Journal of Shipping and Trade

ORIGINAL ARTICLE

Open Access

Hazard analysis of autonomous vessel operation during the interaction and execution between remote operation centre controller and onboard controllers

Mir Md Ashfaque Sumon[1*], Hyungju Kim[1] and Børge Rokseth[1]

*Correspondence:
mir.m.a.sumon@ntnu.no

[1] Norwegian University of Science and Technology (NTNU), Jonsvannsveien 105A, 7050 Trondheim, Norway

Abstract

A critical challenge in the safe operation of autonomous vessels is ensuring that control commands are executed accurately and promptly by both shore-side and onboard systems. In this paper, we build on a use case of an autonomous ship, where the control hierarchy includes Human Operators on the shoreside, along with the Ship Motion Controller, Power Management System, and Battery Management System, among other controllers on the shipside. Incorrect execution of control actions by these controllers can lead to hazardous situations of varying severity. This study aims to identify and analyze hazards related to these four controllers and provide insights into how inadequate control may occur and create hazardous situations with the controllers. Recently, STPA has emerged as the mainstream approach for identifying hazards resulting from control action failures. Therefore, this study applies the System Theoretic Process Analysis (STPA) method to explore how control actions of different controllers might fail, ensuring safe operation. A control structure hierarchy has been developed that identifies (1) control actions and (2) feedback signals between controllers based on their responsibilities. Using STPA, a total of 127 unsafe control actions are identified that could result in hazards. We classify the significance of Unsafe Control Actions based on hazard severity, operational mode, and suggest the level of attention each controller requires. The results offer a structured foundation for prioritizing safety–critical control actions in battery-powered autonomous ships, facilitating more effective risk mitigation strategies for designers, operators, and regulators.

Keywords: MASS, Autonomous controller, Battery-powered, PMS, BMS, Hazard analysis, Safety, STPA, Approval

Introduction

Automation in the maritime industry is being revolutionized with the introduction of Maritime Autonomous Surface Ships (MASS). The first project to research MASS technology was the MUNIN project (MUNIN 2015) that was developed in Norway to make a substantial contribution to the sustainability of the European shipping industry.

Successively, several other industrial approaches were initiated (Bolbot et al. 2020; SEAMLESS 2023b; Smartmaritime 2020; Yara 2021) to commercialize MASS.

Alongside the increasing emphasis on autonomy, the development of zero-emission ships has emerged as a key focus in the maritime industry. According to the IMO GHG4 study (IMO 2018b) greenhouse gas (GHG) emissions from maritime transport rose from 978 million tons in 2012 to 1.076 billion tons in 2018. With the continued growth in demand for maritime transport, these emissions are projected to increase by 90–130% by 2050 compared to 2008 levels (Ölçer and Alamoush 2024). This trend runs counter to the Paris Agreement's goals of limiting global temperature rise (Paris Agreement 2018). IMO has taken several steps to protect the environment from carbon emissions within the maritime industry. To reduce carbon and other toxic gas emissions, IMO (2018a, b) has envisaged some initial strict regulations aimed at 2050. Recently, IMO has adopted a revised GHG reduction strategy that opens a new chapter toward maritime decarbonization (IMO , 2023). However, the maritime transportation sector is facing the challenge of reducing greenhouse gas (GHG) emissions considerably. One of the most effective strategies for reducing or eliminating emissions from ship propulsion systems is the adoption of alternative, emission-free fuels. Commonly explored options include batteries, hydrogen, liquefied natural gas (LNG), liquefied petroleum gas (LPG), methanol, solar energy, and nuclear energy. A significant review of alternative fuels for maritime transportation is presented in Al-Enazi et al. (2021).

This research investigates the application of alternative fuels in autonomous maritime operations, focusing on a case study from the SEAMLESS project involving an autonomous vessel that is planned to operate between Bergen and Ågotnes (SEAMLESS 2023a). The case study will investigate the application of a transport system like that of ASKO, as described in Hagaseth et al. (2023), where a dedicated liner service for transporting containers between two ports is operated by an autonomous ship. A structured description of the use case has been demonstrated by Sumon et al. (2024a, b). The selected use case involves a battery-powered autonomous vessel; therefore, this study concentrates solely on battery-electric propulsion systems, which offer zero operational emissions.

Among multiple battery types of applications, the most popular battery for maritime propulsion systems is the rechargeable Lithium-ion (LI) battery. This popularity is because of its high specific power (up to 2000 W/kg) and specific energy (100–250 Wh/kg) (Inal et al. 2022). An entire description of the use of battery electric propulsion, including the regulations of the IMO and classification societies for maritime propulsion, is reviewed in Alnes et al. (2017) and Andersson et al. (2017). Besides, the power system of autonomous ships is fully digitalized so that remote condition monitoring and control become possible. One of the abundant challenges for autonomous ship operations is to maintain a resilient and fault-tolerant power system that preserves the survivability of ships during worst-case failure in unpredictable maritime weather conditions.

IMO and the Republic of Korea jointly organized a symposium on May 30, 2023, intending to develop and enhance the current IMO MASS code (IMO 2021). The symposium's objective is to eventually implement a compulsory MASS code within the framework of the "Safety of Life at Sea (SOLAS)" regulations. Several studies on MASS focus on aspects such as operation, design (both technical and commercial), routing, and system requirements. These studies outline the various phases of MASS operation, including practical technical design stages, and highlight the challenges related to ensuring safe operation. For example, Andreas Lien Wennersberg et al. (2020) formulate a structure and description-based framework for autonomous ship systems and operations to develop a formalized concept of operations (ConOps); Burmeister et al. (2014) demonstrate how E-Navigation focuses on increasing the safety of navigation by better integrating ship and shore based on MUNIN's (Maritime Unmanned Navigations through Intelligence in Networks) result; Chae et al. (2020) address the technical challenges of MASS to suggest the future direction of MASS development through a literature review; Hagaseth et al. (2022) propose a methodology to formalize the Concept of Operations (CONOPS) with Unified Modeling Language (UML) for autonomous ship systems by defining the roles and activities of key actors, including the vessel, remote control center, and supporting entities, to simplify the verification and approval process; Komianos (2018) describes autonomous ships, reviews relevant projects, and examines operational, regulatory, and quality assurance challenges associated with their deployment, while highlighting their advantages over manned vessels through analysis of human-error-related accidents.

To ensure MASS's safe and reliable operation, it is required to address various challenges (Alamoush et al. 2024) through comprehensive safety assessments. These challenges typically relate to navigation, collision avoidance (CA), environmental factors, socio-technical, and cybersecurity (Jalonen et al. 2016). However, Jalonen et al. (2016) also, include that, unlike traditional ships, the responsibility for threat recognition and response is partially shifted from onboard crew members to intelligent software systems and sensor technologies, or to remote supervisors managing the vessels through data links from onshore control centers.

Ensuring safe operations necessitates that these vessels pose no threats to themselves, other ships, surrounding infrastructure, or the marine environment (Jalonen et al. 2016). Hence, several studies conducted safety analyses of MASS to identify the potential hazardous scenarios. Table 1 summarizes some of the significant studies, detailing their methods, objectives, tools, and other relevant aspects.

Most of these studies employ traditional safety analysis methods and mainly focus on how technical, mechanical, electrical, and software failures result in hazardous situations during the design and operational phases. However, in addition to component failures, accidents can be caused by design errors, component interactions, control failures, and other social and organizational factors (Leveson 2016). Furthermore, the simultaneous shift towards autonomous vessels and zero-emission or low-emission operations is likely to introduce new safety challenges. Remote or autonomous power management of these novel power systems is particularly complex, involving multiple intricate controllers whose interactions may lead to unforeseen and potentially unsafe behaviors. Safety is essential for both cases. Traditional methods may not be enough to analyze them.

The Systems-Theoretic Process Analysis (STPA) method is a recently developed method that is particularly well-suited for software-intensive complex systems and for identifying potential unsafe behaviors (Leveson and Thomas 2018). Since STPA is designed to analyze large-scale and complex systems, it is particularly suitable for Maritime Autonomous Surface Ships (MASS) (Ventikos et al. 2020). By utilizing a functional

Table 1 MASS safety analysis studies

Reference	Scope/goal	Method/tool	Findings/recommendations
(BahooToroody et al. 2022)	Evaluate the reliability of ship machinery systems to determine safe operational duration without supervision	Bayesian Belief Network (BBN) for probabilistic reliability assessment	The framework forecasts the ship performance at various autonomy levels, considering uncertainty and limited data
(Bao et al. 2022)	Assess and control risks in auto-mooring systems	Failure Mode and Effects Analysis (FMEA) with risk ranking	Model identifies high-risk failure modes and suggests targeted risk control measures
(Bolbot et al. 2022)	Propose an automated process for generating traffic scenarios to test collision avoidance (CA) systems	Demonstrates a case study that identifies hazardous scenarios and calculates risk vectors using AIS data and clustering algorithms	The process identifies traffic scenarios and serves as a substitute for AIS data, particularly in testing the CA system
(Chang et al. 2021)	Develops an approach to assess the risk levels of key hazards in MASS	Failure Modes and Effects Analysis (FMEA) combined with Evidential Reasoning (ER) and a Rule-based Bayesian Network (RBN)	Interaction with manned vessels and object detection pose the highest risks, followed by cyber-attacks, human error, and equipment failure
(Fan et al. 2020)	Examines four operational phases to identify navigational risk influence factors (RIFs)	Examines 4 phases and 4 factors (4P4F) Framework and applies expert panel evaluations to compare their influence	A total of 55 RIFs is identified, where open sea navigation is the phase with the highest number of RIFs
(Li et al. 2023)	Identifies potential operational risks of MASS and examines its intertwined causal relationships	The single-risk and multiple-risk identification are realized via network modeling	Findings provide insight into the structure of operational risks, offering practical guidance for effective risk management and the safe operation of MASS
(Jensen 2015)	Establish a risk picture for the autonomous operation of an unmanned vessel	Fault tree analysis (FTA) and event tree analysis (ETA)	Unmanned vessel operation of the use case is as safe as a conventional vessel under ideal ship-shore conditions
(Burmeister et al. 2014)	Build on the Use case of the MUNIN project to identify risks and simplify operational risks	Risk-based design method, based on the Formal Safety Analysis method (FSA)	The risk-based method structures hazard identification, facilitating the recognition of key challenges and guiding development
(Bolbot et al. 2021)	Develops a novel hybrid, semi-structured process for identifying and ranking hazardous scenarios	A hybrid operational functional approach with Hazard Identification (HAZID) method	The most critical hazards related to safety, security, and cybersecurity are associated with situational awareness, remote control, and propulsion systems, and improvements at the design stage are suggested

model of the system, STPA is more effective than other hazard analysis methods, such as fault tree analysis (FTA), failure modes and effects criticality analysis (FMECA), and hazard and operability analysis (HAZOP), in identifying potential hazards across various levels of autonomy (Ventikos et al. 2020). Yuzui and Kaneko (2025) recently conducted a systematic review following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to identify more effective risk analysis methods for MASS. Their study suggests that qualitative analysis using STAMP/STPA and quantitative analysis through BN based on the STAMP/STPA results are effective for MASS safety analysis. Chaal et al. (2020) analyzed unsafe interactions between system components of the onboard ship controllers and provided recommendations to prevent hazards resulting from unsafe control actions. Solberg (2018) conducted a hazard analysis using STPA on the ReVolt autonomous ship prototype, developed a specialized control structure, and recommended improvements to the model. (Wróbel et al. 2018) carried out an initial STPA hazard analysis of autonomous merchant vessels using a specified safety control structure. The authors noted that this control structure, which represented a simplified model of the vessel's operation system, significantly contributed to the analysis of uncertainties. In addition, the evaluation of the effectiveness of the STAMP/STPA in risk analysis of autonomous ship systems in the early design stage is studied by Yamada et al. (2022), who suggested the improvement of the control structure and extracted the functional requirements for the hypothetical autonomous ship. Hüllein et al. (2024) use STPA for the hazard identification and comparison of two alternative hybrid power and propulsion systems for a small-scale fishing vessel. They conclude that automated control systems and user interaction with the system require special attention. Rokseth et al. (2017) also perform risk analysis with STPA on maritime dynamic positioning (DP) systems, and their result suggest that the system safety constraints of DP can be violated in multiple ways other than component failure.

