frontiers | Frontiers in Marine Science

TYPE Original Research
PUBLISHED 25 July 2025
DOI 10.3389/fmars.2025.1601515

OPEN ACCESS

EDITED BY
Spyros Hirdaris,
American Bureau of Shipping, United States

REVIEWED BY
Xinjian Wang,
Dalian Maritime University, China
Thomas Porathe,
Norwegian University of Science and Technology, Norway

*CORRESPONDENCE
Jeongmin Kim
jmkim@seaman.or.kr

RECEIVED 28 March 2025
ACCEPTED 24 June 2025
PUBLISHED 25 July 2025

CITATION
Park H and Kim J (2025) STPA analysis for safe operation of maritime autonomous surface ship under degradation state. *Front. Mar. Sci.* 12:1601515. doi: 10.3389/fmars.2025.1601515

STPA analysis for safe operation of maritime autonomous surface ship under degradation state

Hyeri Park[1] and Jeongmin Kim[2]*

[1]Maritime Industry and Safety Research Division, Shipping Logistics and Maritime Affairs Research Department, Korea Maritime Institute, Busan, Republic of Korea, [2]Ocean Technology Training Team, Korea Institute of Maritime and Fisheries Technology, Busan, Republic of Korea

As Maritime Autonomous Surface Ships (MASS) move toward commercialization, ensuring operational safety under degraded states has emerged as a critical challenge. This study conducts a risk analysis to identify hidden hazards that may occur when MASS operate in degraded states—conditions where the ship stays within the operational environment (OE) but outside its operational design domain (ODD). The analysis applies the System-Theoretic Process Analysis (STPA) methodology, focusing on the interactions among MASS, Remote Operations Centers (ROC), and Remote Operators (ROs) as defined in the MASS code being enacted by the International Maritime Organization (IMO). STPA modeling reveals that loss of situational awareness, information asymmetry, delayed commands, and failures in inter-system coordination are primary risk factors during degraded conditions. Based on the analysis, the study identifies control actions and safety constraints to address these hazards and proposes practical safety guidelines. These findings contribute to the development of risk-based operational modes and standards to support the safe navigation of MASS, even in degraded states.

KEYWORDS

STPA, MASS, degradation state, ship operation, remote operation, remote operator

1 Introduction

The global maritime industry has entered the core of the Fourth Industrial Revolution with the emergence of Maritime Autonomous Surface Ships (MASS). Comprehensive efforts are being made by governments, regulatory bodies, and private stakeholders across the world to ensure their successful deployment and operation at sea (Wróbel et al., 2017). These efforts include the development of enabling technologies, legal frameworks, and international policies for autonomous navigation (Porathe et al., 2014). Traditionally, ship operations have relied on the physical presence of officers on the bridge, maintaining a 24-hour watchkeeping system. Navigational safety has been ensured through human capabilities, employing all available means for lookout and decision-making. However, a new paradigm, Remote Operation, has emerged, in which computer vision, lidar, and extra

sensors enable ships to be controlled either partially or entirely from locations outside the vessel. This approach represents a fundamental shift from conventional manned navigation (Katija et al., 2021).

The International Maritime Organization (IMO) is actively developing the MASS Code to keep pace with this technological evolution. The MASS Code aims to establish global standards for the safe design, construction, and operation of MASS. It is expected to be adopted as a non-mandatory code in 2026 and later incorporated into the International Convention for the Safety of Life at Sea (SOLAS) as a mandatory code by 2032, following an Experience Building Phase (EBP) (International Maritime Organization (IMO), 2024). Central to the MASS Code are two key operational boundaries: the Operational Envelope (OE) and the Operational Design Domain (ODD) (International Maritime Organization (IMO), 2024). The OE encompasses the external and internal conditions under which a MASS can operate safely. These include the vessel's intended functions, geographic area of operation, environmental parameters, mode-switching capabilities, and the division of responsibilities between automated systems and human operators. On the other hand, the ODD defines the functional limits of individual components or subsystems, based on risk assessments conducted during the design and testing phases (International Maritime Organization (IMO), 2025). Although redundancy is a fundamental design concept employed to minimize operational disruptions, it may not fully mitigate cascading failures caused by shared vulnerabilities across redundant systems. Such events may lead to the vessel operating outside its ODD while still remaining within the OE—a condition classified as a degraded state (International Maritime Organization (IMO), 2025).

The MASS Code recognizes that even autonomous ships must maintain human interaction at various stages of their lifecycle (Ringbom, 2019). Full autonomy does not eliminate the need for accountability—particularly in situations involving unpredictable hazards or ethical decision-making (Wróbel et al., 2017). Accordingly, the Code defines clear roles for human involvement, including the designation of onboard crew, remote operators, and a master (Ringbom, 2019; International Maritime Organization (IMO), 2021). Each role carries specific responsibilities, and a command hierarchy is maintained to ensure legal and operational clarity. In particular, a Remote Operator (RO) is defined as a qualified individual who performs control and monitoring tasks from a Remote Operation Centre (ROC). This role requires certified maritime training and professional experience (Porathe et al., 2014). The MASS Code also stipulates that when onboard personnel are present, they have operational priority over remote operators (Porathe et al., 2014). Furthermore, a designated master must always retain ultimate responsibility for the vessel, regardless of its mode of operation (Wróbel et al., 2017; Ringbom, 2019).

To support the implementation of these regulatory principles, Belgium has developed a national framework titled *Concepts on the Management of Remote Operations* and submitted it through the 108th MSC Committee. This proposal offers a legal and organizational basis for overseeing ROC-based ship operations (Internantional Maritime Organization (IMO), 2024). It introduces the concept of Remote Operation Management (ROM)—a new legal entity responsible for supervising ROC functions and ensuring compliance (Internantional Maritime Organization (IMO), 2024). Under this model, the MASS and ROC are treated as a unified system subject to joint certification by relevant flag States. The framework also ensures that ROC authorization remains valid regardless of geographic location, supporting transnational operations and multi-flag fleet management (Internantional Maritime Organization (IMO), 2024). In addition, the model addresses critical issues such as cross-company responsibilities, software updates, and cybersecurity risks (Internantional Maritime Organization (IMO), 2024). By formalizing the interaction between the ROC, ship systems, and flag States, the framework enhances legal accountability and operational efficiency in autonomous shipping.

As MASS operations expand beyond experimental deployments into real-world maritime environments, it becomes increasingly important to establish mechanisms that ensure continued safety under non-ideal conditions. One such condition is the degraded state, in which the vessel experiences a reduction in system functionality due to partial failures or unforeseen events. Although the ship may remain operational within the OE, the risk of accidents and system instability becomes significantly elevated (International Maritime Organization (IMO), 2025). Despite its critical relevance, current literature provides limited insight into practical response strategies or analytical methods tailored to such states (Wróbel et al., 2017).

This study seeks to address this gap by applying a safety-oriented analytical approach to the degraded state of MASS. The methodology adopted is System-Theoretic Process Analysis (STPA), which provides a structured framework for identifying unsafe control actions and system vulnerabilities. STPA moves beyond traditional component-failure models by focusing on system behavior, control structures, and human–system interactions (Leveson and Thomas, 2018). This makes it particularly suitable for assessing the safety of complex autonomous systems such as MASS. The present research aims to identify key hazard scenarios that may arise under degraded conditions and to analyze how remote operators and masters can intervene to maintain safe operations. The findings are expected to contribute to the development of operational guidelines for MASS under degraded conditions and to inform future revisions of the MASS Code and related international regulations.

