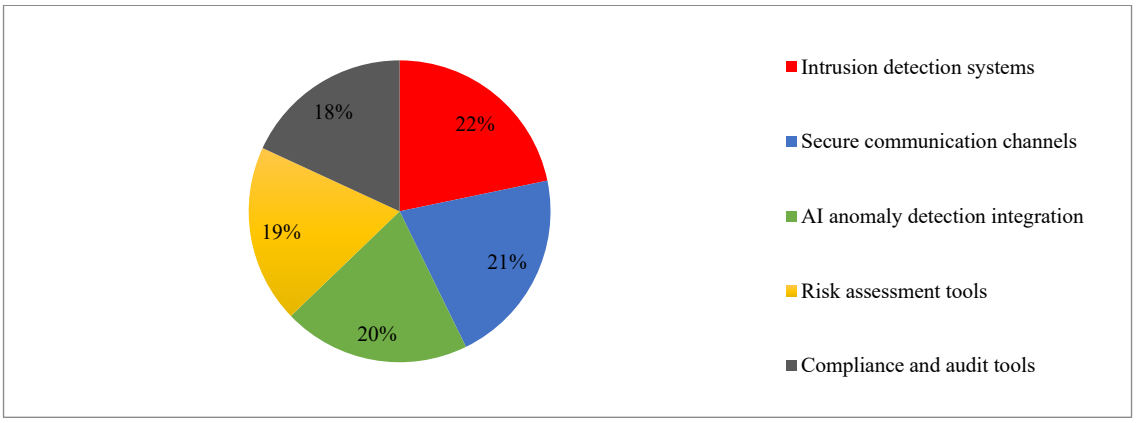

Figure 5: Cybersecurity Investment Priorities for Autonomous Vessels

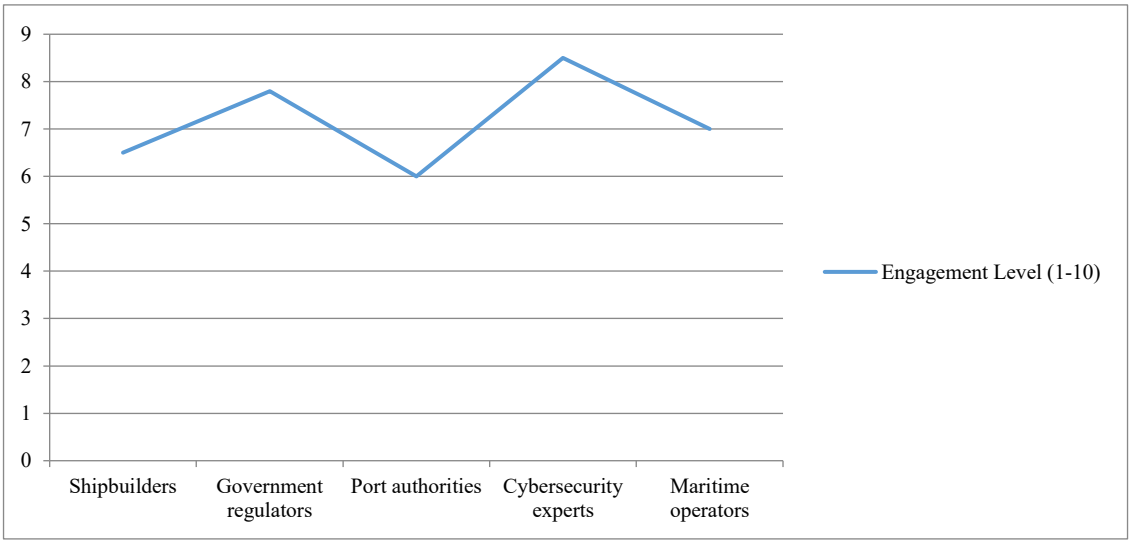

Figure 6: Level of Stakeholder Engagement in Cybersecurity Collaboration

The figure 4 graph analyzes the effectiveness of various strategic recommendations in overcoming implementation barriers. “Modular and scalable standards” was rated the highest at 8.5 out of 10, showing strong support for frameworks that flexibly accommodate different types of vessels and levels of technology maturity. Creating simulation and testing environments also scored high (8.2), demonstrating support for testing frameworks in realistic deployment scenarios before full-scale operational integration. Cybersecurity training for operational staff (7.8) and intelligence sharing platforms (8.0) highlight the need for effective cross-disciplinary herd mobilization control measures relevant to the rest of the sector. The rating of 7.5 given to government financial incentives shows supporting but less enthusiasm toward funding that is perceived as difficult to access, indicating a need for simpler and more transparent funding pathways. From the analysis, it can be concluded that these respondents are more likely to support multi-faceted strategies that combine techniques, finance, and education. The graph (Figure 5) shows the priority investment for autonomous vessels in the area of cybersecurity. The foremost area of concern is intrusion detection, which is allocated a priority score of 9.0, meaning these systems are crucial for detecting, responding to, and neutralizing threats. Secure communication channels (8.7), which focus on encryption, also reinforce the need to protect interactions between vessels and control centers. AI-enabled anomaly detection (8.3) indicates high concern as well, meaning there is heightened focus placed on autonomous and predictive threat neutralization systems. Risk assessment tools (7.9) and compliance mechanisms (7.5) are also prioritized but to a lesser extent, signifying their supporting role in helping achieve necessary regulatory benchmarks. This graph underlines an investment approach that seeks to integrate detection, secure infrastructure, and compliance with regulations while remaining forward-thinking. The graphical representation (Figure 6) illustrates the degree to which various stakeholders are involved in cooperative cybersecurity activities. Cybersecurity professionals have the highest engagement level at 8.5, which shows their involvement in dealing with maritime threats is strong. Government regulators score 7.8 which indicates they play some active role in policy and standardization activities. Maritime operators (7.0) and shipbuilders (6.5) are at moderately engaged levels, probably because of differences in available skills and resources. Port authorities show least engagement at 6.0 which may be because of low interaction with vessel-specific systems or uncertainty in regulation.

All these outcomes suggest that more efforts need to be made in the design and execution of maritime cybersecurity plans to foster multi-sector collaboration at all stakeholder levels.

5.3 Importance of Collaborating with Stakeholders within the Cybersecurity Domain