MASS is operated by various controllers from shore and onboard. Failures of the controllers and their wrong execution can be hazardous. Several studies discuss the operational procedure and functionalities of these controllers during the design and construction phases (ABS 2020; Alnes et al. 2017; DNV 2021; Hagaseth et al. 2023; Karkosiński et al. 2021; Lucà Trombetta et al. 2024). Meanwhile, hazard-related studies of onboard battery-powered systems tend to focus on individual controller functionalities during the manufacturing phase (Andersson et al. 2017; Baird et al. 2020; Johansen et al. 2007; Xie et al. 2007; Yanchin and Petrov 2020). However, studies considering all controllers together, especially from a hazard analysis perspective, are limited. Particularly, in complex, large-scale systems, accidents such as collisions, groundings, and sinkings can arise not only from the failure of individual components or subsystems, but also from hazardous interactions between them (Yamada et al. 2022). Additionally, there are limited studies that have identified the hazards associated with the combination of autonomous ships and battery propulsion.

In this study, we perform a hazard analysis using the STPA method on specific controllers of battery-driven autonomous ships. The novelty of this research is the application of the STPA method to a battery-powered autonomous ship, with a specific focus on the power supply system under the constrained autonomy level. This work integrates and analyses the interactions among multiple onboard and remote controllers, such as the Remote Operations Center (ROC), Power Management System (PMS), Battery Management System (BMS), and Ship Management and Control (SMC), to identify potential hazardous scenarios that extend beyond prior works, which often concentrate on navigational hazard analysis. Moreover, the novelty also lies in extending the STPA method to prioritize the sensitivity of hazards.

This study aims to identify the most safety–critical control actions associated with individual controllers based on their hazardous impacts, thereby informing the level of attention required for each controller. The key contributions include: (1) specifying system-level hazards and safety constraints, (2) the development of a detailed control structure for a battery-powered autonomous ship with an emphasis on the power system, and (3) the identification of associated Unsafe Control Actions (UCAs) and potential loss scenarios.

Furthermore, the Norwegian Maritime Authority (NMA 2022) stipulates that to obtain regulatory approval and establish the reliability of Maritime Autonomous Surface Ships (MASS), it must be demonstrated that their safety performance is at least equivalent to, or greater than, that of conventional vessels. In this context, hazard analysis using a structured and systematic methodology can play a key role in streamlining the approval process while ensuring compliance with required safety standards. The method adopted in this study contributes to this objective by supporting a risk-based framework for evaluating and approving autonomous ships. Moreover, the application of the Systems-Theoretic Process Analysis (STPA) method will gain traction among industry practitioners, further underscoring its practical value for comprehensive hazard identification and analysis in autonomous maritime operations.

The next sections of this study are as follows: Sect. 2 describes the materials and methodology where the hazard analysis method including the autonomy levels of MASS, system-level description, and responsibilities of the controllers of this study is presented, Sect. 3 presents the result that is obtained from the hazard analysis, Sects. 4 and 5 demonstrate the discussion including the limitations and conclusion.

Materials and method

Autonomy levels

Autonomy level is a significant aspect in determining the autonomous functionalities of MASS. Different taxonomies have classified autonomy levels based on the allocation of tasks between humans and the system (Camila Correa-Jullian 2023).

In this paper, we have adopted the four degrees of autonomy levels described in the report (Nordahl and Wennersberg 2024) and the levels are updated in the report from (Nordahl et al. 2023; Rødseth et al. 2022). These are given as follows:

- **Direct Control (DC):** The operator fully controls the system using levels and push buttons, aided by basic automation and decision support. This is the standard automation mode on conventional ships today
- **Automatic Operations (AO):** The automation system performs the operations under continuous supervision by an operator. Examples are auto-docking, auto-tracking, and dynamic positioning. While the automation performs the operation, it is the operator who makes decisions such as when to activate a function or system, what

option to choose from proposals generated by decision support, providing setpoints, routes, or motion trajectories (e.g., for a crane), or deviating from a plan.

- **Constrained Autonomous (CA):** The automation performs the operations without continuous supervision of a human operator. Decision making is automated such that function and system activation, setpoints and commands to controllers are done by the automation. However, there are clearly defined conditions specifying the decision-making capability of the automation (e.g., visibility, environmental conditions, or system status), which must be satisfied. If conditions are not satisfied, the decision-making shall be handed over to the ROC operator. Furthermore, the ROC operator creates and uploads a digital mission defining the voyage, cargo operations, and schedule, as well as the conditions and limitations for automated decision-making. Legal responsibility, i.e., the role of the master, remains with the ROC operator.
- **Fully autonomous (FA):** The ship's operating system can make decisions and determine actions independently.

Controllers and their responsibilities

Onboard and Remote Operation Centre (ROC) controllers are significant to the safe operation of autonomous vessels, with their roles often necessitating close interaction and coordination to ensure both operational efficiency and safety. In the context of this study, the system includes the following four controllers:

1. Remote Operation Center (ROC)
2. Ship Motion Controller (SMC)
3. Battery Management System (BMS)
4. Power Management System (PMS)

ROC

The remote operation center is a shore-based control station that is controlled by the human operator/s and holds the role of master, navigator, or engineer/s from the shore. The main task of ROC is to upload the vessel's mission (voyage plan, navigation, cargo handling, docking, etc.). ROC monitors all the autonomous operations from the shore, receives feedback or information from the Autonomous Onboard Controller (AOC), and updates the voyage plan when necessary. The Remote Operation Centre (ROC) also maintains communication with other ROCs, conventional vessels, and the Vessel Traffic Service (VTS), managing the exchange of information and operational directives. Additionally, the ROC is responsible for handling exceptional situations. For instance, when the Autonomous Onboard Controller (AOC) detects that one or more parameters exceed predefined thresholds, it issues an alert, such as an alarm or signal to the ROC, prompting it to initiate high-attention monitoring mode. ROC updates any action or voyage plan to the AOC if required. Based on the situation, it may initiate the fallback strategy. However, when AOC initiates a fallback, ROC responds to the fallback recovery. A structured description of ROC is presented in Dybvik et al. (2020) and Hagaseth et al.

(2022). A case study of a remotely operated vehicle (ROV) with four operational modes with different LoAs is used to illustrate in Yang et al. (2020). The results show that the proposed approach helps clarify how responsibilities shift between the human operator and the system controller in different operational modes. It explains how responsibility is shared and what changes are needed in the operator's and controller's understanding to ensure a smooth transition.

SMC

The ship motion controller controls the ship's course and speed as per the voyage plan (Wang et al. 2023). For this use case, SMC is regulated by the onboard autonomous controller, and the human operator takes control in case of exceptional circumstances.

BMS

Multiple parts are integrated to form the battery system (BS). These are battery cells (consisting of anode, cathode, separator, electrolyte), mechanical structure and protective box(es), thermal management system, electric connections, and the control and management system, typically called the Battery Management System (BMS) (Chin et al. 2019). The BMS plays a critical role in ensuring the safe and reliable operation of the battery system. Its key functions include estimating the state of charge (SOC) and state of health (SOH), controlling thermal behavior to prevent overheating, enabling or disabling the battery connection, and protecting the battery from potentially damaging operating conditions (Chin et al. 2019).

PMS

A power management system (PMS) functions as a centralized controller for the shipboard power system and commands the local controller (Reddy et al. 2023). The PMS is designed with anything from simple to advanced intelligent algorithms based on artificial intelligence (Xie et al. 2022). The main objective of the PMS is to ensure that a sufficient and balanced power supply is continuously available, i.e., blackout prevention. This means that "no single-point failure in the power plant will have consequences beyond the worst-case single-point failure chosen by design, which may typically be a short circuit in a main switchboard when operating in a two-split configuration, leading to loss of half of the power generation capacity, and half of the thruster capacity" (Johansen et al. 2007). Within the scope of this study, Fig. 1 highlights the key responsibilities assigned to each controller.

System description: In our study, autonomous refers to the autonomy level Constrained Autonomous (see Sect. 2.1) for our use case. The use case vessel operation is more like the constrained autonomous where no seafarer is onboard. AOC performs the autonomous operation based on the predefined vessel mission (defining the voyage plan, cargo operations, and schedule) that is uploaded digitally from the ROC. Figure 2 illustrates the shore-side and ship-side controllers' interaction. Initially, the ROC initiates the vessel voyage plan (navigational route, time, speed set points, etc.) and monitors the operation. AOC executes the mission by setting the Onboard Systems in the correct mode, providing the setpoints and commands to initiate, abort or complete the execution of an assigned task by the onboard control systems (such as automation and power