2 Literature survey

2.1 Review of MASS operation sector by IMO

The IMO is currently developing the MASS Code to ensure the safe operation and navigation of MASS The code is intended to be adapted as a non-mandatory code in 2026, in a way that will facilitate a future transition to mandatory status. It outlines the

design, functional, and operational requirements of MASS to ensure safe, secure, and environmentally sound operations, while also considering necessary revisions to existing IMO instruments—such as SOLAS—that may be impacted by the shift to autonomous navigation (International Maritime Organization (IMO), 2024). This means that the increasing use of automation in ship operations, along with the expected increase in remote control and autonomous operation of key functions, requires a change in approach. This will require adjustments to the existing standards for onboard manual intervention and control, as reflected in SOLAS and other IMO instruments (International Maritime Organization (IMO), 2025).

In this code, MASS is a ship which, to a varying degree, can operate independently of human interaction (International Maritime Organization (IMO), 2024). Its operational context includes all aspects of ship function—whether performed autonomously or remotely—as well as the external environment that may affect performance. This context encompasses the Concept of Operations (ConOps), the Operational Envelope (OE), system-specific Operational Design Domains (ODDs), degraded states, fallback states, Modes of Operation (MoO), and Operator Control Modes (OCMs) (International Maritime Organization (IMO), 2025).

The OE refers to the normal operational capabilities and limitations of the ship as a whole under autonomous or remote operation. Within the OE, the ODD defines the safe operating conditions and boundaries for specific functions or systems. According to Chapter 8 of the MASS Code, establishing the OE involves the following considerations (International Maritime Organization (IMO), 2025):

1. The definition of the ship functions and conditions and its use case(s);
2. The geographic area of operations, including coverage/connectivity and traffic conditions;
3. The description of the environmental limitations;
4. The description of operational limitations for different modes of operation during a single voyage;
5. The use and management of the modes of operation, including the division of functions and allocation of tasks between humans and automation; and
6. Any other factors that have a significant impact on MASS operations.

In addition, the MoO of MASS could be changed according to the situation at each navigation stage. The criteria, procedures, and methods for such transitions should be described in advance and included in the ConOps. According to chapter 8 of the MASS Code, the description of MoO should also identify (International Maritime Organization (IMO), 2025):

1. Which ship functions are autonomous or remotely operated;
2. How autonomous or remotely operated ship functions are allocated to different agents (human or software);
3. How the affected ship functions are supervised, and by which agents;
4. Where the different agents are located (on -board or remote); and
5. Which other systems and other roles (personnel) are involved in performing the control action.

When a MASS is no longer in a safe operating state and faces a high risk of an accident, predefined actions and procedures for entering and recovering from a degraded or fallback state should be in place. In particular, if the vessel deviates from its OE, it should transition into a predefined fallback state to provide an additional layer of mitigation. These measures are intended to prevent further deterioration of the ship's condition or increases in risks to life at sea, other ships, infrastructure, or the marine environment.

The literature review for this study was conducted based on the most recent developments in IMO discussions and updates to the MASS Code. Key IMO committee reports and regulatory guidelines were reviewed to ensure this study aligns with the latest international regulatory frameworks governing MASS operations. As noted earlier, the IMO is currently developing a non-mandatory code for adoption in 2026 and is actively discussing specific requirements and standards for MASS operation. Since MASS remains in the technology development phase, it is expected that practical requirements and procedures will be established in the future based on real-world MASS operation data.

2.2 Review on the previous research

The application of the STPA to autonomous maritime systems has emerged only recently as a method to proactively identify hazards associated with autonomous ship operations and for supporting safety-informed design. In several earlier studies, the development of a hierarchical control structure—corresponding to Step 2 of the STPA methodology, which involves modeling the system's control structure to identify unsafe control actions—was omitted due to the limited availability of detailed technical and functional information about the autonomous ship systems in question (Banda and Kannos, 2017; Omitola et al., 2018).

Instead, these studies focused on applying Steps 3 and 4 of STPA, which involve identifying unsafe control actions and determining their causal scenarios, in order to derive critical safety information relevant to early-stage design of autonomous vessel concepts. For example, Valdez Banda and Kannos proposed a methodology for identifying and mitigating hazards in the operation of autonomous urban ferries (Banda and Kannos, 2017), while Omitola et al. investigated cybersecurity risks affecting navigation in conceptual autonomous ship systems (Omitola et al., 2018).

In contrast, Wróbel et al. conducted a preliminary STPA-based hazard analysis for autonomous merchant vessels, supported by a simplified but defined safety control structure (Wróbel et al., 2018). Despite acknowledging the lack of operational data as a significant constraint, their study highlighted the value of even a basic control

structure for analyzing system-level uncertainties (Wróbel et al., 2018). This framework was later reused in a follow-up study involving fully autonomous ship models (Wróbel et al., 2019).

Solberg applied STPA to the ReVolt prototype vessel, developing a tailored control structure and proposing design enhancements based on hazard analysis outcomes (Solberg, 2018). Similarly, Zou applied STPA to a generic autonomous ship model composed of three simplified functional blocks and compared the effectiveness of STPA with other hazard analysis techniques (Zou, 2018). The study provided recommendations for refining the identification of unsafe control actions and their causal pathways. STPA was also reapplied to the ReVolt model to construct a more detailed control architecture (Zou, 2018).

Rokseth et al. proposed a methodological framework for deriving system requirements and verification procedures for autonomous ships using STPA (Rokseth et al., 2019). Their approach featured a hierarchical control structure composed of key operational subsystems, including automatic sailing, autopilot, motion control, and power systems, and resulted in a set of generalized functional requirements (Rokseth et al., 2019).

Utne et al. applied STPA in a case study involving an autonomous ship concept, where the control structure was modeled at a high level of abstraction with three control layers: monitoring, guidance, and execution (Utne et al., 2020). The study aimed to integrate the STPA results into a Bayesian Belief Network to support real-time risk management in autonomous maritime systems, focusing especially on the guidance layer responsible for risk-informed decision-making (Utne et al., 2020).

Glomsrud and Xie applied STPA to a joint analysis of safety and security in unmanned surface vessels (Glomsrud and Xie, 2019). Acknowledging the limited guidance STPA provides for control structure modeling under conditions of limited system knowledge, they proposed a novel approach to bridge Step 1 and Step 2 of the methodology. Their method derived high-level functional requirements from system-level hazards and used them to construct a simplified control model (Glomsrud and Xie, 2019).

More recently, Chaal et al. proposed a structured framework to support the development of hierarchical control structures for autonomous ships, emphasizing the importance of integrating both technical functions and organizational processes early in the design phase (Chaal et al., 2020). Their findings reaffirm the relevance of seafarers' practical knowledge in defining functional roles and highlight that the introduction of autonomous ships into current maritime organizational systems presents safety and integration challenges that must be addressed from the outset (Chaal et al., 2020).

3 Analytical framework and methodology

3.1 Degraded state of MASS

In addition to the definitions of the OE and the ODD, a MASS can operate within a predefined OE as long as it remains in normal operating conditions that align with the criteria of its designated ODD (International Maritime Organization (IMO), 2024).