A vessel’s autonomous operation poses additional cybersecurity challenges which strike at the very fundamental structure of a vessel's operation. There is no boat builder, ship operator, or ship regulator who can independently resolve the entire cyber-physical intricacies. While the government has the jurisdiction to define international laws, treaties, legislation, and policies, it is the responsibility of industry players to provide insights relevant to vessel operation, while cybersecurity professionals delve deeply into tackling cutting-edge threats. Cybersecurity specialists, government and industry practitioners, and other domain professionals will find it convenient to collaborate towards developing a well-aligned approach to the solution which meets established standards, professionally empowered to explore the associated risks. Combining efforts helps institutions protected by law to provide intelligence, practices, and incidents outside their control, leading to improved defensive measures. It also advances the actual balance of technology and security, operational barriers, and advancement pace controlling room windows wide open. Working with other parties from different sectors allows the establishment of a legal cooperative framework were response to proactive policies deal with unforeseen dangers. Besides, where such collaboration exists, advancing pathways to compliance, certification

guidance, and training packages for general industry use is expedited. A collaborative approach guarantees that autonomous vessels are innovative as well as safe, secure, and acceptable to operators, regulators, and the general public."

6 Conclusion

The maritime sector is on the cusp of transformation due to the profound possibilities associated with advancements in technology of autonomous vessels operating without human intervention. Thus, these innovations also pose new sophisticated cyber-physical threats challenges that require immediate action. This paper focused on the equally concerning problem of constructing appropriate dedicated security norms specific to the autonomous vessels control. Such existing standards like ISO/IEC 27001 and NIST SP 800-82 are indeed a good starting point. However, they do not cover the complete spectrum of issues associated with the inclusion of artificial intelligence, remote control, and autonomous navigation, which increases the vulnerability to numerous sophisticated attacks. As demonstrated in the case studies presented, many of these incidents could have been avoided through the proactive implementation of appropriate security strategies. Dynamic risk assessment, continuous system monitoring, and redundancy within systems are critical components for guaranteeing safe and resilient operations. In addition, the lack of cybersecurity expertise in maritime operations, high costs of implementations, and fragmented regulations all highlight the need for collaborative efforts. The recommendations provided focus on flexible standardization, education for stakeholders, and strong international cooperation. With the ongoing developments in autonomous shipping, future studies must address adaptive threat modeling, AI-powered anomaly detection, and real-time autonomous response strategies. Formulation of holistic and universally recognized cyber-physical security frameworks will protect technological innovations and guarantee the sustained safety, efficiency, and reliability of maritime operations conducted autonomously.

References

[1] Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2021). Security in Maritime Cyber–Physical Systems: Current status and challenges. *Journal of Cyber Security Technology, 5(*1), 1–29.