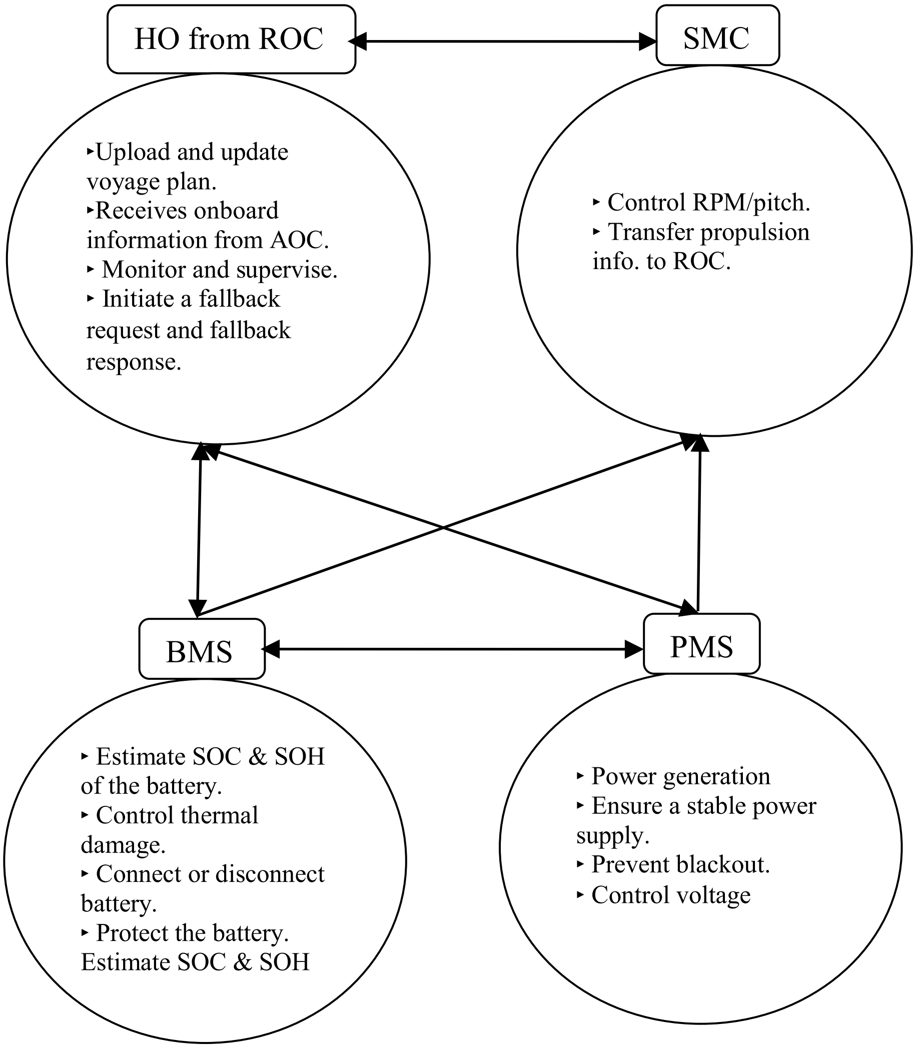

HO from ROC
SMC
‣Upload and update voyage plan.
‣Receives onboard information from AOC.
‣ Monitor and supervise.
‣ Initiate a fallback request and fallback response.
‣ Control RPM/pitch.
‣ Transfer propulsion info. to ROC.
BMS
PMS
‣ Estimate SOC & SOH of the battery.
‣ Control thermal damage.
‣ Connect or disconnect battery.
‣ Protect the battery. Estimate SOC & SOH
‣ Power generation
‣ Ensure a stable power supply.
‣ Prevent blackout.
‣ Control voltage

Fig. 1 Key responsibilities of the individual controllers (Geertsma et al. 2017; Hagaseth et al. 2022; Lucà Trombetta et al. 2024; Nordahl and Wennersberg 2024; Wang et al. 2023)

management systems, navigation and manoeuvring systems, situational awareness systems, safety functions, and communication interfaces). In short, it automates the execution of the vessel's mission. AOC manages the operation such that HO does not need constant supervision. Besides, during different phases of the voyage, the AOC needs confirmation from the ROC for certain transitions, such as between sailing to docking. AOC maintains communication with ROC and also shares navigational information with VTS, other Vessels/s, and ROC. It exchanges data and shares abstracted information between the HO of ROC and the onboard control systems. We consider PMS, BMS, and SMC to be the onboard controllers within the scope of this study.

BMS controls all the functions of the battery system and sends the performance information to AOC via PMS. PMS manages the shipboard power system by automatically operating the main switchboard and updating the information to AOC and SMC. Johansen et al. (2023) mention that Power management systems (PMS) also have a high degree of automation to control electric power generation, power distribution, and blackout prevention on

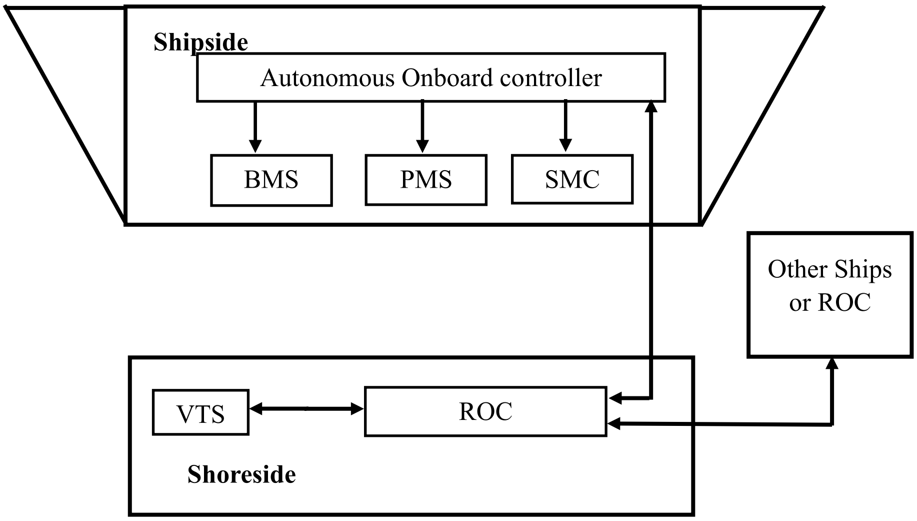


Fig. 2 System illustration of the interaction between shipside and shoreside. Inspired from (Hagaseth et al. 2022)

ships. SMC regulates RPM (Rotation Per Minute) to control the thruster based on speed as well as heading set points. SMC gathers feedback from GPS and sends it to AOC. However, there are specific defined conditions for the decision-making capabilities of the AOC within the system status of the onboard controllers, visibility, and environmental conditions. When one or more conditions cross the predefined thresholds, the AOC notifies the ROC and/or can initiate fallbacks automatically (such as when the communication link is missing for a certain amount of time). Anchoring, DP, and vessel drifting are the common means of a fallback state. Later, ROC responds to the fallback recovery of the vessel. The Remote Operation Centre (ROC) continuously monitors the operational status and data of the autonomous systems while also maintaining communication with the Vessel Traffic Service (VTS) and nearby vessels. A key responsibility of the ROC is managing exceptional scenarios. For example, when the Autonomous Onboard Controller (AOC) identifies that certain parameters have exceeded predefined thresholds, it alerts the ROC, typically via alarms or other signaling mechanisms, and requests elevated monitoring. In response, the ROC may update the voyage plan or issue operational commands to the AOC as needed. Depending on the nature of the situation, the ROC can also initiate a predefined fallback mode to ensure safety.

STPA

When performing hazard analysis for autonomous ships, it is important to broaden the focus beyond just equipment failures and also to include software and human factors (Yamada et al. 2022). This study intends to identify and understand the hazards that may arise from inadequate control and unsafe interactions among the controllers from the remote operation center and onboard the ship during autonomous ship operations. System Theoretic Process Analysis (STPA) is a hazard analysis method that is based on Systems-Theoretic Accident Modeling and Processes (STAMP), which is an accident model focusing on potential causes of accidents beyond component failures (Leveson 2016). This STPA method is applied based on a hierarchical control structure of the system, where the relationship and interactions between controllers (such as human and electronic controllers) and controlled processes are modeled through control actions and feedback signals. Leveson (2016) presents that even with limited information and empirical data, STPA can be utilized for hazard analysis. In STAMP (and STPA), the fundamental premise is that accidents result from insufficient and unsafe control (Leveson 2016). STPA aims to determine how unsafe control actions might arise within the hierarchical control structure and how they can be avoided (Leveson and Thomas 2018). STPA has been applied in the autonomous operation of different industries for the identification of unsafe control actions such as Johansen et al. (2023) and Thieme et al. (2021) in the maritime industry, Castilho et al. (2018) in the aviation industry, Rejzek and Hilbes (2018) in nuclear power plants, Oginni et al. (2023) in the railway project.

Recently, the method has attracted attention in the safety assessment of autonomous ships. Sumon et al. (2024a, b) performed the STPA on different control actions (emergency shutdown and speed change) of hydrogen-driven autonomous vessels and determined 44 unsafe control actions. Johansen and Utne (2022) approached a risk model represented by a Bayesian Belief Network (BBN), which is based on a systems theoretic process analysis (STPA), to assess navigational risks for an autonomous cargo ship while sailing as part of a supervisory risk controller (SRC) for high-level control of the ship. Further, during the interaction between the Supervisory Risk Controller and Human Supervisors from ROC (Johansen et al. 2023), along with 12 experts from specific system-level experts conducted STPA and identified a total of 60 unsafe control actions.

Bolbot et al. (2019) applied STPA on Service Operation Vessels to control the hazardous scenarios of a power system. Their study identifies hazardous scenarios based on unsafe control actions in direct current (DC) and direct current battery power systems. They show that battery power DC creates more hazardous scenarios compared to conventional DC.

However, the main idea in the accident causation model is that safety is a control problem, following the ideas presented by Rasmussen (1997) and that accidents happen due to insufficient control and enforcement of safety constraints within a hierarchical control structure, where each layer influences the next. The goal of STPA is to identify potential areas of inadequate control, understand how it might occur, and impose constraints to prevent it (Rokseth et al. 2018).

STPA analysis approach

The STPA method can be applied in four steps. This hereby study includes an extended step to obtain the intended research result. A short description of the steps following the STPA handbook (Leveson and Thomas 2018) is presented in the following Fig. 3:

Step 1: Define the purpose of the analysis

The first step defines the purpose of the analysis as per the whole system. Based on the system-level description, it identifies losses, system-level hazards, and system-level constraints, and refining hazards is an optional part of it.

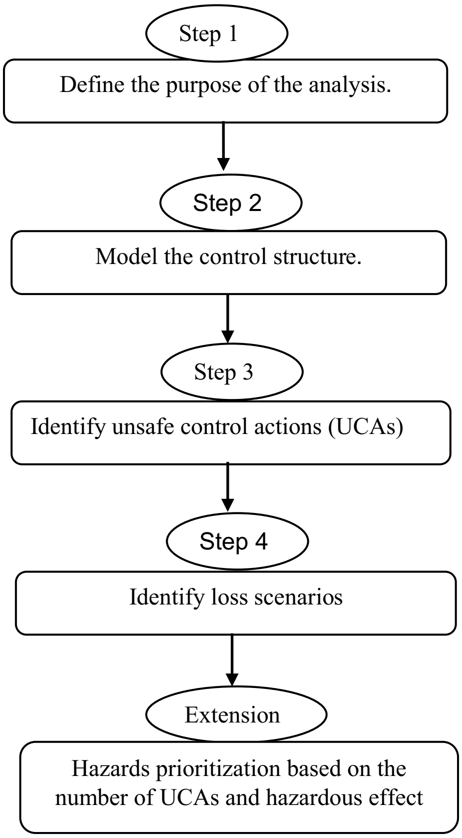

Step 1
Define the purpose of the analysis.
Step 2
Model the control structure.
Step 3
Identify unsafe control actions (UCAs)
Step 4
Identify loss scenarios
Extension
Hazards prioritization based on the number of UCAs and hazardous effect

Fig. 3 Flowchart of the analysis method

Step 2: Model the control structure

In this step, functional relationships and interactions are captured by modeling the system as a set of feedback control loops. A hierarchical control structure is a system model that is composed of feedback control loops. This is an illustration where controllers and actuators are shown to execute the control actions and feedback as a response to the controllers.

Step 3: Identify unsafe control actions

This step identifies the control actions that are unsafe and lead to system-level hazards. Leverson and Thomas (2018) define an unsafe control action as "a control action that, in a particular context and worst-case environment, will lead to a hazard".