Redundancy refers to the duplication of critical equipment in parallel, ensuring that if one component fails, an alternative system can immediately take over its function. This concept minimizes operational disruption by providing an immediate replacement in the event of failure. However, Eriksen (Eriksen and Lützen, 2022) analyzed the impact of equipment redundancy on system reliability and highlighted that redundancy is not a perfect solution—particularly when redundant components fail due to a common underlying cause, leading to cascading failures. Nevertheless, redundancy remains highly effective in mitigating single-point failures, which is why autonomous ships fundamentally adopt redundant system architectures (Eriksen and Lützen, 2022).

In the MASS Code developed by the IMO, Degraded state and Fallback States are defined as shown in Table 1. The deviation of a single autonomous or remotely operated system or function from its ODD does not necessarily imply that the ship has deviated from its OE (International Maritime Organization (IMO), 2025). A degraded state refers to a condition in which an individual autonomous or remotely operated system or function exceeds its ODD, but the ship as a whole can still operate safely within its OE. In other words, even if one part of the system is no longer functioning within its designed parameters, the ship's integrated systems continue to support safe operation.

A MASS is composed of multiple subsystems, each with the potential for failure or malfunction. The MASS can operate within a predefined OE as long as it remains in normal operating conditions that comply with the criteria of its designated ODD. It is essential to consider scenarios in which specific equipment or systems may fail. To address such situations, redundancy can be employed as a potential solution. A degraded state ensures that the failure of a single component or function does not immediately interrupt the ship's operation. It acts as an intermediate stage between normal operation and a fallback state, providing time and flexibility for the vessel to respond appropriately. However, addressing individual component failures alone is insufficient when defining the operational boundaries of a MASS. Therefore, this study aims to analyze the degraded state through the adoption of the STPA methodology, which enables a comprehensive examination of the system's architecture under assumed MASS operational conditions.

TABLE 1 Degraded state and fallback state.

Term	Description
Degraded state	Degraded state means a deviation in the normal operation or condition of the vessel which can potentially result in a fallback state.
Fallback state	Fallback state means a designed state that can be entered through a fallback response when it is not possible for the MASS to stay within the operational envelope.

3.2System theoretic process analysis

3.2.1 Overview

STPA is a hazard analysis process that identifies potential risks and causes of accidents from a system-wide perspective (Leveson and Thomas, 2018). Unlike traditional hazard analysis methods, STPA assumes that accidents can occur not only due to component failures but also due to unsafe interactions between system components, even if no individual component has failed (Leveson and Thomas, 2018).

Traditional hazard analysis techniques, including FTA (Fault Tree Analysis), FMEA (Failure Modes and Effects Analysis), HAZOP (Hazard and Operability Study), and ETA (Event Tree Analysis), are based on sequential accident models (Ministry of Science and ICT & Telecommunication Technology Association, 2018). These methods assume that system failures are caused by one or more faulty components, and that accidents can be prevented by identifying and addressing those faulty components. However, these traditional methods have shown limitations in effectively addressing emerging risks, as modern systems have become increasingly complex and interconnected (Nancy, 2011). STPA has gained attention as a method to overcome these limitations. Unlike sequential accident models that view a system as a simple collection of components, STPA perceives a system as an integrated entity with complex interdependencies. Accidents are considered to result not only from component failures but also from incorrect control actions or unsafe commands that affect overall system safety (Ministry of Science and ICT & Telecommunication Technology Association, 2018).

Nancy G. L. introduced STPA in 2011 as a system-theoretic accident model to address the shortcomings of traditional hazard analysis methods (Leveson and Thomas, 2018). STPA analyzes the system from an integrated perspective, focusing on unsafe interactions and control failures rather than just component malfunctions (Nancy, 2011). Studies have shown that STPA can identify all accident scenarios detectable by traditional methods, as well as additional accident scenarios that would be difficult to uncover using conventional techniques. Moreover, STPA requires fewer resources and less time compared to traditional methods (Nancy, 2011).

STPA has been increasingly adopted across various industries, including aviation, automotive, nuclear energy, and healthcare, since its introduction in 2011. Research and applications of STPA continue to grow, highlighting its effectiveness in modern complex systems (VWAY).

3.2.2 Procedure

STPA is based on the concept that "a system must control safety constraints to ensure system safety" (Leveson and Thomas, 2018). Unlike traditional methods that view hazards as malfunctions of specific functions or component failures, STPA assumes that accidents may originate from control issues between systems or components rather than from individual component failures (Leveson and Thomas, 2018). In this approach, system components are not limited to hardware or software, but also include organizations, regulations, personnel, and environmental factors (Leveson and Thomas, 2018). STPA-based hazard analysis examines the system from a control perspective, identifying inadequate control actions that could lead to hazards (Leveson and Thomas, 2018). The STPA hazard analysis process consists of four main steps:

1) Define losses and hazards

The first step is to define the types of losses to be prevented (e.g., injury, property damage, mission failure) and establish the system's controllable scope. Hazards, which are system states or conditions that can lead to losses, must be identified and linked to at least one predefined loss. While losses may include uncontrollable environmental factors, hazards are considered manageable through design and control measures (Nancy, 2011).

2) Diagram the control structure

The second step is to develop a control structure that identifies the necessary subsystems to prevent hazards and maintain safety constraints. This process involves abstracting the system at a high level and gradually refining it into more detailed models. Typically, the controller is placed at the top and the controlled process at the bottom, with control actions represented by downward arrows and feedback by upward arrows. The process model represents the internal beliefs, information, and rules that the controller relies on to make decisions (Nancy, 2011).

3) Identify Unsafe Control Actions (UCA).

UCAs refer to control actions that could lead to system hazards. Derived from the control structure, UCAs identify unsafe forms of control actions. Depending on the analysis scope, only specific control actions may be considered. Two key factors are analyzed:

a. how the controller issues control actions
b. the specific conditions or situations in which these actions occur (Nancy, 2011).

4) Develop loss scenarios based on UCAs

The loss scenarios are developed based on UCAs. The causes of losses can be intuitively derived from the control structure and are categorized into two types. The first type identifies why a control action was provided unsafely, including failures within the controller (e.g., faulty algorithms, incorrect commands, or inaccurate process models) and issues with feedback or information transmission (e.g., communication delays, errors, or missing data). The second type examines why a control action was not executed or was performed improperly, focusing on issues within the control path (e.g., communication failures, actuator errors) or the controlled process (e.g., incorrect input values, environmental factors, component failures, or command conflicts between controllers). These identified causes form the basis for constructing loss scenarios (Nancy, 2011).

This study aims to derive accident scenarios related to degraded state conditions that may occur during the operation of a MASS using the STPA methodology. Figure 1 presents the flowchart analyzed using the STPA method and the analytical model used in this study.

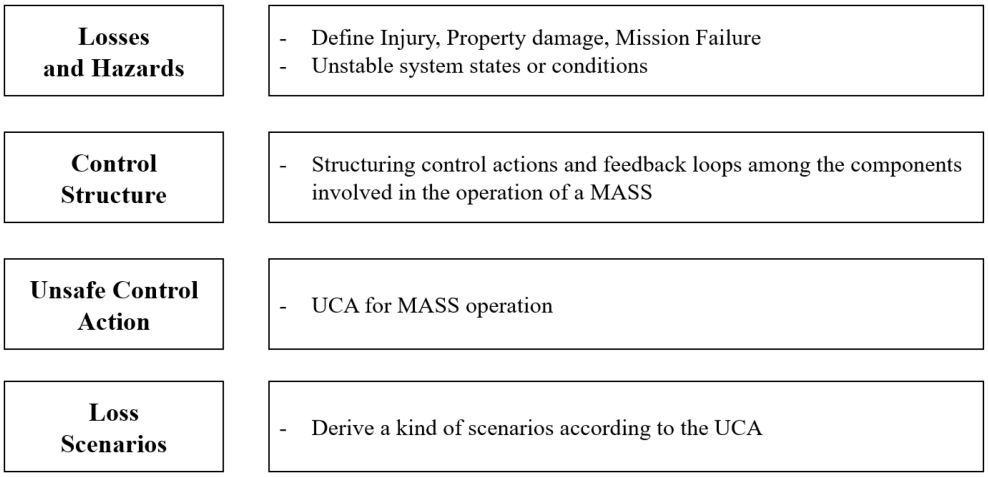

FIGURE 1
Flowchart to make STPA modelling.

