Safety Driven Hardware and Control Architecture for Automated Surface Vessel Systems

Önder Hamamcıoğlu
Department of Engineering & IT
Carinthia University of Applied Sciences
Villach 9500, Austria
Oender.Hamamcioglu@edu.fh-kaernten.ac.at

Semih Bajrami
Department of Engineering & IT
Carinthia University of Applied Sciences
Villach 9500, Austria
Semih.Bajrami@edu.fh-kaernten.ac.at

Viktor Komyshan
Department of Engineering & IT
Carinthia University of Applied Sciences
Villach 9500, Austria
Viktor.Komyshan@edu.fh-kaernten.ac.at

Gehan Dasanayake
Department of Engineering & IT
Carinthia University of Applied Sciences
Villach 9500, Austria
Gehan.Dasanayake@edu.fh-kaernten.ac.at

Mathias Brandstötter
ADMiRE Research Center
Carinthia University of Applied Sciences
Villach 9500, Austria
M.Brandstoetter@cuas.at

Abstract

Maritime Autonomous Surface Ships (MASS) challenge safety frameworks originally developed for conventionally crewed vessels. Although autonomous navigation algorithms have advanced significantly, a critical gap remains in the hardware and control architectures required to deploy them safely in real maritime environments. This paper examines the legal and operational constraints affecting MASS under current international maritime frameworks and reviews the associated challenges of multi-sensor perception and remote human–machine interaction. To address these issues, the study applies System-Theoretic Process Analysis (STPA) to identify unsafe control actions and derive safety constraints at the organizational and supervisory control levels. Based on these results, the paper proposes a safety-driven hardware and control architecture for automated surface vessel systems. The architecture is intended to function as an assurance layer around AI-enabled autonomy by combining hardware redundancy, real-time diagnostic monitoring, independent safety controllers, and mechanisms for safe supervisory intervention. In doing so, it provides the structural basis for fault-tolerant operation, controlled degradation, and transition to a minimum-risk condition under abnormal or degraded conditions.

1 Introduction

Maritime Autonomous Surface Ships (MASS) and other automated watercraft systems are emerging as key technological drivers in the transformation of the maritime domain. According to the International Maritime Organization (IMO), a MASS is "a ship which, to a varying degree, can operate independent of human interaction" [12]. This evolution is driven by rapid advances in sensing, computation, and communication, enabling safety-critical functions to be implemented within system architectures that

The Third Austrian Symposium on AI, Robotics, and Vision (AIROV26).

operate with minimal human supervision. At the same time, it fundamentally challenges established safety, security, and regulatory assumptions developed for conventionally crewed ships.

Ensuring the safety of widely deployed automated watercraft is both critical and complex, as it involves not only the technology itself but also the people who use it and the surrounding environment. From a technological perspective, organizations such as DNV [4] require autonomous and remotely operated vessels to demonstrate a level of safety equivalent to or higher than that of traditional ships. This requires systems to be robust, fault-tolerant, and thoroughly assessed for risks in both their physical components and software. Such a system-level perspective aligns with functional safety standards such as IEC 61508 [7], which establishes strict requirements for the reliability and development of safety-critical electronic systems. Despite significant progress in autonomous navigation algorithms and situational awareness software, a critical gap remains in the physical realization of these systems. Current research predominantly focuses on high-level software logic, often overlooking the underlying hardware architecture and control mechanisms required to execute these functions reliably in a harsh maritime environment. Standard industrial computing platforms may not provide the fault tolerance, determinism, or diagnostic coverage required by safety standards such as IEC 61508 or DNV class guidelines. In emergency situations, a hardware failure can be catastrophic if the system architecture lacks inherent redundancy and hardware-based safety mechanisms. Without a dedicated safety-driven hardware architecture, the theoretical capabilities of autonomous software cannot be safely deployed in real-world scenarios.