Step 4: Identify loss scenarios

A loss scenario represents the specific reasons that lead to unsafe control actions and hazards (Leveson 2016). Two types of loss scenarios are considered.

1) Reasons for the occurrence of unsafe control actions.
2) The reasons for not executing control actions that prevent hazards and wrong execution of control actions that lead to hazards.

Hazard prioritization

Following the application of STPA within the defined scope of this study, a hazard ranking framework is established to assess the impact of both individual and interacting hazards identified through the analysis. The hazards are categorized into three distinct groups, which are mild, moderate, and critical, based on their potential consequences. Subsequently, the Unsafe Control Actions (UCAs) are classified according to these severity levels, enabling a prioritized assessment of control actions. This classification informs the operational attention required, distinguishing whether specific control actions should be monitored under high- or low-attention modes during vessel operation.

Execution of the study

This study was conducted as part of the SEAMLESS project (SEAMLESS 2023b), which brings together a diverse consortium of academic institutions and industrial partners across the maritime domain. The analysis focused on a specific use case developed collaboratively with a selected group of domain experts representing various stakeholder perspectives, including operations, regulation, and system engineering for maritime autonomy. Participants included individuals with between 10 and 30 years of experience in maritime systems engineering and research on autonomous systems design.

The analysis of the study was carried out over four months in 2024, involving a series of structured online workshops (each lasting approximately 1–1.5 h), along with follow-up desktop discussions and asynchronous reviews of documentation. The sessions utilized a semi-structured format grounded in the STPA methodology.

Initially, a high-level control structure diagram was developed by the authors and shared with participants for feedback. This diagram, outlining the responsibilities and control actions of key system controllers, was iteratively refined based on input received during collaborative sessions. Each workshop focused on a specific aspect of the analysis:

- **Workshop 1**: Review the system boundaries and control structure
- **Workshop 2**: Refinement and modification of the control structure diagram based on the experts' feedback.
- **Workshop 3**: Hazard identification and unsafe control actions.
- **Workshop 4**: Causal scenario development.

In subsequent follow-up meetings, we refined the preliminary findings and results. Although the sessions were not formal interviews, we systematically logged participant contributions and synthesized them into the analysis. While we cannot provide detailed descriptions or affiliations of participants due to confidentiality agreements and the small number of individuals involved, the iterative development and review of the control structure diagram and analysis were informed by this diverse and experienced group. We believe that this contextual information offers the reader insight into the validity of the process, even without disclosing identities. Table 2 provides the periodic structure of the progressive study process and interactions.

Table 2 Progressive study process and interactions

Activity/time	Academic researchers (maritime autonomy and safety analysts)	Industry experts (maritime autonomy practitioners)
Month 1 (Initial diagram)	Drafted control structure diagram	Feedback, review, and comments
Month 2 (Diagram modification)	Review the system boundaries and control structure diagram	Boundary input
Month 3 (Diagram validation)	Update the control structure diagram and responsibilities of the controllers	Feedback, comments, and validation
Month 3–4 (Hazardous scenarios identification)	Identifying unsafe control actions	–
Month 4 (Result review)	Prioritize the individual and combine hazards. Identifying loss scenarios	Review and comments

Table 3 Identified losses

L1: Loss of lives
L2: Not able to deliver the cargo
L3: Time delay
L4: Loss of property
L5: Damage infrastructure
L6: Distract marine traffic
L7: Damage to the environment
L8: Financial loss

Result

A four-step STPA analysis was carried out to identify Unsafe Control Actions (UCAs) resulting from interactions among the controllers during autonomous operation. The results of each step are detailed in this section.

Step 1: Eight specific losses are identified and presented in Table 3. Table 4 shows system-level hazards and safety constraints related to the specified losses.

Step 2: Modeled control structure

To illustrate the interaction between the specified controllers, a control structure diagram has been formulated in Fig. 4, where the control actions within the loop of command and feedback have been structured. The responsibilities of the controllers are already mentioned. Initially, the interaction starts between human operator/s from ROC and onboard controllers, which are directed via the autonomous onboard controller (AOC) (also known as Digital Orchestrator). Solid lines in the figure indicate the command action, while dotted lines indicate the response as feedback corresponding to the command action. The first command comes from the ROC to the AOC. ROC uploads and updates the voyage plan to AOC. Speed and heading setpoints are instructed then to SMC via AOC. Later, SMC executes those commands by follow-up commands of RPM and angle change to the thrusters. After execution, AOC receives the speed and location feedback from the vessel's GPS and shares it with ROC.

BMS has two sub-elements which are battery cooling and battery and are linked to the main switchboard. The sub-elements execute the command of BMS through the switchboard. Increasing or decreasing the battery temperature is executed by the former sub-elements whereas the latter one executes the battery connection or disconnection based

Table 4 Identification of system-level hazards and system-level constraints

System-level hazards	System-level constraints
H1: The battery cell/s or battery system becomes extremely hot or has uncontrolled heating on the battery cell/s or system. (L2,3,4,6,8)	**SC1:** The battery cell/s or battery system should maintain a safe temperature to provide optimal power
H2: The entire power supply of the vessel is interrupted or lost. (L3,4,8)	**SC2:** The vessel must have a continuous optimal power supply to prevent interruption or restore vessel power
H3: The vessel approaches too close to another vessel, or another vessel/s is approached too close to the vessel. (L1,2,3,4,5,6,7,8)	**SC3:** The vessel must maintain a safe distance from another vessel to avoid collision
H4: The vessel approaches too close to the seabed, an underwater obstruction, or a shore. (L2,3,4,6,8)	**SC4:** The vessel must maintain a safe distance from the seabed and avoid underwater obstruction or a shore
H5: The vessel approaches too close to any obstacle or infrastructure. (L1,2,3,4,5,6,7,8)	**SC5:** The vessel must not approach too close to an obstacle or infrastructure and should maintain a safe distance
H6: Optimal power supply is not provided to the vessel. (L3,4,5,8)	**SC6:** The vessel must get an optimal power supply for safe propulsion and operation of the auxiliary power-oriented mechanisms
H7: Excessive power supply is provided to the vessel. (L3,7,8)	**SC7:** Excessive power supply should be restricted to avoid overload

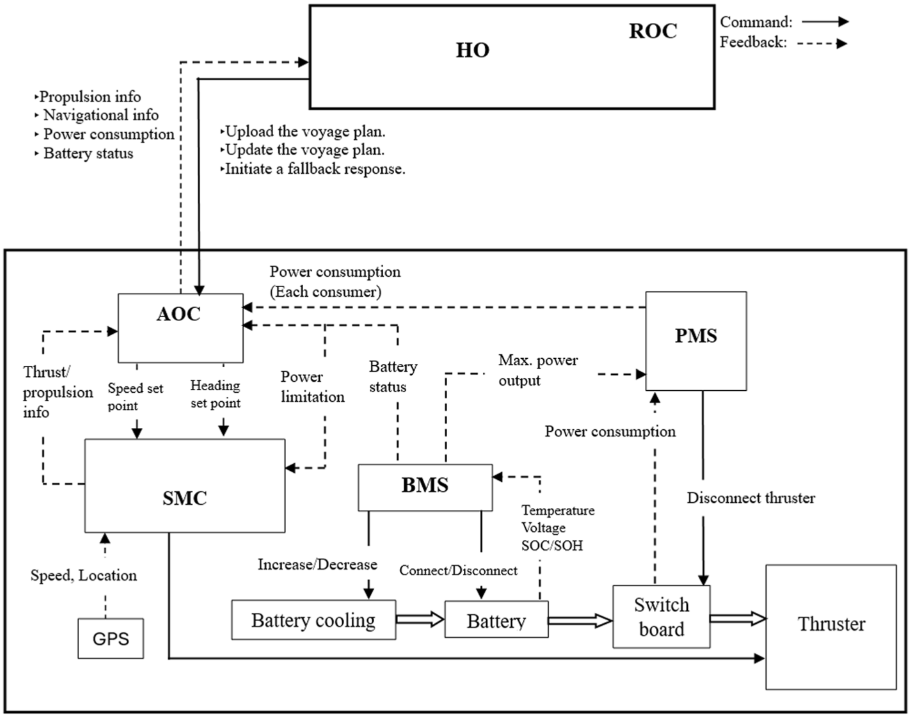


Fig. 4 Control structure diagram of the controllers

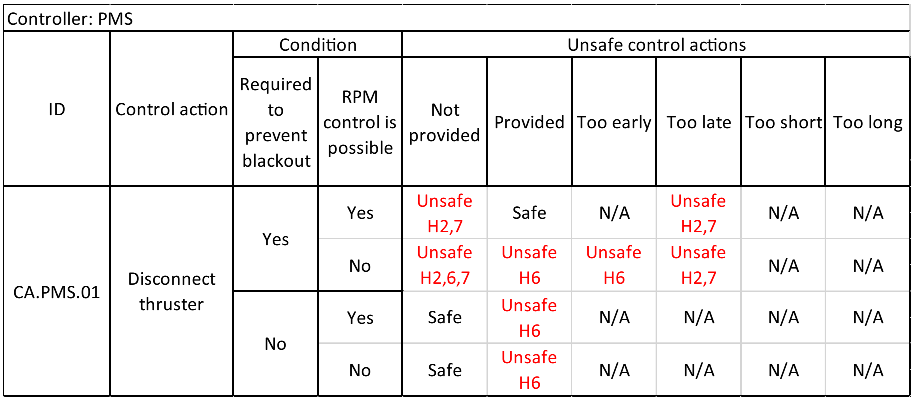
on the power consumption. The battery section sends the physical feedback (i.e., voltage, temperature, level of charge) to the BMS. BMS then transfers the SOC and SOH condition of the active and inactive battery cells to the PMS and AOC.

PMS commands the main switchboard when only thruster disconnection is required and commands the thruster to limit its power depending on the load and

Table 5 Controllers with their control actions during autonomous operation

Controllers	Control actions
Ship motion controller	1)Increase RPM 2) Decrease RPM
Human operator	1)Initiate fallback 2) Initiate a fallback response
Power management system	1)Disconnect thruster 2) Limit power to the thrust
Battery management system	1)Cooling control 2) Connect battery 3) Disconnect battery

Table 6 Example of unsafe control action analysis table



Controller: PMS									
ID	Control action	Condition		Unsafe control actions					
		Required to prevent blackout	RPM control is possible	Not provided	Provided	Too early	Too late	Too short	Too long
CA.PMS.01	Disconnect thruster	Yes	Yes	Unsafe H2,7	Safe	N/A	Unsafe H2,7	N/A	N/A
			No	Unsafe H2,6,7	Unsafe H6	Unsafe H6	Unsafe H2,7	N/A	N/A
		No	Yes	Safe	Unsafe H6	N/A	N/A	N/A	N/A
			No	Safe	Unsafe H6	N/A	N/A	N/A	N/A

consumption. PMS updates the power limitation to the SMC and the power consumption of each consumer (propulsion and onboard auxiliary power consumption) to the AOC. Both BMS and PMS are onboard automatic controllers whose functions are pre-determined. Any exception is notified to the AOC which measures the vessel's safety based on the pre-defined conditions. If the situation demands, AOC initiates a fallback state and also notifies ROC via an audio-visual signal or alarm system. In case of any criticality of AOC, it may request to ROC to initiate a fallback state. Generally, ROC initiates a fallback response and may also initiate a pre-defined fallback state when AOC fails to initiate or fails to realize the criticality of a situation.