[2] Anand, M. D. (2024). Design and Development of Advanced Mechanical Systems. Association *Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(1), 1-6.

[3] Banda, O., van Eeden, G., & Rian, L. (2021). Autonomous Ships: Trends, Challenges, and Future Perspectives. *Journal of Marine Science and Engineering, 9*(7), 748.

[4] Bichou, K., & Bell, M. (2020). Maritime Cybersecurity: The Threat Landscape and the Case for Holistic Approaches. *Safety Science, 129,* 104835.

[5] BIMCO. (2020). Guidelines on Cyber Security Onboard Ships (Version 4.0). *Baltic and International Maritime Council.* https://www.bimco.org

[6] Boehmer, J., & Eling, M. (2021). Insuring Cyber Risk in Autonomous Systems. *The Geneva Papers on Risk and Insurance - Issues and Practice, 46*(2), 235–260.

[7] Caldwell, B., Wuest, T., & Romero, D. (2021). Metrics for Cyber-Physical Resilience in Autonomous Systems. *Procedia CIRP, 104,* 1378-1383.

[8] DNV. (2021). Cyber secure class notation. Det Norske Veritas. https://www.dnv.com

[9] El-Saadawi, E., Abohamama, A. S., & Alrahmawy, M. F. (2024). IoT-based optimal energy management in smart homes using harmony search optimization technique. *International Journal of Communication and Computer Technologies, 12*(1), 1-20.

[10] EMSA. (2020). Study on the Safe Use of Autonomous and Remotely Operated Vessels in the Maritime Sector. *European Maritime Safety Agency.*

[11] Gupta, B., & Quamara, M. (2018). Smart ship cyber security: A critical review. *Journal of Information Security and Applications, 40,* 80–90.
[12] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber–physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172
[13] IMO. (2021). Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS). *International Maritime Organization.*
[14] ISO/IEC. (2013). ISO/IEC 27001: Information Security Management Systems. International Organization for Standardization.
[15] Jagan, B. O. L. (2024). Low-power design techniques for VLSI in IoT applications: Challenges and solutions. *Journal of Integrated VLSI, Embedded and Computing Technologies, 1*(1), 1-5.
[16] Karimov, Z., & Bobur, R. (2024). Development of a Food Safety Monitoring System Using IOT Sensors and Data Analytics. *Clinical Journal for Medicine, Health and Pharmacy, 2*(1), 19-29.
[17] Kessler, D., Zhao, H., & King, R. (2022). *Cybersecurity Threats in Autonomous Maritime Systems. Maritime Technology and Research, 4*(1), 35-48.
[18] Krishnan, V. G., Krishnan, T. N., Karim, S. S., Yuvarajan, G., & Priya, M. R. (2020). Cyber Security in Data Mining to Data Driven Security. *International Journal of Advances in Engineering and Emerging Technology*, *11*(1), 71-76.
[19] Kumar, T. S. (2024). Low-power design techniques for Internet of Things (IoT) devices: Current trends and future directions. *Prog. Electron. Commun. Eng.*, *1*(1), 19-25.
[20] Latha, R. S., & Chandran, M. (2025). Role of Artificial Intelligence-Enabled Marketing Strategies on Purchase Decisions. *Indian Journal of Information Sources and Services, 15*(1), 260–266. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.33
[21] Ojaghloo, M., & Jannesary, A. (2015). Investigate all attacks on Mobile Wireless Networks and Finding security solutions. *International Academic Journal of Innovative Research, 2*(2), 17–27.
[22] Rahman, S., & Begum, A. (2024). Analysis of Structural Integrity in High-Rise Buildings Under Dynamic Load Conditions Using AI: A Computational Perspective. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(2), 6-9.
[23] Rajan, A., & Srinivasan, K. (2025). *Automated Incident Response Systems for Cybersecurity.* In Essentials in Cyber Defence (pp. 1-15). Periodic Series in Multidisciplinary Studies.
[24] Sadulla, S. (2024). Techniques and applications for adaptive resource management in reconfigurable computing. *SCCTS Transactions on Reconfigurable Computing, 1*(1), 6-10.
[25] Schmittner, C., & Ma, Z. (2018). Limitations of current IT security risk assessment frameworks for ICS. *In Critical Information Infrastructures Security.* 45–56. Springer.
[26] Sengupta, R., & Deshmukh, P. (2024). Multi-Stage Filtration Systems for Continuous Separation in Fine Chemical Production. *Engineering Perspectives in Filtration and Separation, 2*(1), 13-16.
[27] Shaikh, S., Chen, Y., & Xie, L. (2020). Standardization Challenges in Maritime Autonomous Surface Ships. *Ocean Engineering, 217,* 107911.
[28] Sharma, S., Ali, A., & Bhatti, M. I. (2021). Adversarial Threats and AI in Autonomous Ships: A cyber risk assessment. *Maritime Cybersecurity Review, 3*(1), 14–29.
[29] Shetty, V., & Kapoor, B. (2024). The Role of Participatory Governance in Strengthening Community Health Systems. *International Journal of SDG's Prospects and Breakthroughs, 2*(3), 10-12.
[30] Smihunova, O., Bohdaniuk, I., Polyakova, Y., & Yehiozarian, A. (2024). Innovative Approaches to Controlling in Agribusiness: The Role of Quality Management Systems in Sustainable Production Practices. *Archives for Technical Sciences, 2*(31), 116–130. https://doi.org/10.70102/afts.2024.1631.116
[31] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16. https://doi.org/10.6028/NIST.SP.800-82r2