To address this challenge, this paper proposes a safety-driven hardware and control architecture specifically designed for automated surface vessel systems. The proposed architecture integrates hardware redundancy, real-time diagnostic monitoring, and independent safety controllers to ensure that the vessel can maintain a safe state even in the event of a component failure. Although the present contribution is architectural, it directly targets the assurance problem posed by AI-enabled maritime autonomy. In MASS, perception, fusion, and planning increasingly rely on learned or data-driven components whose behavior may degrade under adverse weather, sensor corruption, distribution shift, or adversarial interference. The proposed safety-driven architecture therefore serves as an assurance layer around AI-based autonomy by monitoring system health, constraining control authority, and enforcing transitions to minimum-risk operation when AI outputs cannot be trusted.

2 Legal Framework

This section evaluates the legal status of MASS under SOLAS, UNCLOS, and COLREGs. It first identifies provisions that presuppose onboard human presence or immediate human control, then contrasts strict textual and functional interpretations of those provisions, and finally distinguishes the regulatory position of remotely operated vessels from that of fully autonomous vessels.

The legal framework is examined through the International Convention for the Safety of Life at Sea (SOLAS), the United Nations Convention on the Law of the Sea (UNCLOS), and the Convention on the International Regulations for Preventing Collisions at Sea (COLREGs). The International Maritime Organization (IMO) defines the degrees of autonomy as follows [11]:

- Ship with automated processes and decision support
- Remotely controlled ship with seafarers on board
- Remotely controlled ship without seafarers on board
- Fully autonomous ship

The following paragraphs examine how legal instruments apply to autonomous vessels and highlight the regulatory challenges that arise as the degree of autonomy increases.

International Convention for the Safety of Life at Sea (SOLAS): The SOLAS Convention was adopted in 1974. It specifies the minimum acceptable standards for ship construction, equipment, operations, and certification. [10]

One of the main issues in SOLAS for fully automated vessels is found in Chapter V, Regulation 13, which addresses ship manning. This regulation states that the Contracting Governments are responsible for ensuring that each ship flying their flag is sufficiently and efficiently manned. Chapter V, Regulation 19, which addresses the use of automatic pilot systems, states that it must be possible

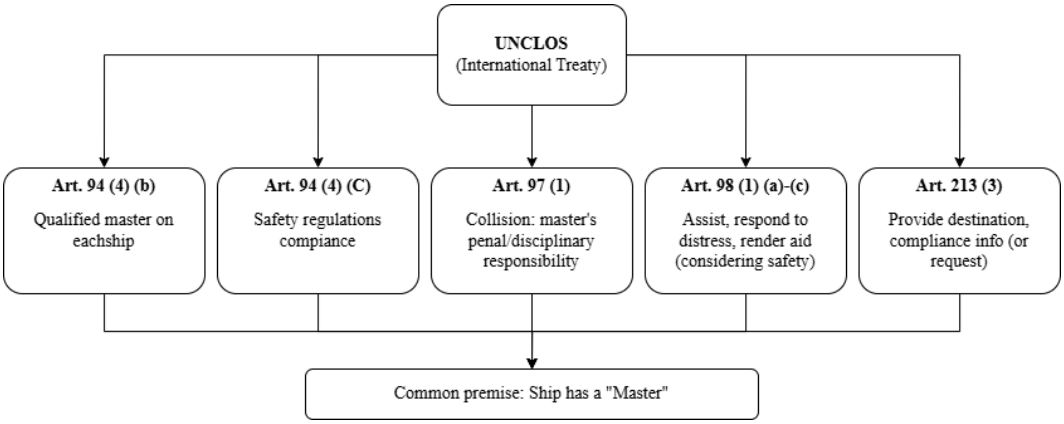

Figure 1: Applicability of UNCLOS Provisions to Unmanned MASS

to establish immediate human control of the ship's steering in high-density traffic and in all other hazardous navigational situations in which the automatic pilot is used.

United Nations Convention on the Law of the Sea (UNCLOS): Figure 1 illustrates a critical gap between UNCLOS and the operation of fully autonomous vessels. The referenced articles are all founded on the core premise that a vessel is commanded by a human "Master". This creates a significant regulatory void and suggests that autonomous vessels are not clearly governed by the existing provisions of UNCLOS [22]. However, this view is debated. For example, McKenzie [17] argues that the terms used in UNCLOS, should be interpreted broadly enough to cover uncrewed maritime vehicles (UMVs). Furthermore, Van Hooydonk [23] notes that the convention's requirement that a vessel be commanded by a "Master" does not strictly require his physical presence on board. He concludes that, through a functional interpretation of the law, a shore-based operator can legally fulfill these obligations, thereby integrating unmanned vessels into the existing maritime system.