Step 3: Identifying unsafe control actions (UCAs)

This step identifies the unsafe control actions when the controllers (HO, SMC, PMS, BMS) interact with one another and execute their control actions. Control actions of these four controllers are presented in the following Table 5:

The execution or non-execution of these control actions during inappropriate times and situations can lead to unsafe outcomes. UCAs are identified systematically under various conditions. Table 6 provides an example of how UCAs are determined when the PMS executes the 'Disconnect Thruster' action under different scenarios.

This study identifies a total of 127 UCAs while executing these 9 control actions by the four controllers from shore and onboard. The number of UCAs from the control actions of SMC, HO, PMS, and BMS are presented in the following Tables 7, 8, 9, 10, and 11. The tables present the number of UCAs of the individual controller. After that, the UCAs are structured as like as the following examples:

"UCA: PMS: 01:001: PMS does not provide the "disconnect thruster" command

Table 7 Number of UCAs from the SMC controller

Number of UCAs from SMC		
Control action	**Conditions**	**No. of UCAs**
Increase RPM (for safe voyage)	Required to prevent collision Increasing power is available or not	9
Increase RPM (optimal voyage)	Required for the optimal voyage Feasible to increase RPM or not Increasing power is available or not	15
Decrease RPM (for safe voyage)	Required to prevent collision	6
Decrease RPM (for optimal voyage)	Required for the optimal voyage Feasible to decrease RPM or not	9
Total		39

Table 8 Number of UCAs from the HO controller

Number of UCAs from HO		
Control action	**Conditions**	**No. of UCAs**
Initiate fallback	AOC loses the object detection or measurement ability Required to maintain vessel safety	9
Response to a fallback recovery	Fallback is initiated Required to continue the regular operation	7
Total		16

Table 9 Number of UCAs from PMS controller

Number of UCAs from PMS		
Control action	**Conditions**	**No. of UCAs**
Disconnect thruster (1)	Required to prevent blackout or not RPM control is possible or not	8
Disconnect thruster (2)	Thrusters violate power limitations from PMS Required to prevent fire or not	10
Limit power to thrust	Required to maintain ship stability Required to maintain ship restriction at the port Required to prevent blackout or not	25
Total		43

Table 10 Number of UCAs from the BMS controller

Number of UCAs from BMS		
Control action	**Conditions**	**No. of UCAs**
Cooling control	Required to prevent battery damage Required to prevent blackout or not	9
Connect battery	Required to maintain power supply Required to prevent blackout or not	11
Disconnect battery	Required to prevent fuel consumption Required to prevent uncontrolled heating or fire	9
Total		29

Table 11 Total number and percentage of UCAs from the controllers

Controllers	Total number of UCAs from the controllers	Percentage of UCAs from the controllers
SMC	39	31%
HO	16	12%
PMS	43	34%
BMS	29	23%
Total	127	

Table 12 Number of loss scenarios from the individual controllers and control actions

Controllers	Control actions	No. of loss scenarios from the control actions	Total no. of loss scenarios from the controllers
SMC	Increase RPM for a safe voyage	30	126
	Increase RPM for the optimal voyage	47	
	Decrease RPM for a safe voyage	21	
	Decrease RPM for the optimal voyage	28	
HO	Initiate fallback	39	59
	Response to a fallback recovery	20	
PMS	Disconnect thruster (1)	26	157
	Disconnect thruster (2)	37	
	Limit power to thrust	94	
BMS	Cooling control	35	115
	Connect battery	43	
	Disconnect battery	37	
Total			457

> *to prevent the entire power loss of the vessel when rotation per minute or RPM control is possible. (H2,7)"*
> *"UCA: PMS: 01:004: PMS provides the "disconnect thruster" command to prevent the entire power loss of the vessel, but RPM control is not possible. (H6)"*

The above UCAs are structured from the example table of UCA analysis that identifies the execution of the "Disconnect thruster" by the PMS controller.

Step 4: Loss scenarios

This section identifies the reasons for unsafe control actions (UCAs). Multiple reasons can exist for a single UCA. In this current analysis, we have identified 457 loss scenarios that may lead to these 127 UCAs. In the following Table 12, the number of loss scenarios of the individual controllers from their assigned control actions is presented.

Each loss scenarios are then documented with respect to lingual expressions that include individual ID numbers. Table 13 presents examples of loss scenarios from each controller.

Table 13 Examples of the loss scenarios from the controllers

Controllers	Loss scenarios
SMC	**LS.SMC.01.001.002:** SMC needs to increase RPM to prevent collision and increasing power is available, but the control action command is not provided. This can happen because of sensor failure and SMC does not get the feedback and cannot execute the action. As a result, the vessel may collide with nearby vessel/s and/ or objects. (H3,4,5)
HO	**UCA.HO.01.001:** HO needs to initiate a pre-defined fallback to maintain the vessel's safety when the vessel loses object detection or measurement ability and AOC does not realize it, but the fallback is not initiated. (H2,3,4,5)
PMS	**LS.PMS.02.003.001:** PMS provides the "disconnect thruster" command for too short a time when thrusters violate power limitations from PMS and to prevent fire on the thruster of the vessel. This happens when the controlled process responds for a short time. As a result, excessive power supply, and uncontrolled heating on the battery or electrical system may occur. (H1,7)
BMS	**LS.BMS.02.001.001:** BMS needs to connect the battery (additional) to maintain optimal power supply and prevent blackout, but the connect battery command is not provided because of the power failure. As a result, an entire power loss of the vessel and/or a non-optimal power supply may occur. (H2,6)

Discussion

This study identifies the hazards that arise during the interaction between the ROC and onboard controllers. The tables and the figures in the result section present the numbers, percentages, and the systematic way of finding the UCAs and potential loss scenarios associated with the predefined controllers during both autonomous and remote operations. Initially, potential hazards and their corresponding safety constraints are identified based on the functional and operational context. Subsequently, Unsafe Control Actions (UCAs) that can lead to these hazards are systematically analyzed, followed by the reasons. Each UCA exhibits either individual or combined hazards, which are then categorized into three distinct groups according to the severity of their potential consequences (i.e., mild, moderate, and critical). Next, UCAs are classified based on the group of their hazards. This classification provides a structured basis for prioritizing control actions and assessing the safety implications of each controller.

Hazardous group from the UCAs

The number of UCAs indicates which controllers and their actions pose a specific number of UCAs, both individually and collectively. Consequently, the effects of UCAs are also considered, as not every UCA creates the same level of severity. Some UCAs cause a single hazard, while others may lead to multiple hazards. Furthermore, certain hazards typically result in the worst possible consequences, while others lead to the least or moderate consequences. To begin with, the hazards mentioned in Sect. 3 are categorized in Table 14 based on their effects.

Both the individual and combined hazards that emerge during the STPA analysis are classified as mild, moderate, or critical. These classifications are derived based on the potential impact of each hazard on system safety and performance. The hazards with non-critical consequences are classified as the "**mild**" group. For example, H2 is under this group, and it is the power interruption or power loss of the vessel. Power interruption or loss is less critical because there is instant backup with a redundant power supply system. Hazards (or combinations thereof) that may cause both environmental and

Table 14 Severity of the individual or combined hazards for the study

	Severity		
	Mild	**Moderate**	**Critical**
Hazards	H2	H1	H3
	H6	H4	H5
	H7	H(1,2,3)	H(3,5)
	H(1,2)	H(1,2,6)	H(2,3,5)
	H(1,6)	H(1,2,7)	H(3,4,5)
	H(1,7)	H(3,7)	H(3,5,6)
	H(2,6)	H(2,3,7)	H(3,5,7)
	H(2,7)		H(2,3,4,5)
	H(6,7)		H(2,3,5,6)
	H(2,6,7)		H(2,3,5,7)
			H(3,4,5,6)
			H(2,3,4,5,7)
			H(2,3,4,5,6,7)

financial loss are classified as "**moderate**" (It can be critical when it causes huge financial and environmental loss). For instance, H1 is in this category, which causes overheating of the battery. Battery heating is notified and monitored continuously, and a standard heating level is fixed, beyond which battery function will stop, and a new battery will be activated automatically. It usually causes financial loss. However, if the standard temperature level is not maintained for some reasons, such as sensor failure; this hazard can be critical. Finally, hazards (or combinations of hazards) that have fatal consequences are designated to the "**critical**" group. For example, H3 can cause a collision of vessels, and the result can be a physical, financial, and environmental loss. Based on the information, level of effect, and frequency of the control action execution, the autonomous operation needs "High operator attention mode" and "Low operator attention mode" from the ROC (Nordahl and Wennersberg 2024). Based on the analysis, the hazard assessment of the individual controller has been discussed.

Hazard assessment of the SMC controller

Under normal operating conditions, the Ship Motion Controller (SMC) is managed by the Autonomous Onboard Controller (AOC), whereas in specific exceptional scenarios, control is transferred to the Human Operator (HO). Upon receiving a command, the SMC executes one of two control actions: "Increase RPM" or "Decrease RPM". Four context variables are considered relevant when considering if it is safe for the SMC to execute "Increase RPM". These are "Whether an increase in RPM is required to prevent a collision, whether additional power is available for the thrusters or not, whether an increase in RPM is required for the optimal voyage (e.g. it is necessary to increase the speed of the vessel to prevent falling behind schedule), and whether it is feasible to increase RPM" Furthermore, the following three conditions decide whether it is safe for SMC to execute Decrease RPM: "Whether a decrease in RPM is required to prevent a collision, whether a decrease in RPM is required for an optimal voyage and feasible to decrease RPM". While executing "Increase RPM" control action SMC can create a total of 24 UCAs out of a total 39 UCAs based on unsafe conditions and control action failures and the remaining 15 UCAs may arise during “Decrease RPM” control action. The former control action mostly leads to the hazards H3,4,5,6,7 while the latter one mostly leads to the same hazards except H7. Given that the combined occurrence of hazards H3, H4, and H5 may come up a total of 14 times in different conditions and are considered in the critical group, this controller needs much attention.

Hazard assessment of the HO controller from ROC

Based on the previous discussion, it is evident that the Human Operator (HO) performs some significant tasks (see Fig. 1) in the initial stages of autonomous operation. During vessel operation, their involvement is primarily limited to occasional supervisory control tasks, ensuring a high level of autonomy. However, HO executes two control actions which are “Fallback recover response and Initiate fallback” under conditions of “Fallback is initiated, and required to continue the regular operation” for the former control task and “AOC loses the object detection or measurement ability, and required to maintain vessel safety” for the later control task. HO may create a total of 16 UCAs whereas both the control action tasks may create the same number of UCAs. 9 UCAs from the “Initiate fallback”, which may lead to both severe and mild effect hazards. Out of 9 UCAs, 7 are in the mild effect (H2 and H7) group, whereas the rest 2 are in the critical effect (poses H2,3,4,5 hazards) group. During “respond to fallback recovery”, all 7 UCAs are in the mild hazardous (H2, H6, H7) effect group. Though the control tasks are not very hazardous, HO must remain alert and active because of the supervisory responsibilities and be dedicated to operational mode selection. Control tasks are very infrequent but need to have adequate care during execution. However, the controller also needs to apply his/her cognitive judgment on the continuous action of the mild group with high frequency throughout the complete control task/s.

