

Article

Systems-Based Safety Analysis for Hydrogen-Driven Autonomous Ships

Mir Md Ashfaque Sumon ^{1,*} , Hyungju Kim ^{2,3} , Seong Na ⁴ , Choungho Choung ⁴ and Elisabeth Kjongsberg ⁵

- ¹ Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU), 7034 Trondheim, Norway
- ² Department of Maritime Operations, University of South-Eastern Norway (USN), 3184 Borre, Norway; hyungju.kim@usn.no
- ³ Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU), 7034 Trondheim, Norway; hyung-ju.kim@ntnu.no
- ⁴ System Safety Research Team, Korea Register (KR), Busan 46762, Republic of Korea; sna@krs.co.kr (S.N.); chchoung@krs.co.kr (C.C.)
- ⁵ Corvus Energy, 5224 Nesttun, Norway; ekjonsberg@corvusenergy.com
- * Correspondence: mir.m.a.sumon@ntnu.no; Tel.: +47-96810376

Abstract: In the maritime domain, hydrogen fuel cell propulsion and autonomous vessels are two important issues that are yet to be implemented together because of a few challenges. It is obvious that there are several individual safety studies on Maritime Autonomous Surface Ships and hydrogen storage as well as fuel cells based on various risk assessment tools but the combined safety studies that include hydrogen fuel cells on autonomous vessels with recent risk analysis methods are extremely limited. This research chooses the “System-Theoretic Process Analysis” (STPA) method which is a recent method for potential risk identification and mitigation. Both hydrogen and autonomous vessels are analyzed and assessed together with the STPA method. Results are not speculative but rather flexible compared to conventional systems. The study finds a total of 44 unsafe control actions (UCAs) evolved from human and central control unit controllers through STPA. Further, the loss scenarios (LS) are identified that lead to those UCAs so that loss scenarios can be assessed and UCAs can be mitigated for safe operation. The objective of this study is to ensure adequate safety for hydrogen fuel cell propulsion on autonomous vessels.

Keywords: safety; System-Theoretic Process Analysis (STPA); autonomous ship; hydrogen; fuel cell; concept of operations (CONOPS)



Citation: Sumon, M.M.A.; Kim, H.; Na, S.; Choung, C.; Kjongsberg, E. Systems-Based Safety Analysis for Hydrogen-Driven Autonomous Ships. *J. Mar. Sci. Eng.* **2024**, *12*, 1007. <https://doi.org/10.3390/jmse12061007>

Academic Editors: Leszek Chybowski, Jingbo Yin and Wenming (Wendy) Shi

Received: 11 April 2024

Revised: 25 May 2024

Accepted: 10 June 2024

Published: 17 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Maritime Autonomous Surface Ships (MASS) are one of the emerging research areas in the maritime industry. With the advancement in information and communication technology, updated computing systems, and technical improvement, core technologies for MASS have already been developed and demonstrated for both short and long routes, and the commercial operation of MASS is also expected soon.

IMO (2018) [1] defines MASS as “a ship which to varying degrees, can operate independently of human interaction”. Though various degrees of autonomy have been explained by [2,3], IMO (2021) [4] describes four degrees of autonomy level as follows:

- Degree 1: ship with automated processes and decision support with seafarers on board to operate and control.
- Degree 2: ships are remotely controlled with seafarers on board.
- Degree 3: the ship is controlled with remote operation from another location and no seafarers are on board.
- Degree 4: fully autonomous ship. The operating system of the ship can make decisions and determine actions.

As human involvement in MASS is highly limited or eliminated, MASS is expected to improve the safety of ship operations because (80–90) % of marine accidents occur directly or indirectly due to human factors [5]. Autonomous ships have a significant impact on trade and commerce due to cost-effectiveness and efficiency. Statistically, 20–30% of a ship's budget accounts for crew costs which can be cut by autonomous ships [6]. In addition, it increases the efficiency of maritime transportation as there is no accommodation, galley, or mess room for the crew, so the vessel will be able to carry more cargo [7,8]. Autonomous ships also contribute to reducing air pollution [9], as they are planned to operate with zero-emission alternative fuel. Reducing or eliminating human involvement on board will also reduce air pollution that can occur due to human activities.

The vision of autonomous ships into reality reached the limelight with the project “Maritime Unmanned Navigation through Intelligence in Networks (MUNIN)” [7] and “Advanced Autonomous Waterborne Applications Initiative (AAWA)” by Rolls-Royce [10]. International Maritime Organization (IMO) addressed autonomous ships for the first time in March 2018 and initiated the work on autonomous ships for safe, secure, and environmentally friendly operations [1]. Many international organizations have come forward to cooperate with the users, researchers, and authorities who have an interest in developing and promoting autonomous ships. From the very beginning, MASS has received significant attention from academic researchers [11], and recently from the industry. An overview of autonomous ships is presented by Vakil [12], and Yang et al. 2023 [13] delineate the dynamic maintenance and safe operation. Wróbel et al. [14] evaluated the safety of autonomous maritime navigation. On 30 May 2023, a symposium was held to establish and strengthen the contemporary IMO MASS code, and the event was co-hosted by IMO and the Republic of Korea [15]. The goal of the symposium was to adopt a mandatory MAAS code under “Safety of Life at Sea (SOLAS)” in the future. MASS code will establish a robust safety regime for MASS that ensures the safety of life at sea, as well as the safety of cargo on board and the MASS itself. Moreover, recently Japan's maritime industry has taken significant strides in the commercialization of full-scale autonomous ships with the MEGURI2040 Autonomous Ships project [16].