4 MASS modelling

4.1 Definition of losses and hazard in the degraded state

The losses associated with a degraded state can be classified in the context of MASS, as shown in Table 2, into major accidents, minor accidents, schedule delays of the MASS, and cost losses. The classification of marine accidents is based on Article 2 of the *Korean Act on the Investigation of and Inquiry into Marine Accidents* (Ministry of Oceans and Fisheries, 2020).

The term "marine accident" means any of the following accidents, which happen at sea and in the inland waters:

1. An accident in which a person dies, disappears, or is injured in connection with the structure, equipment, or operation of ships;
2. An accident which causes damage to a ship or shore or marine facilities in connection with the operation of ships;
3. An accident in which a ship is lost, derelict, or missing;
4. An accident in which a ship collides with another ship, is stranded, capsizes, or sinks, or it is impossible to steer a ship;
5. An accident that causes marine pollution damage in connection with the operation of shipsIn this study, a major accident is defined as a case in which the affected ship becomes non-operational, there is a loss of human life, or a severe marine pollution incident occurs.

System-level hazards refer to specific system states or conditions —under defined worst-case environmental scenarios—that may lead to losses. A system is a collection of components that work together as a whole to achieve certain common goals and intended outcomes. The connection between the 10 identified hazards and the 4 types of losses is shown in Table 3. The hazards and losses identified in this study were derived from expert workshops involving maritime safety experts, combined with insights from IMO regulatory documents and relevant maritime safety literature.

TABLE 2 Description of Loss under degraded state.

No	Loss	Description
L-1	Major Accident	- In the event that the MASS is unable to operate (e.g. Fire, Grounding, Capsizing etc.) - Loss of life - Severe marine pollution
L-2	Minor Accident	- A marine accident that does not interrupt ship operation
L-3	Schedule Delay	- Failure to meet the designated berthing schedule or pilot boarding time
L-4	Cost Loss	- Cost loss incurred due to an accident.

TABLE 3 Hazard under degraded state.

No	Hazard	Tracking with Loss
H-1	Failure of a remote-control system	L-1, L-2, L-3
H-2	Failure of a propulsion/ thruster system	L-1, L-2, L-3
H-3	Failure of sensors	L-1, L-2, L-3
H-4	Failure of connectivity	L-1, L-2, L-3
H-5	Vessel not under command	L-1, L-3, L-4
H-6	Misunderstanding by RO	L-2, L-3
H-7	Cybersecurity Threats	L-1, L-2, L-3, L-4
H-8	Unexpected weather-related risk	L-1, L-2, L-3
H-9	Crew interaction complexity	L-2, L-3
H-10	Unexpected risk by cargo condition	L-1, L-2, L-3, L-4

The loss categories follow the classifications in Article 2 of the *Korean Act on the Investigation of and Inquiry into Marine Accidents*, ensuring their validity and relevance.

4.2 Analysis of the control structure

The control structure of a MASS encompasses the relationships between control actions and feedback among key entities, including the ROC, management companies, the Flag State, the Port and Coastal States, cyber threats, and emergency situations. This control structure is not limited to hardware systems but is designed to incorporate various elements such as organizations, equipment, technologies, regulations, information, actions, and environmental factors that influence the operation of MASS. The overall relationships among these entities and the control flows are illustrated in Figure 2.

The ROC serves as the central hub for controlling MASS operations, where the RO monitors the ship and makes navigational decisions. The RO can directly control the MASS via a remote system or use automated systems to determine the route. Additionally, manual override can be executed when necessary. The ROC continuously receives operational status feedback from MASS, ensuring navigational safety and system efficiency. The Flag State performs a crucial role in applying operational regulation and approving compliance for both the MASS and the ROC management companies. The ROC management company provides operational information, manages vessel specifications, and monitors MASS operations.

The MASS management company oversees the ship's operations based on information received from the ROC management company and ensures compliance with Flag State regulations. The automation system within the MASS supports the RO's navigational decisions and can independently determine navigation routes when needed. The MASS transmits operational status data to the ROC and management companies and is equipped to respond immediately to cyber threats or emergency situations. In the event of an emergency, an alert system is activated, transmitting crisis response data and emergency signals. The Port State and Coastal State manage scheduling, transit, and berthing regulations for the MASS, continuously monitoring its operational status. These entities influence the ship's schedule and ensure adherence to navigation regulations within their respective maritime domains.

The control algorithm of the MASS is executed by the ROC and RO, working in coordination with automation systems to make operational decisions. Navigation can be performed through direct control by the RO, automated decision-making, or manual override when necessary. Cargo operations are also carried out either through remote control by the RO or via automation.

The emergency alert system is a critical component of crisis response, automatically activating during emergencies and

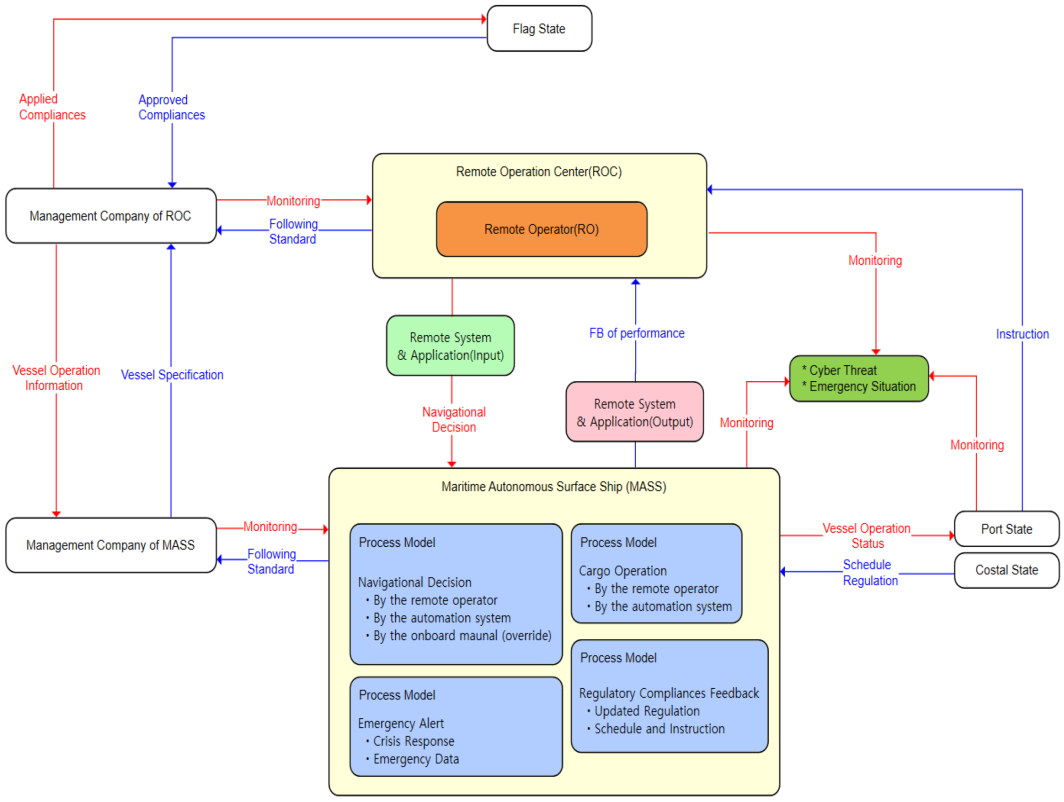

FIGURE 2
Control structure of MASS operation.