Hazard assessment of the PMS

Disconnecting thruster/s is the major control action of the PMS under four different conditions: "Whether it is required to prevent a blackout, if RPM control is possible, whether thrusters violate power limitations from PMS, and if it is required to prevent fire." In contrast, “Whether it is required to maintain ship stability, maintain speed restrictions at the port, or prevent blackout” outlines the three conditions for executing the control action “Limit power to thrust." These two control actions may result in a total of 43 UCAs, which is the maximum number of UCAs from an individual controller in this study. The Limit power to thrust action alone results in a total of 25 UCAs, while disconnecting thruster/s in two different situations yields 18 UCAs (8 and 10). H2, 6, and 7 present the greatest number of hazards, alongside a few from H1, 3, and 5 associated with this controller. 27, 6, and 10 UCAs fall into the mild, moderate, and critical groups, respectively. All 10 UCAs in the critical group are coherent with the Limit power to thrust controller, whereas disconnecting thruster/s are associated with the mild and moderate groups. Therefore, this action must be approached with high attention and requires regular maintenance and rigorous verification of this control algorithm.

Hazard assessment of the BMS

The Battery Management System (BMS) performs three control actions: regulating cooling, connecting the battery, and disconnecting the battery, based on specific operational conditions, including the need to prevent battery damage, avoid power blackouts, ensure continuous power supply, reduce fuel consumption, and mitigate uncontrolled temperature rise. During the execution of these control actions, BMS generates a total of 29 UCAs where 9, 11, and 9 UCAs emerge from cooling control, connect battery, and disconnect battery respectively. H1,2,6 and 7 are individual and combined hazards from BMS. 26 UCAs are in the mild hazardous effect group, and the remaining 3 UCAs are in the moderate effect group. There is no UCA in the critical group. Though battery fire can be severe, the possibility is very low. This is because (1) there is a sensor through which BMS identifies the standard temperature level of the battery/s. In case of overheating, the BMS shuts down the heat battery and starts a new one. (2) The sensor is updated regularly and is checked before the voyage as per the checklist. (3) The human operator is supervising the battery performance. In case of BMS failure, HO from the ROC can take the necessary steps. Therefore, low attention mode with this controller is expected to be adequate.

In Fig. 5, the total number of UCAs from the specified controllers is arranged based on the hazardous effects. From Fig. 4, out of a total of 127 UCAs, 93 UCAs belong to the mild effect group, and 7 and 27 UCAs are in the moderate and critical groups, respectively. The majority of the UCAs from all the controllers are within the mild effect group. That means most of the UCAs are less hazardous and need less attention mode to operate depending on the automation and frequency of action. SMC, HO, PMS, and BMS may emerge 0, 0, 4, and 3 UCAs respectively with moderate effects while 14, 2, 11, and 0 UCAs with critical effects. The SMC system exhibits a high potential for critical hazards, as it operates continuously in response to traffic and navigational routes throughout the voyage. During navigation, it may adjust course and speed set points to maintain safety when interacting regularly with other control systems. Consequently, these dynamic interactions increase the likelihood of hazardous events. However, HO experiences the fewest critical hazardous effects due to its limited and infrequent control actions. Its primary role in vessel control involves responding to fallback recovery procedures. But such fallback events are expected to occur infrequently. Common fallback strategies,

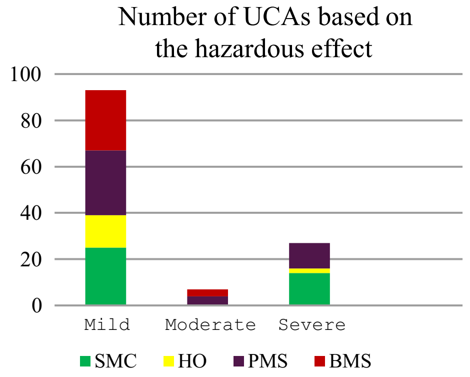


Fig. 5 Number of UCAs based on the hazardous effect

including anchoring, dynamic positioning (DP), and drifting, require HO intervention to transition the vessel back to regular operation. During fallback recovery, the HO follows predefined protocols that generally do not involve managing high-risk hazardous situations. Additionally, the HO may request the initiation of a fallback if the AOC fails to accurately assess a critical situation or predefined safety constraints. This may occur if the AOC loses object detection capabilities, encounters measurement errors, or fails to assess situational risks effectively. In such cases, HO intervention is necessary to ensure vessel safety by triggering the appropriate fallback response. From this control action a significant finding related to UCAs "*UCA.HO.01.007: HO needs to initiate pre-defined fallback to maintain the vessel's safety though the vessel does not lose object detection or measurement ability, and AOC does not realize it, but fallback is not initiated (H2)*" and "*UCA.HO.01.008: HO needs to initiate a pre-defined fallback to maintain the vessel's safety though the vessel does not lose object detection or measurement ability, and AOC does not realize it, but fallback is initiated after a long-time delay* (H2)" is that along with the object detection ability, the vessel is likely to violate other safety constraints that need to be scrutinized.

PMS, as the controller of the power system, exhibits the highest number of hazardous effects compared to other controllers, according to the analysis findings. This elevated risk level is attributed to its continuous operation, direct influence on critical power distribution, and interactions with multiple subsystems. Any failure or malfunction within the PMS can significantly impact vessel safety, propulsion, and operational efficiency. Therefore, implementing robust fault detection, redundancy mechanisms, and real-time monitoring strategies is crucial to mitigate these risks and enhance the overall reliability of autonomous ship power systems. The Battery Management System (BMS) is susceptible to generating a considerable number of hazardous effects; however, notably, none of these are classified as critical. While the STPA analysis identifies potential scenarios leading to battery fires, these events are considered highly unlikely due to the BMS's continuous monitoring and protective shutdown mechanisms. Although battery fires can have severe consequences, the probability of occurrence remains minimal for several reasons:

The BMS utilizes sensors to monitor battery temperature levels. If overheating is detected, the system automatically shuts down the affected battery and activates a backup unit.

These sensors undergo regular pre-voyage inspections in accordance with established checklists.

A human operator supervises battery performance, ensuring an additional layer of oversight.

In the event of a BMS failure, the Autonomous Onboard Controller (AOC) can initiate a fallback if predefined safety thresholds are exceeded. Additionally, the Human Operator (HO) at the Remote Operations Center (ROC) can intervene and update the voyage plan with appropriate corrective actions to maintain vessel safety.

Loss scenarios of this analysis play a vital role in reducing or mitigating the UCAs. If the specific reasons behind these UCAs are identified, safe control actions can be executed. Though there can be unforeseen reasons, loss scenarios identify the maximum possible reasons that lead to the UCAs. From this analysis, 457 loss scenarios are identified. From Table 10, it is obvious that each control action failure may have multiple reasons. Most of the common reasons are power failure, physical failure of the controller, communication or transmission error due to sensor failure, wrong interpretation of the feedback, flawed controlled process, and so on. From this analysis, SMC, HO, PMS, and BMS are individually involved with 126, 59, 157, and 115 scenarios respectively that may lead to the UCAs. PMS evolves the maximum number of UCAs, so the number of loss scenarios is also maximum for this controller.

This study gives significant insight into the potential reasons for the occurrence of hazardous scenarios. A single UCA can have multiple reasons for occurrence. Consequently, a single UCA can create multiple hazardous scenarios. By studying this analysis, operators can get familiar with the maximum number of reasons and scenarios. Thus, maximum precaution can be ensured.

While this study highlights various challenges, it is equally important to consider how AI can positively contribute to risk management in Maritime Autonomous Surface Ships (MASS). With advanced prognostic and diagnostic capabilities, AI can facilitate predictive maintenance by monitoring system performance and identifying potential issues in ship operations (Cheliotis et al. 2020) before they escalate into failures. This not only enhances operational reliability but also aids in preventing safety incidents. Additionally, AI can support dynamic fault detection and risk evaluation by synthesizing data from multiple sources in real time, enabling quicker and more accurate responses to evolving maritime conditions (Simion et al. 2024). These functions highlight AI's valuable role in strengthening safety and reducing risk in shipping operations. Therefore, future research will focus on augmenting the safety analysis of this proposed MASS study by integrating advanced AI-driven techniques.

Limitations of the study

This study has certain constraints that should be considered when interpreting the findings. The main limitation concerns the frequency at which the evolved UCAs occur. These UCAs arise only when controllers fail to execute control actions, making it challenging to estimate both the frequency of occurrence and the associated hazardous effects. Kim et al. (2021) encounter the same limitation when analyzing the safety of autonomous ships using the STPA method. This is primarily due to the fact that the autonomous vessel is still in a more conceptual stage and lacks substantial practical operational information. Additionally, the sheer number of potential loss scenarios complicates the identification of which specific loss scenario influences a UCA without thorough investigation. Additionally, since the recent concept of autonomous ship operation and the case study are under trial, some unforeseen hazards of real-time operation might not be counted. That means the use case autonomous ship of this study has not performed its practical commercial operation yet, and it eliminates the human interface from the vessel. Hence, the overall behavior of such a huge complex system is unknown and may cause new types of hazards. For example, during winter in ice areas or extreme weather, the communication link may fail to work, and the systems show unpredictable behavior (Chang et al. 2021). Furthermore, lack of an adequate definition of a fallback strategy. For example, in which particular states a fallback plan is expected, the procedure of initiating a fallback, and fallback recovery, etc. A comprehensive analysis is required to conduct both qualitative and quantitative hazard assessments for individual controllers, with particular emphasis on ship-side controllers. The STPA method is more qualitative, so it does not attempt to estimate and assess the risk level (Zhou et al. 2020).

Conclusion

This study conducts a systematic hazard analysis focusing on the interaction between remote operations center (ROC) controllers and onboard controllers in the autonomous operation of a use case short-sea service vessel. Additionally, it examines control action failures within individual controllers that contribute to hazardous situations. The use case aims to reduce human tasks and errors to improve safety by increasing the vessel's autonomy. The analysis considers four specific controllers: the Human Operator (HO) at the ROC on the shoreside, as well as the Ship Motion Controller (SMC), Power Management System (PMS), and Battery Management System (BMS) on the autonomous ship side. Using the Systems-Theoretic Process Analysis (STPA) method, this study identifies unsafe control actions arising during the execution of critical control functions and the interactions among these controllers. This study determines the UCAs from the individual control actions and prioritizes them based on the hazardous effect. Thus, this study helps in identifying less to more sensitive controllers and control actions. Based on the sensitivity, the controllers are considered with potential attentions that improve the safety of the operation.

Some significant observations are found when controllers with their control actions are classified depending on the UCAs and their hazardous effects.

Observation 1: Except for BMS, the other three controllers (SMC, HO, PMS) pose almost the same number of UCAs. BMS emerges as two-thirds of the UCAs of the average of the other three controllers. From the shoreside, VTS is a controller that does not create any control action failures. The reason is that it is not directly connected to any onboard control command for autonomous operation. VTS only communicates with the ROC and regulates the marine traffic instructions and information. Therefore, the only risk can be if the instruction and information to ROC are received late or interpreted incorrectly. AOC shares real-time navigational information with VTS.