Convention on the International Regulations for Preventing Collisions at Sea (COLREGs): COLREGs were designed in October 1972 to update and replace the collision regulations of the SOLAS Convention, which were adopted in June 1960. [6, 9]

The first rule of the COLREGs specifies to which vessels the rules apply. It is applied to all vessels upon the high seas and all waters connected to the high seas and navigable by seagoing vessels. Under Rule 3 "General Definitions" paragraph (a), "every description of water craft, including non-displacement craft and seaplanes, used or capable of being used as a means of transportation on water," this definition does not exclude the autonomous ship from being characterized as a "vessel".

The second rule covers the responsibility of the master, owner, and crew to comply with the rules. According to Komianos [14], this rule must be adjusted to reflect the master's absence on the autonomous ship.

Rule 7, paragraph (c) warns that "assumptions shall not be made on the basis of scanty information, especially scanty radar information." The "scanty radar information" highlights the importance of the audio and visual information to a human presence on board.

Summary: This paper adopts a cautious functional interpretation. In our view, existing treaty language may accommodate remotely operated MASS where a shore-based operator can perform the practical role of master, but fully autonomous vessels remain subject to substantial legal uncertainty under current international law. The key conclusion drawn from the SOLAS, UNCLOS, and COLREG conventions is that current international maritime law is fundamentally structured around the physical presence of humans. However, the extent to which this creates a barrier is a matter of debate. While a strict interpretation of the text suggests that mandatory requirements for the presence of a master on board, crew qualifications, and manual control mechanisms make the existing framework incompatible with MASS operations, legal experts favor a functional interpretation. According to this view, shore-based operators could legally fulfill the role of "master" potentially permitting the

use of remotely operated vessels without revising the conventions. However, significant regulatory gray areas remain, particularly for fully autonomous vessels. Resolving this contradiction – whether through progressive legal interpretation or formal amendments – is essential before unmanned vessels can be used safely and legally worldwide.

3 Hardware Architecture and Sensor Integration for Safety-Critical Perception

Despite advances in autonomous navigation algorithms, a significant gap remains in the physical implementation of these systems. By describing the environmental restrictions and operational needs of maritime sensors, this chapter aims to fill this gap.

3.1 Operational Sensor Requirements and Regulatory Constraints

As discussed earlier, current regulations present significant challenges for autonomous operations. Regulators seek to address these issues by invoking the SOLAS provisions on "Exemptions" and "Equivalents", thereby permitting automated systems to replace human crew only when they can demonstrate an equivalent level of safety. However, the application of these provisions is only the first step. The next challenge lies in ensuring that these systems and their associated sensors can operate reliably under operational and environmental constraints such as:

- **Safety Constraints:** Usage of active sensor technologies has potential safety risks to human operators. For example, long-range LiDARs can scan distances of several kilometers by frequently producing laser beams that can exceed eye-safety limits [21].
- **Cybersecurity Restrictions:** Access to sensor data is usually restricted by safety protocols. Traditional maritime cybersecurity practices isolate ship systems from external networks, and private manufacturer interfaces often limit data transfer, restricting the integration of data into autonomous perception systems [21]. Additionally, deep learning-based perception systems relying on cameras, LiDARs, and RADARs are potential targets for adversarial attacks, where injected errors can disrupt navigation safety [5].
- **Weather Conditions:** Optical systems such as LiDARs and cameras are heavily impacted by meteorological conditions. While LiDARs suffer from noise scattering in rain, snow and fog, cameras are limited by ambient lighting and visibility [5].
- **Structural Limitations:** The physical placement of sensors on a vessel can cause field-of-view (FOV) restrictions. For example, a single 360-degree LiDAR is often restricted by the ship's structure, creating blind spots hat necessitate the use of multiple units [21].