Though there are several studies on MASS [14–22], they are still in the initial stage. Some autonomous inland vessels and ferries are already in operation although these are under strict observation. Due to a large ship's potential to cause damage as well as the value of the ship and its cargo itself, autonomous ships need to consider safety with high importance [23]. Recently, IMO regulation for autonomous ships [24] has been implemented. Regulations are associated with the operation, maintenance, technological issues, and so on where all these aspects are implemented to ensure enough safety. Fan et al. [25] proposed a framework that enlisted navigational risk factors of remotely controlled MASS for four operational phases including voyage planning, berthing and unberthing, port approaching and departing, and open sea navigation. Chae et al.'s [26] study on technological developments of MASS suggests improvements in six research fields that cover all technological shortcomings. Risk analysis by system theoretic analysis (STPA) and the functional resonance analysis method (FRAM) is one of the significant research fields of the study that ensures adequate safety. Ventikos along with his team illustrate how a single control action failure affects the level of safety with the increase in autonomy level by the STPA method [27]. In addition, Veitch and Andreas highlight that human interaction has an active role in ensuring autonomous ship safety by including 42 studies [28]. Their study also suggests that STPA and Bayesian Networks are the most common and effective risk assessment tools for autonomous vessel safety. Unknown risks for autonomous ships emerge from the transfer of decision-making and action from the crew to either intelligent software and/or remote operators based on the shore [29]. Krzysztof Wróbel and his team analyzed a total of 46 control functions, affecting 24 high-level components of the MASS system based on STPA [30]. According to the study, the majority of the safety constraints can be articulated as technical issues, because new technology in the system can create new complexity and unknown hazards. Chang et al. quantify both technical and human

failure risk levels by combining Failure Mode Effects and Analysis (FMEA), Evidential Reasoning (ER), and Rule-based Bayesian Network (RBN) during MASS operation [31]. Hence, the Norwegian Maritime Authority has introduced guidance in connection with the construction or installation of automated functionality [32]. The guidance mentions all the required documents and principles related to autonomous and fully or partially remotely operated vessels. The aim is to ensure the same or more safety for MASS than that of conventional vessels. Compliance with the ISM Code is mandated in chapter 9 of the regulation, and as such, a Safety Management System (SMS) must be in place for any MASS that satisfies all the requirements of SOLAS, 1974. Due to the lack of specific rules and standards for the new technology of MASS, the European Maritime Safety Agency (EMSA) focuses on an alternative design approach where individual flags may have clear interpretations to create different safety levels [33]. To perform a functional study, EMSA has contracted DNV. The purpose of that study is to develop a risk-based assessment tool (RBAT) and software for MASS specifically.

Reducing the emission of gases from vessels is another emerging research area in the maritime industry. One of the major sources of the world's carbon footprint is due to the transportation sector. Among the total carbon emissions of transportation, about 71% of the impact is from maritime transportation as it is a major source of global trade [34]. For marine propulsion, long-term used conventional fuels have a high amount of sulphur content and release toxic gases when burnt [35]. To reduce greenhouse gas emissions, sulphur, and nitrogen contents, IMO [36] has envisaged reducing the carbon emission to zero level by 2050 in the world maritime industry. Very recently IMO has adopted a revised GHG reduction strategy that opens a new chapter towards maritime decarbonization [37]. It has been reported that the aim is to reduce the total annual GHG emissions from international shipping by at least 20%, striving for 30% by 2030 and at least 70%, striving for 80% by 2040 compared to 2008. There are many measures to reduce GHG in the maritime industry such as route planning optimization, efficient port operations, slow steaming, energy on board saving, etc. [38] but the best way is to transition to renewables and cleaner sources of fuel. As a result, alternative fuels that emit zero carbon, and low or no toxic contents are under trial, and some have been implemented already to execute the greener ship plan of IMO. Some common alternative fuels are hydrogen, battery, liquefied natural gas (LNG), liquefied petroleum gas (LPG), biofuels, methanol, solar energy, nuclear energy, etc. Most of the fuels are very recent in the maritime industry. The purpose of alternative fuels was also clearly discussed by DNV [38]. In addition to accelerating the greener ship plan, several opportunities and challenges of maritime alternative fuels have been described by Foretich et al. [39]. Among these alternative fuels, hydrogen is one of the most promising alternative fuels for zero-emission shipping. Being a renewable energy, cleaner as well as greener, and abundant in nature, hydrogen has the potential to play a central role in the energy transition [40]. Hydrogen fuel can be used with "Internal Combustion Engines (ICE) and fuel cells" for marine propulsion. Among these, the use of hydrogen fuel cells is more competitive and safer [41,42]. Hydrogen fuel cells are used to produce electricity from hydrogen fuel for propulsion. American Bureau of Shipping defines a fuel cell as a device that continuously converts an oxidizing fuel (hydrogen, methane, etc.) into electricity and water through an electrochemical reaction [43]. The proton Exchange Membrane Fuel Cell (PEMFC) seems to be the best candidate for use in naval applications when operated with hydrogen [44] because PEMFC can operate with low-temperature fuel cells and hydrogen fuel is preserved and operated at very low temperatures. The performance of PEMFCs depends on the catalyst, bipolar plate, membrane electrode, and sealing materials [45]. The first hydrogen-powered ferry "MF Hydra" for a short route was introduced in 2023 [46].