Observation 2: Both the SMC and HO mostly execute the control actions to maintain safe navigational operation. The majority of their UCAs may arise during collision avoidance action. Loss of their control actions raises critical hazard H3. Navigational sensor failure and wrong interpretation of the sensor feedback are two major reasons for the unsafe control actions. Hence, these control actions need "High attention operation mode" from ROC. Besides, HO also performs a control action of PMS when PMS fails to do it.

Observation 3: Two-thirds of the total number of UCAs are in the mild hazardous effect group and need "Low attention operator mode" to execute and operate. "Limit power to thrust" is a control action of the PMS that creates the highest number of UCAs compared to the other control actions. Almost half of the UCAs are in the mild hazardous effect group while almost half of them are in the critical hazardous effect group. Though almost half of their UCAs are in the critical group, the action may continue with

"Low operator attention mode". This is because the probability of UCA occurrence is low due to its automatic functionality.

Observation 4: Both PMS and BMS exhibit the majority of the mild hazardous effects UCAs whereas BMS exhibits zero hazardous effects in the critical group. This is because both the controllers perform automatic functioning and are free of external influences which means no effect from other controllers during interaction. Due to their automatic functionality, they perform their control actions based on pre-defined conditions. Most of their loss scenarios are related to the physical failure of the sensor that leads to hazardous scenarios.

Observation 5: The reasons for the discussed loss scenarios are almost similar across individual controllers. The controller that generates more UCAs (Unsafe Control Actions) exhibits the highest number of loss scenarios, while the controller with comparatively fewer UCAs demonstrates a lower number of loss scenarios. This implies that a specific UCA can be associated with multiple potential loss scenarios. As the number of UCAs increases, the probable reasons contributing to their occurrence also expand. Control action "Limit power to thrust" from the PMS has a total of 94 reasons for control action failure. It can lead to almost the same number of mild and severe hazards. So, this control action can be critical at any time. However, studying these loss scenarios will possibly help to reduce or mitigate the UCAs.

STPA is a hazard analysis method that is popular in academia to identify the control action failure in the early design stage for any software-intensive complex system. Given that an autonomous ship is a software-intensive system, it is particularly suited for the application of the STPA method in hazard analysis. As our use case autonomous vessel is currently in the trial stage, the application of STPA assists in identifying and eliminating as many foreseen and unforeseen hazards as possible, thereby facilitating the approval process. Consequently, STPA opens new avenues for industrial approval.

However, further research is needed to strengthen the impact of this study and to support the advancement of the maritime autonomous industry. A priority is to clearly define operation modes, which outline the working principles, behaviors, and intentions of a new technology or system, to support a clearer understanding and analysis. Validation of Unsafe Control Actions (UCAs) through targeted testing or simulation is also essential, beginning with severe cases and progressing to moderate and mild scenarios. This process will enable the removal of low-impact UCAs and the implementation of targeted risk-reduction measures for those with significant effects. In addition, the specific responsibilities of the Autonomous Onboard Controller (AOC) and its interactions with shore-side controllers require closer examination. Finally, adopting a quantitative approach could strengthen the analysis method, drawing on current autonomous systems in other industries as a foundation. Such an approach would enable the evaluation and assessment of UCA frequency, leading to the reorganization of UCAs and their hazardous effects, and ultimately facilitating the establishment of more accurate hazard groupings.

Abbreviations

MASS	Maritime autonomous surface ships
IMO	International Maritime Organization
CA	Collision avoidance

SOLAS	Safety of life at sea
LNG	Liquified natural gas
LPG	Liquified petroleum gas
LIB	Lithium-ion battery
SOC	State of charge
SOH	State of health
SEAMLESS	Safe, efficient and autonomous: multimodal library of European shortsea and inland solutions
ROC	Remote Operation Center
HO	Human operator
AOC	Autonomous onboard controller
SMC	Ship motion controller
PMS	Power management system
BMS	Battery management system
VTS	Vessel traffic service
STAMP	System-theoretic accident modeling and processes
STPA	System theoretic process analysis
FTA	Fault tree analysis
FMECA	Failure modes effects and criticality analysis
HAZOP	Hazard and operability
BBN	Bayesian belief network
UCA	Unsafe control action
LS	Loss scenario
RPM	Rotation per minute

Acknowledgements
We extend our gratitude to the team members of Kongsberg Maritime and SINTEF Ocean involved in the SEMALESS project use cases for their invaluable support, which greatly facilitated this study.

Author contributions
MMAS: Plan for the whole paper. Introduction, methodology, data collection, analysis, result, discussion, writing. HK: Data curation, interpretation, editing, and validation. BR: Methodology, review and editing, discussion, supervision.

Funding
Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital). Funded by the European Union, Grant Agreement N° 101096923. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Declarations

Ethics approval and consent to participate
Not applicable. Our study does not involve any human participants, human data, human tissue, or animals.

Consent for publication
Not applicable. The manuscript does not contain any individual person's data in any form (including images, videos, or personal details).

Availability of data and materials
The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Competing interests
The authors declare that they have no competing interests.

Received: 17 October 2024 Revised: 12 August 2025 Accepted: 27 August 2025
Published online: 02 October 2025

References

ABS. (2020). *Advisory on Autonomous Functionality*. 24.

Alamoush AS, Ölçer AI, Ballini F (2024) Drivers, opportunities, and barriers, for adoption of maritime autonomous surface ships (MASS). J Int Marit Saf Environ Aff Shipp 8(4):2411183. https://doi.org/10.1080/25725084.2024.2411183

Al-Enazi A, Okonkwo EC, Bicer Y, Al-Ansari T (2021) A review of cleaner alternative fuels for maritime transportation. Energy Rep 7:1962–1985. https://doi.org/10.1016/j.egyr.2021.03.036

Alnes O, Eriksen S, Vartdal B-J (2017) Battery-powered ships: a class society perspective. IEEE Electrif Mag 5(3):10–21. https://doi.org/10.1109/MELE.2017.2718823

Andersson P, Wikman J, Arvidson M, Larsson F, Willstrand O (2017) Safe introduction of battery propulsion at sea. http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-30020

Andreas Lien Wennersberg L, Nordahl H, Ørnulf Jan R, Fjortoft K, Ambros Holte E (2020) A framework for description of autonomous ship systems and operations. IOP Conference series: materials science and engineering. https://www.academia.edu/91209079/A_framework_for_description_of_autonomous_ship_systems_and_operations

BahooToroody A, Abaei MM, Valdez Banda O, Montewka J, Kujala P (2022) On reliability assessment of ship machinery system in different autonomy degree; a Bayesian-based approach. Ocean Eng 254:111252. https://doi.org/10.1016/j.oceaneng.2022.111252

Baird AR, Archibald EJ, Marr KC, Ezekoye OA (2020) Explosion hazards from lithium-ion battery vent gas. J Power Sources. https://doi.org/10.1016/j.jpowsour.2019.227257

Bao J, Yu Z, Li Y, Wang X (2022) A novel approach to risk analysis of automooring operations on autonomous vessels. Maritime Transp Res 3:100050. https://doi.org/10.1016/j.martra.2022.100050

Bolbot V, Puisa R, Theotokatos G, Boulougouris E, Vassalos D (2019) A comparative safety assessment for direct current and direct current with hybrid supply power systems in a windfarm service operation vessel using system-theoretic process analysis: European STAMP Workshop & Conference. https://www.stamp-workshop.eu/

Bolbot V, Theotokatos G, Boulougouris E, Wennersberg LAL, Nordahl H, Rødseth ØJ, Faivre J, Colella MM (2020) Paving the way toward autonomous shipping development for European Waters—The AUTOSHIP project. Royal Institution of Naval Architects. https://strathprints.strath.ac.uk/73981/

Bolbot V, Theotokatos G, Lars Andreas LW, Faivre J, Vassalos D, Boulougouris E, Jan Rødseth Ø, Andersen P, Pauwelyn A-S, Van Coillie A (2021) (PDF) A novel risk assessment process: Application to an autonomous inland waterways ship. ResearchGate. https://doi.org/10.1177/1748006X211051829

Bolbot V, Gkerekos C, Theotokatos G, Boulougouris E (2022) Automatic traffic scenarios generation for autonomous ships collision avoidance system testing. Ocean Eng 254:111309. https://doi.org/10.1016/j.oceaneng.2022.111309

Burmeister H-C, Bruhn W, Rødseth ØJ, Porathe T (2014) Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: the MUNIN perspective. Int J E-Navig Maritime Econ 1:1–13. https://doi.org/10.1016/j.enavi.2014.12.002

Camila Correa-Jullian JG (2023) Proceedings of the 4th international workshop on autonomous systems safety. https://doi.org/10.34948/G4MW2N

Castilho DS, Urbina LMS, de Andrade D (2018) STPA for continuous controls: a flight testing study of aircraft crosswind takeoffs. Saf Sci 108:129–139. https://doi.org/10.1016/j.ssci.2018.04.013

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

Chae C-J, Kim M, Kim H-J (2020) A study on identification of development status of MASS technologies and directions of improvement. Appl Sci (Switzerland). https://doi.org/10.3390/app10134564

Chang C-H, Kontovas C, Yu Q, Yang Z (2021) Risk assessment of the operations of maritime autonomous surface ships. Reliab Eng Syst Saf 207:107324. https://doi.org/10.1016/j.ress.2020.107324

Cheliotis M, Lazakis I, Theotokatos G (2020) Machine learning and data-driven fault detection for ship systems operations. Ocean Eng 216:107968. https://doi.org/10.1016/j.oceaneng.2020.107968

Chin CS, Xiao J, Ghias AMYM, Venkateshkumar M, Sauer DU (2019) Customizable battery power system for marine and offshore applications: trends, configurations, and challenges. IEEE Electrif Mag 7(4):46–55. https://doi.org/10.1109/MELE.2019.2943977

DNV (2021) Supporting remote control operations in shipping: DNV publishes pioneering new competence standard and recommended practice. DNV. https://www.dnv.com/news/supporting-remote-control-operations-in-shipping-dnv-publishes-pioneering-new-competence-standard-and-recommended-practice-213200

Dybvik H, Veitch E, Steinert M (2020) Exploring challenges with designing and developing shore control centers (SCC) for autonomous ships. Proc des Soc des Conf 1:847–856. https://doi.org/10.1017/dsd.2020.131

Fan C, Wróbel K, Montewka J, Gil M, Wan C, Zhang D (2020) A framework to identify factors influencing navigational risk for maritime autonomous surface ships. Ocean Eng 202:107188. https://doi.org/10.1016/j.oceaneng.2020.107188

Geertsma RD, Negenborn RR, Visser K, Hopman JJ (2017) Design and control of hybrid power and propulsion systems for smart ships: a review of developments. Appl Energy 194:30–54. https://doi.org/10.1016/j.apenergy.2017.02.060

Hagaseth, M., Jan Rødseth, Ø., Håkon Meland, P., Wille, E., Murray, B., & Meling, P. (2022). Methodology for Approval of Autonomous Ship Systems CONOPS. *Zenodo (CERN European Organization for Nuclear Research)*. https://www.academia.edu/109255625/Methodology_for_Approval_of_Autonomous_Ship_Systems_CONOPS