[32] Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In *2018 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE.
[33] Vaishnav, V. A. D., Dewangan, H., & Verma, M. (2025). Investigating the hidden ecosystems vibrant underneath hydrothermal vents and deepest oceanic trenches. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 45–53. https://doi.org/10.70102/IJARES/V5I1/5-1-06
[34] Vasquez, A., & Sorensen, I. (2025). The Effects of Education on Social Mobility: A Study of Intergenerational Mobility. *Progression Journal of Human Demography and Anthropology, 2*(1), 21-26.
[35] Veerappan, S. (2023). The Role of Digital Ecosystems in Digital Transformation: A Study of How Firms Collaborate and Compete. *Global Perspectives in Management, 1*(1), 78-89.
[36] Veerappan, S. (2024). Digital Management and Sustainable Competitiveness: Using Eco-innovation and Green Absorptive Capacity in Travel and Hospitality Enterprises. *Global Perspectives in Management, 2*(3), 32-43.
[37] Vimal, S., & Muthukkumarasamy, V. (2022). Secure satellite communications for autonomous maritime navigation systems. *Ad Hoc Networks, 130,* 102757.
[38] Wan, Q., & Hu, X. (2024). Legal Framework for Security of Organ Transplant Information in the Digital Age with Biotechnology. *Natural and Engineering Sciences, 9*(2), 73-93. https://doi.org/10.28978/nesciences.1569190
[39] Zahedi, M. R., Ramezan, M., & Hajighasemi, R. (2019). Prioritizing the components of intellectual capital intechnology-based organizations using the FGAHP method. *International Academic Journal of Organizational Behavior anHuman Resource Management*, *6*(1), 1-23. https://doi.org/10.9756/IAJOBHRM/V6I1/1910001
[40] Zhu, Z., Jiao, T., & LiInnovative, Z. (2024). Applications of IoT in Smart Home Systems: Enhancing Environmental Monitoring with Integrated Sensor Technologies and MQTT Protocol. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(4), 69-89. https://doi.org/10.58346/JOWUA.2024.I4.006

Authors Biography

Dr. Deepa Rajesh stands as a beacon of excellence in academia, administration, research, and philanthropy. With an impressive portfolio of qualifications, including M.Com, MBA, M.Phil, and Ph.D., she epitomizes intellectual prowess and leadership. Her unparalleled contributions continue to inspire and redefine maritime education on a global scale, reflecting her relentless pursuit of excellence and commitment to shaping future generations. A prolific researcher and thought leader, Dr. Deepa Rajesh has an illustrious record of publications in prestigious Scopus, UGC-CARE, and high-impact factor journals. Her thought-provoking research papers have graced numerous national and international conferences, further solidifying her standing in the academic community. Her two published books stand as a testament to her dedication to knowledge dissemination. Moreover, her successful completion of funded research projects underscores her ability to secure grants and contribute significantly to scholarly advancements. Serving as an editorial board member for reputed journals, she continues to shape the academic discourse with her insightful perspectives.

Capt. Ramesh Balasubramanian is a Master Mariner with 25 years of extensive sea-going experience in the deck department, having served on various dry fleet vessels. He holds academic qualifications from NIPM and HIMT and currently serves as an Associate Professor at AMET University. With a strong commitment to maritime education, he brings practical industry knowledge into the classroom, effectively preparing future marine professionals through structured training and real-world insights.