3.2 Standardization and Certification Frameworks

The development of MASS Code by IMO is still in progress and it is not expected to be completed and mandated until 2032. Therefore, currently there is no globally accepted international standard or mandatory code for these autonomous systems [3]. Consequently, the industry currently lacks any specific standards for established maritime technologies except existing general ISO/IEC standards regarding safety (e.g. IEC 60825-1, the international safety standard for laser products which includes LiDARs [8])

To address this regulatory gap, the maritime sector has adopted a "Goal-Based Standard" (GBS) approach [3]. Unlike prescriptive rules that mandate technical specifications based on best practices, GBS defines the safety objectives and functional requirements that a system must meet. This approach allows various technologies (e.g., different sensor arrays or AI models) to be used as long as they can prove the safety outcome is achieved [3]. Currently, some classification societies -such as UK Maritime and Coastguard Agency, China Classification Society, RINA and DNV- have issued GBS-based rules for certifying autonomous vessels. These rules focus on the maturity of technology and the specific "Concept of Operation" instead of equipment lists.

3.3 Multi-Sensor Fusion for Situational Awareness

In the context of surface vessels, establishing a comprehensive understanding of the environment is critical. Reliance on a single sensor type is insufficient since no single sensor technology is able to deliver adequate information across all conditions [1, 21]. Multi-sensor perception systems are required to ensure availability and integrity simultaneously. This means that targets undetectable by one sensor should be detected by another. Furthermore, sensor fusion allows observations to be cross-validated. This way the "best-perceived truth" of the environment can be mapped [1].

To process this diverse data, the hardware architecture typically forms in one of these two main fusion strategies:

1. **Centralized Fusion:** This approach collects raw data (e.g. LiDAR point clouds and camera pixels) into a central processing unit before detection takes place. This allows Deep Learning models to extract rich features from the combined data, resulting in an accurate picture of the environment [21].
2. **Decentralized Fusion:** In this architecture, individual sensors process their own data to generate object tracks (e.g. a RADAR track or an AIS vector). These independent tracks are then merged and used for extracting the position and velocity of targets, often involving techniques like distributed Kalman filtering to associate tracks from different sources. [21]

The final output of this fusion process is a comprehensive, real-time map of the environment [21]. This map integrates static obstacles and dynamic objects into a unified base, which serves as the critical input for the path planning algorithms to generate safe and collision-free trajectories.

3.4 Human-Machine Interface (HMI) and Remote Supervision

The operational architecture of MASS necessitates a fundamental shift from the traditional onboard bridge HMI to a Shore Control Centre (SCC) interface. The role of the navigator transforms from active controlling to supervising, meaning the automated systems handle monitoring, controlling and collision avoidance [1]. The SCC acts as a remote command post that continuously monitors the vessel, when it is released by the crew, allowing operators to take control if unexpected situations occur [13].

A critical requirement for the remote interface is the support of a high level of situational awareness, particularly the ability to anticipate threats without overwhelming the operator. Achieving this is challenging, as the SCC relies on advanced visualization technologies such as augmented and virtual reality [1]. Consequently, remote operators face the risk of “cognitive barriers” when processing the high amount of information generated by sensors, leading to bottlenecks [13]. This situation is very similar to the bandwidth challenges for satellite and cellular links caused by continuously transmitted high-resolution sensor data. To prevent cognitive overload, the HMI should adopt a user-centred design philosophy that organizes information around the operator’s tasks rather than the underlying sensor technology, presenting only task-relevant information to support accurate decision-making [20]. In this respect, it functions analogously to sensor fusion by integrating and filtering multiple inputs into a coherent operational picture.

Sensor fusion is performed onboard to process and classify raw data locally. This significantly reduces the size of data transmitted to the SCC while ensuring the operator still receives the related information for safe supervision [1, 20].

4 System-Theoretic Control Design for Safety (STPA-Based)

4.1 Transition to System-Theoretic Safety Control

Recent studies on autonomous surface vessels indicate that conventional safety analysis techniques, such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA), are insufficient for capturing the full range of hazards in complex autonomous systems. These methods rely on sequential accident models that assume safety failures originate solely from component faults. [18]

In contrast, the system-theoretic perspective emphasizes that accidents frequently result from incorrect control actions or unsafe commands, even in the absence of component failures [16]. For instance,

a technically functional optical sensor may misclassify the horizon under glare, triggering unsafe maneuvers [2].