transmitting current status and response measures to the ROC. The control structure illustrated in Figure 2 was developed through a detailed analysis of existing MASS operational frameworks, supported by expert interviews with personnel involved in the Korean MASS R&D project and maritime safety experts. Reference materials included IMO guidelines, published studies, and operational documentation from pilot MASS projects.

MASS utilizes a variety of sensors and actuators to collect operational data, which is then analyzed by the RO and automation systems to facilitate navigation decisions. Key sensors include remote data collection systems, maritime surveillance radars, vessel information system imaging, wireless communication networks, and satellite data analysis systems. Actuators consist of command transmission systems for the RO, automation-based operational systems, and emergency response mechanisms.

Several external environmental factors affect MASS operations. These include adverse weather conditions such as typhoons and high waves; cybersecurity threats; technical failures such as communication errors and sensor malfunctions; and potential accidents, including grounding, collisions, or sinking. As these factors directly impact operational stability, continuous monitoring and proactive countermeasures are essential.

In conclusion, the control structure of MASS is designed to facilitate interaction among the ROC, management companies, regulatory authorities, and the ship itself. With real-time monitoring and feedback systems in place, the safety and efficiency of autonomous vessel operations can be maintained. Moreover, the system is structured to provide rapid responses to cyber threats and emergency situations through a collaborative framework between automation systems and remote operators.

4.3 Analysis of the UCA

In the STPA handbook, control actions that can lead to UCAs are broadly classified into four types (Nancy, 2011):

a. Not providing the control action leads to a hazard
b. Providing the control action leads to a hazard
c. Providing a potentially safe control action, but too early, too late, or in the wrong order
d. The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones)

When identifying UCAs, deriving the context is essential. The handbook recommends that each UCA must include its context, taking into account environmental conditions, the state of the controlled process, the controller's status, prior actions, and relevant parameters (Nancy, 2011).

Deriving this context requires significant effort, expert opinions, and detailed input from developers (Nancy, 2011). As illustrated in Figure 2, various control actions are exchanged between each controller and the controlled process. For the purpose of identifying UCAs, a comprehensive list of control actions within MASS operations is summarized in Table 4. This identification process is supported by various reference documents during the UCA phase of STPA analysis for MASS. The operational scenarios were developed by referring to current conventional ship operation practices.

Table 5 presents the identified UCAs based on these operational scenarios, categorized by control action type. UCAs and subsequent Loss Scenarios (LS) were systematically derived following STPA guidelines. Initial UCAs were formulated through literature reviews, historical maritime incident analysis, and expert input. Each UCA was then explored through scenario-based analysis in expert workshops, resulting in a comprehensive list of loss scenarios reflecting realistic operational contexts.

A total of 92 LSs were derived based on the 31 identified UCAs. The causes of these loss scenarios are diverse and complex. Each loss scenario was analyzed from two main perspectives:

a. Why the UCA occurred, and
b. Why the control action was not executed or was executed inappropriately.

4.4 Deriving a loss scenarios

For each UCA, LSs were systematically derived by examining the behavior of the corresponding independent controller. A standardized cause analysis approach was used, modeling each LS based on the structure and behavior of the controller. Each LS is denoted as [LS-XX], and its association with a UCA is marked as [UCA-X]. For example, for [UCA-4], "The MASS does not activate backup propulsion when primary propulsion fails", the corresponding loss scenarios include [LS 4-1]. The MASS drifts into a high-traffic zone [LS 4-2]. The MASS drifts toward a shallow

TABLE 4 List of controls between controller and target.

Control Action	Controller	Control Target
Navigation Control Actions	Remote Operation Center	MASS
Propulsion & Speed Control Actions	Remote Operation Center	MASS
Sensor Control Actions	Sensor, Equipment	MASS
Communication	Remote Operation Center Onboard Crew	MASS Remote Operation Center
Cybersecurity & Unauthorized Access Control Actions	Security Monitor System Remote Operation Center	MASS
Human Interaction	Remote Operator Onboard Crew	MASS

TABLE 5 List of UCA.

No	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon
Navigation Control Actions	**UCA-1**: ROC does not send navigation commands when MASS loses autonomy. **UCA-10**: The MASS updates navigation decisions too late after recovering sensor data. **UCA-12**: The MASS does not operate to remote control mode after losing communication. **UCA-23:** The MASS mistakenly blocks a legitimate control action.	**UCA-2**: ROC sends conflicting navigation commands. **UCA-3**: ROC sends multiple conflicting commands in an incorrect order.	**UCA-25**: The MASS does not adjust its route based on real-time weather updates. **UCA-26**: The MASS overreacts to minor weather fluctuations.	
Propulsion & Speed Control Actions	**UCA-4:** The MASS does not activate backup propulsion when primary propulsion fails.	**UCA-5:** The MASS engages propulsion despite damage. **UCA-17:** The MASS engages propulsion while in NUC state.	**UCA-6:** The MASS activates an emergency stop command too late. **UCA-7:** The MASS sends conflicting speed commands to different propulsion units.	**UCA-28:** The onboard crew overrides ROC's decisions incorrectly (e.g., cancels an emergency stop prematurely).
Sensor Control Actions	**UCA-8**: The MASS does not activate backup sensors when primary sensors fail. **UCA-30:** The MASS does not detect shifting cargo in time. **UCA-31:** The MASS misidentifies a hazardous cargo condition.	**UCA-9**: The MASS misinterprets sensor data and falsely detects an obstacle.	**UCA-11**: The MASS switches between sensors erratically, leading to conflicting readings.	
Communication	**UCA-13**: The MASS delays communication recovery response. **UCA-15**: The MASS does not activate emergency signals when NUC occurs.	**UCA-16:** The MASS transmits a false NUC signal.	**UCA-14:** The MASS switches between communication channels excessively, causing unstable data transmission. **UCA-18**: The MASS fails to stabilize when drifting.	**UCA-29:** Communication failures delay crucial decision-making.
Cybersecurity & Unauthorized Access Control Actions	**UCA-22**: The MASS does not detect an unauthorized command injection.	**UCA-24**: The MASS delays security measures when detecting a cyberattack.	**UCA-23:** The MASS mistakenly blocks a legitimate control action (e.g., preventing a stop command).	
Human Interaction	**UCA-19:** The RO mistakenly overrides a correct manual control by onboard. **UCA-27:** The onboard crew does not respond to critical alerts.	**UCA-21:** The RO issues contradictory commands due to misunderstanding the MASS's status.	**UCA-20:** The RO delays response during an emergency.	