Hagaseth M, Meland PH, Rødseth ØJ, Wille E, Nesheim DA (2023) Methodology for safety and security analysis (p. 88) [Project report]. AEGIS. https://aegis.autonomous-ship.org/resources/reports-and-articles/page/2/

Hüllein AS, Rokseth B, Utne IB (2024) Using STPA for hazard identification and comparison of hybrid power and propulsion systems at an early design stage. Ocean Eng 314:119752. https://doi.org/10.1016/j.oceaneng.2024.119752

IMO (2018a) 2018 Initial IMO Strategy. https://www.imo.org/en/OurWork/Environment/Pages/Vision-and-level-of-ambition-of-the-Initial-IMO-Strategy.aspx

IMO (2018b) International Maritime Organisation—An overview | ScienceDirect Topics. https://www.sciencedirect.com/topics/engineering/international-maritime-organisation

IMO (2021) Autonomous ships: Regulatory scoping exercise completed. https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx

IMO (2023) Revised GHG reduction strategy for global shipping adopted. https://www.imo.org/en/MediaCentre/PressBriefings/pages/Revised-GHG-reduction-strategy-for-global-shipping-adopted-.aspx

Inal O, Charpentier J-F, Deniz C (2022) Hybrid power and propulsion systems for ships: current status and future challenges. Renew Sustain Energy Rev. https://doi.org/10.1016/j.rser.2021.111965

Jalonen R, Tuominen R, Wahlström M (2016) Safety and security in autonomous shipping: challenges for research and development. Remote and Autonomous Ship. http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf

Jensen F (2015) Hazard and risk assessment of unmanned dry bulk carriers on the high seas. https://doi.org/10.24406/publica-3740

Johansen T, Utne IB (2022) Supervisory risk control of autonomous surface ships. Ocean Eng 251:111045. https://doi.org/10.1016/j.oceaneng.2022.111045

Johansen, T. A., Sørensen, A. J., Nordahl, O. J., Mo, O., & Fossen, T. I. (2007). *Experiences from Hardware-in-the-loop (HIL) Testing of Dynamic Positioning and Power Management Systems*. 10.

Johansen T, Blindheim S, Torben TR, Utne IB, Johansen TA, Sørensen AJ (2023) Development and testing of a risk-based control system for autonomous ships. Reliab Eng Syst Saf 234:109195. https://doi.org/10.1016/j.ress.2023.109195

Karkosiński D, Rosiński WA, Deinrych P, Potrykus S (2021) Onboard energy storage and power management systems for all-electric cargo vessel concept. Energies 14(4):1048. https://doi.org/10.3390/en14041048

Kim H, Lundteigen MA, Hafver A, Pedersen FB (2021) Utilization of risk priority number to systems-theoretic process analysis: a practical solution to manage a large number of unsafe control actions and loss scenarios. Proc Inst Mech Eng Part o J Risk Reliab 235(1):92–107. https://doi.org/10.1177/1748006X20939717

Komianos A (2018) The autonomous shipping era. Operational, regulatory, and quality challenges. TransNav Int J Mar Navig Saf Sea Transp. https://doi.org/10.12716/1001.12.02.15

Leveson NG (2016) Engineering a safer world: systems thinking applied to safety. The MIT Press. https://library.oapen.org/handle/20.500.12657/26043

Leveson NG, Thomas JP (2018) STPA handbook. MA, USA, Cambridge

Li X, Oh P, Zhou Y, Yuen KF (2023) Operational risk identification of maritime surface autonomous ship: a network analysis approach. Transp Policy 130:1–14. https://doi.org/10.1016/j.tranpol.2022.10.012

Lucà Trombetta G, Leonardi SG, Aloisio D, Andaloro L, Sergi F (2024) Lithium-ion batteries on board: a review on their integration for enabling the energy transition in shipping industry. Energies 17(5):Article 5. https://doi.org/10.3390/en17051019

MUNIN (2015) MUNIN D9 2 Qualitative Assessment CML Final | PDF | Ships | Risk. Scribd. https://www.scribd.com/document/515631920/MUNIN-D9-2-Qualitative-Assessment-CML-Final

NMA (2022) Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations—Norwegian Maritime Authority. https://www.sdir.no/en/shipping/legislation/directives/guidance-in-connection-with-the-construction-or-installation-of-automated-functionality-aimed-at-performing-unmanned-or-partially-unmanned-operations/

Nordahl H, Wennersberg LA (2024) D2.3—Concept of Operations and requirements for SEAMLESS building blocks (Project 101096923; p. 119). https://www.seamless-project.eu/wp-content/uploads/2024/09/SEAMLESS_D2.3-Concept-of-Operations-and-requirements-for-SEAMLESS-Building-blocks_Final.pdf

Nordahl H, Rødseth ØJ, Nesheim DA, Wennersberg LAL, Murray B (2023) [D8.2] Roadmap for Autonomous ship adoption and development [IA Innovation Action]. 18/03/2025. https://www.autoship-project.eu/wp-content/uploads/2023/03/Roadmap-for-Autonomous-ship-adoption-and-development.pdf

Oginni D, Camelia F, Chatzimichailidou M, Ferris TLJ (2023) Applying system-theoretic process analysis (STPA)-based methodology supported by systems engineering models to a UK rail project. Saf Sci 167:106275. https://doi.org/10.1016/j.ssci.2023.106275

Ölçer AI, Alamoush AS (2024) MASS and decarbonisation policy: exploring the nexus between maritime autonomous surface ships and decarbonisation efforts. In: Chae C-J, Baumler R (eds) Maritime autonomous surface ships (MASS)—regulation, technology, and policy: three dimensions of effective implementation. Springer, Switzerland, pp 235–262. https://doi.org/10.1007/978-3-031-69437-0_12

Paris Agreement (2018) Paris agreement—an overview | ScienceDirect Topics. https://www.sciencedirect.com/topics/earth-and-planetary-sciences/paris-agreement

Rasmussen J (1997) Risk management in a dynamic society: a modelling problem. Saf Sci 27(2):183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reddy NP, Skjetne R, Papageorgiou D (2023) A decentralized droop-based power management system for ship power systems using hybrid dynamical systems framework. 5. Scopus. https://doi.org/10.1115/OMAE2023-102570

Rejzek M, Hilbes C (2018) Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants. Nucl Eng des 331:125–135. https://doi.org/10.1016/j.nucengdes.2018.02.030

Rødseth ØJ, Wennersberg LAL, Nordahl H (2022) Levels of autonomy for ships. 1–9. https://sintef.brage.unit.no/sintef-xmlui/handle/11250/3011307

Rokseth B, Utne IB, Vinnem JE (2017) A systems approach to risk analysis of maritime operations. Proc Inst Mech Eng Part O J Risk Reliabil 231(1):53–68. https://doi.org/10.1177/1748006X16682606

Rokseth B, Utne IB, Vinnem JE (2018) Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. Reliab Eng Syst Saf 169:18–31. https://doi.org/10.1016/j.ress.2017.07.015

SEAMLESS (2023a) Demo & Transferability cases. Seamless Project. https://www.seamless-project.eu/demo-transferability-cases/

SEAMLESS (2023b) The project. Seamless Project. http://test.seamless-project.eu/the-project/

Simion D, Postolache F, Fleacă B, Fleacă E (2024) AI-driven predictive maintenance in modern maritime transport—enhancing operational efficiency and reliability. Appl Sci 14(20):Article 20. https://doi.org/10.3390/app14209439

Smartmaritime (2020) ASKO to build two autonomous vessels for Oslo fjord operations. Smart Maritime Network. https://smartmaritimenetwork.com/2020/09/01/asko-to-build-two-autonomous-vessels-for-oslo-fjord-operations/

Solberg CL (2018) An STPA analysis of the ReVolt—expanding and improving the system-theoretic process analysis (STPA) framework [Master thesis, NTNU]. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2560799

Sumon MMA, Kim H, Na S, Choung C, Kjønsberg E (2024a) Systems-based safety analysis for hydrogen-driven autonomous ships. J Mar Sci Eng 12(6):Article 6. https://doi.org/10.3390/jmse12061007

Sumon MMA, Rokseth B, Nordahl H, Wennersberg LAL (2024b) System theoretic process analysis based safety on different autonomy levels of autonomous ships for short sea service. ESREL 2024(1):10

Thieme CA, Rokseth B, Utne IB (2021) Risk-informed control systems for improved operational performance and decision-making. Proc Inst Mech Eng Part o J Risk Reliabil. https://doi.org/10.1177/1748006X211043657

Ventikos NP, Chmurski A, Louzis K (2020) A systems-based application for autonomous vessels safety: hazard identification as a function of increasing autonomy levels. Saf Sci 131:104919. https://doi.org/10.1016/j.ssci.2020.104919

Wang L, Li S, Liu J, Hu Y, Wu Q (2023) Design and implementation of a testing platform for ship control: a case study on the optimal switching controller for ship motion. Adv Eng Softw 178:103427. https://doi.org/10.1016/j.advengsoft.2023.103427

Wróbel K, Montewka J, 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. https://doi.org/10.1016/j.ress.2018.05.019

Xie P, Guerrero JM, Tan S, Bazmohammadi N, Vasquez JC, Mehrzadi M, Al-Turki Y (2022) Optimization-based power and energy management system in shipboard microgrid: a review. IEEE Syst J 16(1):578–590. https://doi.org/10.1109/JSYST.2020.3047673

Xie Y, Seenumani G, Sun J, Liu Y, Li Z (2007) A PC-cluster based real-time simulator for all-electric ship integrated power systems analysis and optimization 396–401. https://doi.org/10.1109/ESTS.2007.372116

Yamada T, Sato M, Kuranobu R, Watanabe R, Itoh H, Shiokari M, Yuzui T (2022) Evaluation of effectiveness of the STAMP / STPA in risk analysis of autonomous ship systems. J Phys Conf Ser 2311(1):012021. https://doi.org/10.1088/1742-6596/2311/1/012021

Yanchin I, Petrov O (2020) Towards autonomous shipping: benefits and challenges in the field of information technology and telecommunication. TransNav Int J Mar Navigat Saf Sea Transpor 14(3):611–619. https://doi.org/10.12716/1001.14.03.12

Yang X, Utne IB, Sandøy SS, Ramos MA, Rokseth B (2020) A systems-theoretic approach to hazard identification of marine systems with dynamic autonomy. Ocean Eng 217:107930. https://doi.org/10.1016/j.oceaneng.2020.107930

Yara (2021) Yara Birkeland | Press kit | Yara International. Yara None. https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/

Yuzui T, Kaneko F (2025) Toward a hybrid approach for the risk analysis of maritime autonomous surface ships: a systematic review. J Mar Sci Technol 30(1):153–176. https://doi.org/10.1007/s00773-024-01040-0

Zhou X-Y, Liu Z-J, Wang F-W, Wu Z-L, Cui R-D (2020) Towards applicability evaluation of hazard analysis methods for autonomous ships. Ocean Eng 214:107773. https://doi.org/10.1016/j.oceaneng.2020.107773

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.