This study employs System-Theoretic Process Analysis (STPA) to embed safety constraints directly into the control hierarchy, proactively managing such emergent hazards [16]. The analysis begins by defining unacceptable system-level losses and the hazardous states that may lead to them, providing the basis for subsequent safety constraint development.

4.2 Losses and Hazards Definition

In the context of Maritime Autonomous Surface Ships (MASS), unacceptable system-level losses (L) and the corresponding hazardous system states (H) are defined as follows [16, 19].

Unacceptable Losses (L):

- **L-1 (Major Accident):** Total vessel loss, collision, grounding, capsizing, loss of life, or severe marine pollution.
- **L-2 (Minor Accident):** Marine incidents that do not interrupt vessel operation but degrade safety margins.
- **L-3 (Schedule Delay):** Failure to meet designated operational timelines (e.g., berth or pilot boarding schedules).
- **L-4 (Financial Loss):** Economic losses arising from accidents, delays, or operational inefficiencies.

Hazardous System States (H):

- **H-1–H-4:** Degradation or loss of critical operational capabilities, including remote control, propulsion, sensing, or communication.
- **H-5:** Vessel Not Under Command (NUC), resulting in loss of effective navigational control.
- **H-6–H-7:** Loss of effective supervisory control due to Remote Operator (RO) misunderstanding or cybersecurity compromise.
- **H-8–H-10:** Hazardous system states arising during adverse weather, complex traffic or crew interactions, and cargo-related operational constraints.

To examine how the identified hazardous states may arise from control interactions, the hierarchical control structure (HCS) is constructed following STPA guidelines.

4.3 Hierarchical Control Structure (HCS)

The HCS models the relationship between control actions and feedback among key entities to assess safety. In STPA, controllers issue control actions to a controlled process and receive feedback on system behavior. In this study, lower-level automated functions and physical vessel processes are abstracted into the controlled process to maintain an appropriate level of analysis. This abstraction is consistent with STPA guidance on managing system complexity during control structure modeling [16].

Organizational and Regulatory Layer: The Flag State establishes operational regulations and approves compliance standards for both the MASS and Remote Operation Center (ROC), receiving compliance evidence through operational monitoring. Port and Coastal States oversee scheduling, transit, and berthing regulations for the MASS, continuously monitoring its operational status to ensure adherence within their maritime domains [19].

Human Supervisory Control Layer: The RO, operating from the ROC, monitors MASS operations and performs manual intervention when necessary during degraded or abnormal operating conditions. To support effective supervisory control, the RO maintains a process model of the vessel based on operational status feedback received from the MASS [16, 19].

Based on the constructed hierarchical control structure, control actions are systematically analyzed to identify potentially unsafe control actions (UCAs) and derive corresponding safety constraints (SCs).

Table 1: UCAs and Derived SCs

Layer	UCA	Safety Constraint	SC
Organizational and Regulatory	Failure to impose operational restrictions under degraded conditions	Impose operational restrictions when degraded conditions are identified.	SC-ORG-1
	Authorization beyond defined safety limits	Do not authorize operation beyond defined safety limits.	SC-ORG-2
	Delayed issuance of safety directives	Issue regulatory directives without delay under degraded conditions.	SC-ORG-3
	Premature lifting or prolonged enforcement of restrictions	Lift restrictions only after safe operation is verified.	SC-ORG-4
Human Supervisory Control (RO/ROC)	RO fails to intervene during degraded or abnormal operation	Initiate supervisory intervention when degraded conditions exceed safety limits.	SC-RO-1
	RO issues inappropriate supervisory commands	Ensure supervisory commands remain consistent with safe vessel operation.	SC-RO-2
	RO intervenes too late to mitigate hazards	Issue supervisory intervention in a timely manner based on operational feedback.	SC-RO-3
	RO terminates supervisory control prematurely	Do not terminate supervisory control until safe operation is restored.	SC-RO-4

4.4 Unsafe Control Actions (UCAs) and Derived Safety Constraints (SCs)

In STPA, UCAs are control actions that, under specific contextual conditions, may lead to hazardous system states when they are not provided, provided inappropriately, provided too early or too late, or applied for an inappropriate duration [16]. Recent STPA-based analyses of MASS emphasize that identifying UCAs is only an initial step, and that safety assurance requires controller-specific safety constraints to proactively prevent their activation [19]. In this study, UCAs are identified for the organizational and human supervisory control layers defined in Section 4.3. Consistent with the scope of this work, the analysis focuses on safety-critical supervisory and organizational control actions influencing vessel operation under degraded or abnormal operating conditions, as summarized in Table 1.