Bold: UCA, Unsafe Control Actions.

area. Through this methodical approach, the study identified a total of 92 loss scenarios linked to the UCAs.

4.4.1 Loss scenarios for navigation control actions

The control actions related to navigation pertain to the MASS's ability to maintain its course during operation. It is assumed that the vessel receives real-time updates of optimized routes from the onboard autonomous navigation system. A total of 8 UCAs were identified in this category, from which 21 LSs were derived. The corresponding LSs for each UCA are summarized in Table 6.

4.4.2 Loss scenarios for propulsion system

The control actions under the propulsion system pertain to the maneuvering of the MASS and include all actions related to the ship's actual movement throughout the voyage, including system connectivity with the ROC. A total of 6 UCAs were identified in this category. From these, 20 loss scenarios (LSs) were derived. The corresponding LSs for each UCA are summarized in Table 7.

4.4.3 Loss scenarios for sensors

The control actions related to sensors involve potential malfunctions or imperfect operation of sensors installed either on the autonomous ship or at the ROC for remote operation. These sensors are not limited to navigation but also include those related to cargo condition and overall vessel safety (e.g., fire detection, flooding sensors). A total of 5 UCAs were identified in this category. From these, 17 LSs were derived. The corresponding LSs for each UCA are summarized in Table 8.

TABLE 6 List of LS for navigation control action.

Unsafe Control Action	Loss Scenario
UCA-1: ROC does not send navigation commands when MASS loses autonomy.	**LS-1** The MASS drifts uncontrollably due to lack of commands.
	LS-2 The MASS enters incorrect area due to lack of commands.
	LS-3 The MASS does not fit a berthing schedule due to navigation command delay.
UCA-10: The MASS updates navigation decisions too late after recovering sensor data.	**LS-4** The MASS does not react in time to an approaching vessel.
	LS-5 The MASS fails to adjust for new weather conditions.
	LS-6 The MASS miscalculates its approach angle during docking.
	LS-7 The MASS responds too late to an ice detection warning.
UCA-12: The MASS does not operate to remote control mode after losing communication.	**LS-8** The MASS drifts uncontrollably after communication loss.
	LS-9 The MASS fails to avoid a navigational hazard due to lost control.
	LS-10 The MASS fails to control in the middle of a busy route, causing disruption.
	LS-11 The MASS continues executing last-received commands.
UCA-23: The MASS mistakenly blocks a legitimate control action.	**LS-12** The MASS ignores an emergency stop command.
	LS-13 The MASS denies a course correction request due to security restrictions.
UCA-2: ROC sends conflicting navigation commands.	**LS-14** The MASS alternates between two course corrections, leading to erratic movement.
	LS-15 The MASS receives an outdated command and turns to incorrect route.
UCA-3: ROC sends multiple conflicting commands in an incorrect order.	**LS-16** The MASS engages full throttle before completing a turn.
	LS-17 The MASS attempts to stop before changing course.
UCA-25: The MASS does not adjust its route based on real-time weather updates.	**LS-18** The MASS enters into a severe weather condition like a typhoon due to outdated weather data.
	LS-19 The MASS does not reroute around an ice field.
UCA-26: The MASS overreacts to minor weather fluctuations.	**LS-20** The MASS performs an unnecessary course change, increasing travel distance.
	LS-21 The MASS reduces speed unnecessarily in moderate waves.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

TABLE 7 List of LS for propulsion system.

Unsafe Control Action	Loss Scenario
UCA-4: The MASS does not activate backup propulsion when primary propulsion fails.	**LS-22** The MASS drifts into a high-traffic zone.
	LS-23 The MASS drifts towards a shallow area.
	LS-24 The MASS becomes unresponsive during docking.
	LS-25 The MASS drifts for hours, causing a schedule delay.
UCA-5: The MASS engages propulsion despite damage.	**LS-26** The MASS engages full power despite engine damage, leading to severe accident like fire.
	LS-27 The MASS moves while the thruster is jammed.
	LS-28 The MASS tries to stop but fails due to engine overload.
	LS-29 The MASS burns excessive fuel due to a hidden engine malfunction.
UCA-17: The MASS engages propulsion while in NUC state.	**LS-30** The MASS's propulsion system sustains further damage due to forced operation.
	LS-31 The MASS unintentionally moves into a hazardous area.
	LS-32 The MASS accelerates abruptly, causing onboard cargo damage.
	LS-33 The MASS's propulsion reactivation overloads the electrical system.
UCA-6: The MASS activates an emergency stop command too late.	**LS-34** The MASS collides because it fails to stop in time.
	LS-35 The MASS runs aground because it does not decelerate in time.
	LS-36 The MASS's emergency braking causes internal cargo damage.
	LS-37 The MASS delays stopping, leading to a schedule delay.
UCA-7: The MASS sends conflicting speed commands to different propulsion units.	**LS-38** The MASS becomes unstable due to alternating speed commands.
	LS-39 The MASS overreacts to a speed reduction command.
UCA-28: The onboard crew overrides ROC's decisions incorrectly.	**LS-40** Crew cancels an emergency stop command, leading to a collision.
	LS-41 Crew manually increases speed in rough weather against ROC's recommendations.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

TABLE 8 List of LS for sensors.

Unsafe Control Action	Loss Scenario
UCA-8: The MASS does not activate backup sensors when primary sensors fail.	**LS-42** The MASS drifts into a high-traffic zone.
	LS-43 The MASS drifts towards a shallow area.
	LS-44 The MASS becomes unresponsive during docking.
	LS-45 The MASS drifts for hours, causing a schedule delay.
UCA-30: The MASS does not detect shifting cargo in time.	**LS-46** The MASS suffers severe listing or capsizing due to unnoticed cargo shift.
	LS-47 Internal structural damage occurs from undetected cargo movement.
	LS-48 The MASS loses maneuverability due to unbalanced load, drifting into hazardous areas.
	LS-49 Cargo shift damages critical ship systems or propulsion equipment.
UCA-31: The MASS misidentifies a hazardous cargo condition.	**LS-50** The MASS unnecessarily initiates emergency response, disrupting operations.
	LS-51 Failure to correctly identify hazardous cargo leads to mishandling and potential accidents.
	LS-52 The MASS incorrectly alerts authorities, wasting emergency response resources.
	LS-53 False hazardous cargo detection leads to unnecessary route diversions, increasing operational costs.
UCA-9: The MASS misinterprets sensor data and falsely detects an obstacle.	**LS-54** The MASS performs an emergency stop in open waters due to a false obstacle detection.
	LS-55 The MASS reroutes unnecessarily, increasing fuel costs.
	LS-56 The MASS slows down unexpectedly, causing congestion.
	LS-57 The MASS takes evasive action for a non-existent hazard.
UCA-11: The MASS switches between sensors erratically, leading to conflicting readings.	**LS-58** The MASS moves abnormally due to discrepancies between sensors.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

4.4.4 Loss scenarios for connectivity

The control actions related to connectivity pertain to the communication and connection status between the MASS and the ROC, as well as among system components within the ship itself. A total of 6 UCAs were identified in this category. From these, 17 LSs were derived. The corresponding LSs for each UCA are summarized in Table 9.

TABLE 9 List of LS for connectivity.

Unsafe Control Action	Loss Scenario
UCA-13: The MASS delays communication recovery response.	**LS-59** The MASS remains in fail-safe mode longer than necessary, delaying operations.
	LS-60 The MASS does not update its navigation system after connectivity restoration.
	LS-61 The MASS ignores a critical system update after regaining connection.
UCA-15: The MASS does not activate emergency signals when NUC occurs.	**LS-62** The MASS drifts into a busy traffic lane without warning.
	LS-63 The MASS drifts into a shallow water.
	LS-64 A rescue tug arrives late due to missing NUC alerts.
	LS-65 Port traffic controllers remain unaware of the vessel's distress.
UCA-16: The MASS transmits a false NUC signal.	**LS-66** Nearby vessels take unnecessary evasive action, increasing collision risk.
	LS-67 A rescue operation is dispatched unnecessarily, wasting emergency resources.
	LS-68 The MASS is denied entry into a port due to an incorrect NUC declaration.
	LS-69 The MASS incorrectly activates collision avoidance systems due to a false NUC alert.
UCA-14: The MASS switches between communication channels excessively, causing unstable data transmission.	**LS-70** The MASS receives conflicting navigation data due to unstable network switching.
	LS-71 The MASS loses connection completely after excessive network switching.
UCA-18: The MASS fails to stabilize when drifting.	**LS-72** The MASS drifts into a strong current, pushing it off course.
	LS-73 The MASS rolls excessively, causing damage to sensitive cargo
UCA-29: communication failures delay crucial decision-making.	**LS-74** Delayed crew response to an engine control leads to drift.
	LS-75 Crew misinterprets remote commands, leading to incorrect maneuvers.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

4.4.5 Loss scenarios for cybersecurity

The control actions related to cybersecurity involve unauthorized access, hacking, or ransomware infiltration directly targeting the MASS. These actions are also associated with potential delays or operational losses resulting from such cyber threats. A total of 3 UCAs were identified in this category. From these, 7 loss scenarios (LSs) were derived. The corresponding LSs for each UCA are summarized in Table 10.

TABLE 10 List of LS for cybersecurity.

Unsafe Control Action	Loss Scenario
UCA-22: The MASS does not detect an unauthorized command injection.	**LS-76** A hacker gains control and sends a false navigation command.
	LS-77 A hacker manipulates The MASS's speed controls.
	LS-78 A ransomware attack locks The MASS's control systems.
	LS-79 Cyberattack disables emergency response systems.
UCA-24: The MASS delays security measures when detecting a cyberattack.	**LS-80** The MASS remains exposed to a cyberattack longer than necessary.
UCA-23: The MASS mistakenly blocks a legitimate control action (e.g., preventing a stop command).	**LS-81** The MASS ignores an emergency stop command.
	LS-82 The MASS denies a course correction request due to security restrictions.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

4.4.6 Loss scenarios for human interaction

Although an autonomous navigation system is installed on the MASS, remote operation still involves human input, and command errors or misunderstandings by the RO or onboard crew cannot be completely ruled out. Therefore, the control actions related to human interaction include imperfect actions or behaviors by the RO and onboard crew. A total of 4 UCAs were identified in this category. From these, 10 loss scenarios (LSs) were derived. The corresponding LSs for each UCA are summarized in Table 11.

TABLE 11 List of LS for human interaction.

Unsafe Control Action	Loss Scenario
UCA-19: The RO mistakenly overrides a correct manual control.	**LS-83** The RO overrides an onboard maneuver, causing a collision.
	LS-84 The RO incorrectly overrides operation, extending the voyage duration.
UCA-27: The onboard crew does not respond to critical alerts.	**LS-85** Crew fails to respond to an engine failure alert.
	LS-86 Crew ignores a navigation hazard alert due to communication errors.
	LS-87 Crew fails to respond to an onboard security breach.
UCA-20: The RO delays response during an emergency.	**LS-88** The RO fails to respond in time to a critical engine failure.
	LS-89 The RO does not respond quickly to an approaching vessel.
	LS-90 The RO delays response to abnormal condition, leading to delay schedule.
UCA-21: The RO issues contradictory commands due to misunderstanding the MASS's status.	**LS-91** The RO orders simultaneous acceleration and turning, destabilizing The MASS.
	LS-92 The RO mistakenly switches between manual and remote control, confusing the system.

Bold: UCA, Unsafe Control Actions; LS, Loss Scenarios.

4.5 Discussion and future works

This study conducted a safety analysis of MASS operating under degraded conditions using the STPA methodology. STPA effectively identifies complex interactions and unsafe control actions within the overall MASS system architecture. Unlike traditional hazard analysis methods that focus solely on component failures, STPA emphasizes systemic interactions and control issues. As such, it serves as a proactive tool capable of revealing potential hazards and loss scenarios that might otherwise remain undetected by conventional approaches.

However, STPA is not without limitations —particularly in detecting "unknown unknowns." Because STPA relies heavily on predefined control structures, hazards, and loss conditions, unforeseen operational situations or entirely unpredictable events may fall outside its analytical scope. Thus, its effectiveness in capturing risks beyond the defined boundaries remains limited. Moreover, actual operational data for MASS remains extremely scarce, and the precise ways in which MASS will emerge and operate within the maritime industry remains largely unknown.

To address these methodological constraints, this study integrated various resources, including expert workshops and the latest IMO MASS Code updates, to develop a comprehensive and realistic control structure. Although the rigorous STPA process employed aimed to encompass a wide range of operational scenarios, unpredictable events arising from subtle interactions among system components remain difficult to eliminate entirely. Future research should continue to address these gaps through complementary analytical approaches, such as anomaly detection using machine learning and scenario-based resilience assessments.

Additionally, the ongoing accumulation of operational data from real-world MASS deployments will be essential. Regular updates and validations of STPA outcomes using empirical data can progressively enhance the methodology's reliability. Through such continuous refinements, the practical safety management of MASS operations can be significantly strengthened.

5 Conclusion

This study conducted an extensive STPA-based risk assessment aimed at enhancing operational safety during degraded operational conditions in the remote-controlled and autonomous operations of MASS. Degraded conditions—specifically defined as scenarios wherein MASS operates beyond the predetermined 'Operational Design

Domain' yet remains within allowable operational environments—present unique and complex challenges for maintaining safety and reliability. The research systematically identified critical risk factors by developing a comprehensive control structure and rigorously defining UCAs through a structured methodology.

Through this systematic approach, 31 distinct UCAs were identified, covering essential functional domains critical to MASS operations, including navigation, propulsion and speed control, sensor management, communication systems, cybersecurity measures, and human–machine interactions. Leveraging the STPA methodology, the research further derived 92 detailed LSs. Each scenario explicitly outlined potential hazardous outcomes that could arise when UCAs occurred due to absent, incorrect, untimely, or prolonged application of control actions. The classification of these loss scenarios into four categories—major accidents, minor accidents, schedule delays, and cost losses—was closely aligned with the standards established under the Korean Act on the Investigation of and Inquiry into Marine Accidents, facilitating consistency and practical applicability.

Additionally, the study identified and categorized ten system-level hazards, ensuring a direct and traceable relationship between identified system failures and their potential consequences. These system-level hazards allowed for an integrated understanding of operational risks and the conditions under which they could escalate into more significant events.

The STPA methodology proved particularly valuable by enabling the structured categorization of UCAs into four standardized classes: (a) non-provision of required control actions, (b) provision of inappropriate control actions, (c) incorrect timing of control actions, and (d) inappropriate duration of control actions. This detailed classification allowed for the clear derivation of potential failure pathways and facilitated realistic scenario analyses. These scenarios explicitly incorporated interactions among various controllers involved in MASS operations, including the ROC, RO, onboard crew, and autonomous control systems.