The derived safety constraints provide the basis for translating control-level safety requirements into architectural design decisions. The contribution of this work lies in directly mapping STPA-derived constraints into enforceable hardware architecture requirements, as elaborated in the following section.

4.5 Safety-Driven Hardware Architecture Implications

The STPA-based analysis not only identifies unsafe control actions and hazardous system states, but also reveals the architectural capabilities required to prevent these conditions from emerging during operation. In this sense, the analysis serves not merely as a diagnostic tool, but as a design driver for the development of a safety-oriented MASS architecture. Consistent with the STPA safety-guided design process, safety must therefore be embedded in the system architecture from the earliest design stages, rather than introduced later as an additional corrective layer. This requires the deliberate integration of architectural features that can eliminate, constrain, detect, or mitigate unsafe control actions before they propagate into system-level hazards [15].

For MASS, these implications are particularly important because safety cannot be guaranteed solely through nominal autonomy functions. The architecture must also support fault tolerance, controlled degradation, reliable supervisory intervention, and safe transitions between operational modes under abnormal conditions. Accordingly, the safety constraints derived from the STPA analysis must be translated into explicit architectural requirements and supported by concrete hardware and control

mechanisms. Table 2 summarizes this translation by illustrating how selected safety constraints map onto corresponding architectural requirements and representative hardware support mechanisms, with particular emphasis on those constraints that require direct architectural or hardware-level enforcement.

Table 2: Mapping STPA-Derived Safety Constraints to Architectural and Hardware Implementations

SC	Architectural Requirement	Hardware Support Implication	Example Implementation
SC-RO-1 / SC-RO-3 Timely Intervention and Response	Deterministic, low-latency feedback and command pathways independent of autonomy execution.	Independent safety-critical control and communication channels supporting timely supervisory intervention.	Redundant CAN/Ethernet buses, RTOS scheduling, watchdog-triggered failover.
SC-RO-2 Conflict Prevention	Mutual exclusion of control authority between autonomous control and RO actions.	Hardware-supported authority arbitration or interlocking mechanisms to prevent simultaneous conflicting commands.	Hardware arbitration unit, safety PLC, master/slave control token switching.
SC-RO-4 Safe Termination	Verification of a safe operational state prior to releasing supervisory control authority.	Hardware-supported state validation and mode management to ensure safe transition between control modes.	Safety controller state machine, interlock signals, propulsion idle verification.
SC-ORG-1 / SC-ORG-3 Operational Restrictions	Mechanisms to enforce operational constraints and restrictions under degraded conditions.	System-level enforcement mechanisms supporting restriction activation and validation.	Geofencing logic, degraded-mode flags, speed/actuation limiters, sensor health monitoring.

5 Conclusion

This paper presents guidance for Automated Surface Vessel Systems designed to close the gap between high-level autonomous logic and the physical reliability required in maritime environments. By integrating hardware redundancy, real-time diagnostic monitoring, and independent safety controllers, the proposed system enables a stable transition to a Minimum Risk Condition (MRC) during internal failures or external hazards. Although existing legal frameworks rely on a human "master," our analysis suggests that functional equivalence and goal-based regulatory approaches may support safety-preserving deployment pathways. Furthermore, the study demonstrates that it is possible to map safety constraints, such as command pathways independent of autonomy execution and hardware-supported authority arbitration, directly into the hardware design through the application of System-Theoretic Process Analysis (STPA). Ultimately, this architecture provides the determinism and fault tolerance required to satisfy global safety requirements, thereby enabling the safe deployment of autonomous software in real-world conditions.

References

[1] Anas S Alamoush and Aykut I Ölçer. Maritime autonomous surface ships: architecture for autonomous navigation systems. *Journal of Marine Science and Engineering*, 13(1):122.