Significantly, the analysis highlighted not only purely technical risks—such as delayed transmission of remote operator commands, sensor failures, and communication disruptions—but also underscored critical human-related factors. Inadequate situational awareness, delayed responses, and flawed decision-making by remote operators and onboard crew were prominently identified as key contributors to operational risk.

However, the identification of UCAs represents only the foundational stage in an ongoing, iterative process toward robust safety assurance. To progress effectively, future research must emphasize the practical and systematic development of targeted countermeasures, including:

- Design of controller-specific safety constraints to proactively prevent UCA activation.
- Implementation of real-time monitoring algorithms and anomaly detection systems for early identification and management of emerging UCAs.
- Development of robust redundancy and fallback mechanisms within critical control loops, including autonomous overrides and backup systems.
- Improvement of human-machine interface (HMI) designs to minimize operational misunderstandings and enhance decision-making accuracy.
- Incorporation of advanced predictive technologies, such as machine learning algorithms and rule-based logic systems, to anticipate and proactively manage potentially unsafe control sequences.
- Strengthening cybersecurity protocols, emphasizing real-time adaptive responses to unauthorized access attempts and command injections.
- Creation of standardized libraries containing clearly defined UCA-response templates to streamline MASS design, operational guidelines, and certification processes.

Moreover, continuous validation and prioritization of identified risks through structured expert assessment methodologies —such as the Delphi method or the Analytic Hierarchy Process (AHP)—will be indispensable. These methods will ensure a data-driven and objective approach in guiding policy formation, operational enhancements, and regulatory adjustments. Comprehensive future analyses should also address emerging areas such as maritime environmental protection, cybersecurity enhancements, and optimized coordination with maritime traffic management systems.

Ultimately, sustained research and development efforts must aim to establish refined, globally accepted operational standards and regulatory frameworks. Doing so will significantly enhance the safety, resilience, and long-term operational reliability of MASS, paving the way for safer and more efficient autonomous maritime transportation systems.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material. Further inquiries can be directed to the corresponding author.

Author contributions

HP: Data curation, Writing – original draft, Methodology, Conceptualization, Investigation, Software, Formal Analysis, Resources. JK: Validation, Visualization, Project administration, Writing – review & editing, Supervision, Investigation, Funding acquisition.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This research was supported by the Korean Institute of Marine Science & Technology Promotion (KIMST), funded by the Ministry of Oceans and Fisheries, Korea. (20200615, Development of Au-tonomous Ship Technology).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

VWAY. Available online at: https://www.vway.co.kr. (Accessed January 22, 2025).

Banda, O. A. V., and Kannos, S. (2017). *Hazard analysis process for autonomous vessels. In Technical Report*. (Finland: Yrkeshögskolan Novia)

Chaal, M., Valdez Banda, O. A., Glomsrud, J. A., Basnet, S., Hirdaris, S., and Kujala, P. (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. *Saf. Sci.* 132, 104939. doi: 10.1016/j.ssci.2020.104939

Eriksen, S., and Lützen, M. (2022). The impact of redundancy on reliability in machinery systems on unmanned ships. *WMU J. Maritime Affairs* 21, 161–177. doi: 10.1007/s13437-021-00259-7

Glomsrud, J. A., and Xie, J. (2019). "A structured STPA safety and security co-analysis framework for autonomous ships," in *European Safety and Reliability conference, Germany, Hannover*. doi: 10.3850/978-981-11-2724-3_0105-cd

Internantional Maritime Organization (IMO) (2024). *Development of a goal-based instrument for Maritime Autonomous Surface Ship (MASS), Concept on the management of remote operations, MSC 108/4/2*.

International Maritime Organization (IMO) (2021). *Outcome of the Regulatory Scoping Exercise for Maritime Autonomous Surface Ships (MASS). IMO MSC.1/Circ.1638*. (London: IMO).

International Maritime Organization (IMO) (2024). *Report of the Working Group (MASS), MSC 109/WP.8*. (London: IMO).

International Maritime Organization (IMO) (2025). *Report of the Correspondence Group (MASS Code), MSC 110/5*.

Katija, K., Orenstein, E., Schlining, B., Lundsten, L., Barnard, K., Sainz, G., et al. (2021). FathomNet: A global image database for enabling artificial intelligence in the ocean. *Sci. Rep*. 12, 15914. doi: 10.1038/s41598-022-19939-2

Leveson, N. G., and Thomas, J. P. (2018). *STPA Handbook* (Cambridge, Massachusetts, USA: Massachusetts Institute of Technology).

Ministry of Oceans and Fisheries (2020). *Article 2 of the Korean Act on the Investigation of and Inquiry of Marine Accidents* (Korea Legislation Research Institute). Available online at: https://www.law.go.kr. (Accessed January 25, 2025).

Ministry of Science and ICT & Telecommunication Technology Association (2018). *Risk Analysis Guide Using STPA*. (Seoul: Telecommunication Technology Association) 2–14pp.

Nancy, G. L. (2011). "STPA: A new hazard analysis technique," in *Engineering a Safer World: Systems Thinking Applied to Safety* (Cambridge, Massachusetts, USA: MIT Press), 211–249.

Omitola, T., Downes, J., Wills, G., Zwolinski, M., and Butler, M. (2018) "Securing navigation of unmanned maritime systems". *CEUR Workshop Proceedings*, Southampton, United Kingdom, Vol. 2331. p. 53–62.

Porathe, T., Prison, J., and Man, Y. (2014). Situation awareness in remote control centers for unmanned ships. In *Proceedings of Human Factors in Ship Design & Operation*, London, UK. 93. doi: 10.3940/rina.hf.2014.12

Ringbom, H. (2019). Regulating autonomous ships—Concepts, challenges and precedents. *Ocean Dev. Int. Law*. 50 (2), 141–169. doi: 10.1080/00908320.2019.1582593

Rokseth, B., Haugen, O. I., and Utne, I. B. (2019). "Safety verification for autonomous ships," in *MATEC web of conferences*, vol. 273. (EDP Sciences), 02002.

Solberg, C. L. (2018). An STPA Analysis of the ReVolt-Expanding and Improving the System-Theoretic Process Analysis (STPA) Framework. (Trondheim, Norway: Master's thesis, NTNU).

Utne, I. B., Rokseth, B., Sørensen, A. J., and Vinnem, J. E. (2020). Towards supervisory risk control of autonomous ships. *Reliab. Eng. Syst. Saf.* 196, 106757. doi: 10.1016/j.ress.2019.106757

Wróbel, K., Krata, P., and Montewka, J. (2019). Preliminary results of a system-theoretic assessment of maritime autonomous surface ships' safety. *TransNav Int. J. Mar. Navig. Saf. od Sea Transport*. 13, 717–723. doi: 10.12716/1001.13.04.03

Wróbel, K., Montewka, J., and Kujala, P. (2017). Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. *Reliab. Eng. Syst. Saf.* 165, 155–169. doi: 10.1016/j.ress.2017.03.029

Wróbel, K., Montewka, J., and Kujala, P. (2018). Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliab. Eng. Syst. Saf.* 178, 209–224. doi: 10.1016/j.ress.2018.05.019

Zou, J. (2018). Systems-Theoretic Process Analysis (STPA) Applied to the Operation of Fully Autonomous Vessels (Master's thesis, NTNU). trondheim, Norway.