[2] Xiang Chen, Yuanchang Liu, and Kamalasudhan Achuthan. WODIS: Water obstacle detection network based on image segmentation for autonomous surface vehicles in maritime environments. *IEEE Transactions on Instrumentation and Measurement*, 70:1–13, 2021.

[3] Pietro Corsi, Sergej Jakovlev, Massimo Figari, and Vasilij Djackov. Analysis and definition of certification requirements for maritime autonomous surface ship operation. *Journal of Marine Science and Engineering*, 13(4):751, 2025.

[4] DNV. Autonomous and remotely operated ships, 2025. Official DNV webpage, accessed 2026-03-13.

[5] Yvan Eustache, Cédric Seguin, Antoine Pecout, Alexandre Foucher, Johann Laurent, and Dominique Heller. Marine object detection using lidar on an unmanned surface vehicle. *IEEE Access*, 2025.

[6] Chris Holder, Vikram Khurana, Joanna Hook, Gregory Bacon, and Rachel Day. Robotics and law: Key legal and regulatory implications of the robotics age (part ii of ii). *Computer Law & Security Review*, 32(4):557–576, 2016. (Discusses legal and regulatory challenges related to robotics).

[7] International Electrotechnical Commission. IEC 61508-1:2010 functional safety of electrical/electronic/programmable electronic safety-related systems – part 1: General requirements, 2010. IEC standard entry, accessed 2026-03-13.

[8] International Electrotechnical Commission. IEC 60825-1:2014 safety of laser products – part 1: Equipment classification and requirements, 2014. IEC standard entry, accessed 2026-03-13.

[9] International Maritime Organization. *Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs)*. IMO, London, 1972. Consolidated Edition 2003.

[10] International Maritime Organization. International convention for the safety of life at sea (solas). International Convention for the Safety of Life at Sea, 1974. International Maritime Organization (IMO), London.

[11] International Maritime Organization. Imo takes first steps to address autonomous ships. Briefing, 25 May 2018, May 2018. International Maritime Organization (IMO).

[12] International Maritime Organization. Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (mass). MSC.1/Circ.1638, June 2021. International Maritime Organization (IMO).

[13] Mingyu Kim, Tae-Hwan Joung, Byongug Jeong, and Han-Seon Park. Autonomous shipping and its impact on regulations, technologies, and industries. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 4(2):17–25, 2020.

[14] Aristotelis Komianos. The autonomous shipping era. operational, regulatory, and quality challenges. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(2):335–348, 2018.

[15] Nancy G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, Cambridge, MA, USA, 2011.

[16] Nancy G. Leveson and John P. Thomas. *STPA Handbook*. Massachusetts Institute of Technology, Cambridge, MA, 2018.

[17] Simon McKenzie. When is a ship a ship? Use by state armed forces of uncrewed maritime vehicles and the united nations convention on the law of the sea. *Melbourne Journal of International Law*, 21(2):373–402, 2020.

[18] Ministry of Science and ICT and Telecommunication Technology Association. *Risk Analysis Guide Using STPA*. Telecommunication Technology Association, Seoul, South Korea, 2018. Pages 2–14.

[19] Hyeri Park and Jeongmin Kim. STPA analysis for safe operation of maritime autonomous surface ship under degradation state. *Frontiers in Marine Science*, 12:1601515, 2025.

[20] Robert Rylander and Yemao Man. Autonomous safety on vessels. *Lighthouse Swedish Maritime Competence Centre*, 2016.

[21] Sarang Thombre, Z. Zhao, H. Ramm-Larsen, et al. Sensors and ai techniques for situational awareness in autonomous ships: A review. *IEEE Transactions on Intelligent Transportation Systems*, 23(1):64–83, 2022. (Discusses GNSS vulnerabilities and sensor failures).

[22] United Nations. *United Nations Convention on the Law of the Sea*. United Nations, New York, 1982. Signed at Montego Bay, Jamaica, on 10 December 1982. Entered into force on 16 November 1994.

[23] Eric Van Hooydonk. The law of unmanned merchant fleets – an exploration. *The Journal of International Maritime Law*, 20(6):403–423, 2014.