It has been accepted globally that hydrogen (H_2) is a clean energy carrier. Hence, more than 1500 hydrogen-related projects were initiated globally by mid-2022, while more than 60 countries have already developed or are developing hydrogen strategies [47]. Hydrogen is considered highly versatile and efficient in production and utilization [48]. According to the International Renewable Energy Agency (IRENA), hydrogen is capable of meeting up to 12% of global energy demands by 2050 [49]. In the past decade, green hydrogen has been a popular alternative fuel. However, risk analysis on the key technologies of hydrogen-driven vessels related to the power source, hydrogen production, hydrogen storage, and hydrogen safety is in progress [50]. Consequently, a noticeable rise in the number of operations in short as well as large vessels is now a matter of time. The use of hydrogen as fuel may require a completely new and specific ship design to meet the safety challenges [50]. Safety rules for using hydrogen are very limited. Especially for the use of hydrogen and fuel cells on board ships, there are no established regulations [51] and risk analysis is also very limited. Hence, the International Code of Safety for ships using gases or other low flashpoint fuels (IGF) is followed [51]. In the aforementioned study, the probable risks associated with hydrogen and fuel cell-driven vessels are presented. In addition, hazard identification on hydrogen storage and hydrogen fuel cell vehicles to determine the accident scenarios is performed [52,53]. Cui et al. [52] used failure mode and effect analysis (FMEA) to identify hazards while Shen et al. [53] carried out both hazard and operability (HAZOP) and FMEA. Leakage control is the major challenge in the use and transportation of hydrogen. Data on the hydrogen system leakage frequencies are available from the Sandia National Laboratories HyRAM [54]. The leakage or diffusion laws and distribution of hydrogen in the compartments of fuel cell ships are different in different situations, which was determined by the software FLUENT [55]. It identified that risks are also different in different locations and instruments, and the hydrogen concentration near the leakage point is near about 100% after around 60s. A significant discussion is presented by Balestra et al. [56] where it is shown that the most leak-prone area is the tank connection space (TCS) of a hydrogen-powered vessel. Hydrogen leakage creates potential risks because of its high flammability in the air. However, there are also several hazards involved with operating liquid hydrogen, e.g., fire, explosion, asphyxiation in indoor accidents, and frostbites due to exposure to extremely low temperatures [57]. Liquefying hydrogen consumes about 30% of the energy content of hydrogen. A very low temperature ($-253\text{ }^{\circ}\text{C}$ under 1 bar) is needed to preserve and transport liquid hydrogen [58]. During huge energy consumption, liquid H_2 faces challenges that occur at the time of liquefaction and in the loss of H_2 through boil-off during storage [48]. Moreover, good insulation and evaporation are required. Hence, the cryogenic state is formulated for liquid hydrogen. Cryogenic hydrogen is a condition where the density of the liquid hydrogen is twice that of the compressed hydrogen at 70 MPa. Millet presents a detailed overview of the cryogenic storage tank [59].

Based on the two emerging research areas, the focus of this study is the combination of autonomous operation and hydrogen fuel cell propulsion. The purpose of this combined operation is to make a safe, efficient, and cost-effective voyage with the help of an autonomous vessel and to make the autonomous vessel greener with the help of hydrogen fuel cell propulsion. The application of alternative fuel in autonomous vessels is a huge revolution [60]. Of particular importance is the use of a liquid form of hydrogen as an alternative fuel because the regular form of hydrogen takes up a huge amount of space to store due to its extremely low density (0.0883 kg/m^3 at atmospheric temperature and pressure), whereas liquid hydrogen (LH_2) has a density three orders of magnitude higher (70.9 kg/m^3) compared to atmospheric conditions [61]. The use of hydrogen fuel cell propulsion on autonomous ships will be unique in the maritime industry. DNV records that “new vessel operational concepts based on the autonomous and remote control of vessel functions shall have a level of safety equivalent or better, compared to conventional operations of vessels concerning safeguarding life, property, and the environment” [62].

As there are an extremely limited number of safety studies on this combined system, an adequate safety analysis is required.

There are several individual safety studies on MASS and hydrogen storage as well as fuel cells based on various risk assessment tools, but combined safety studies on hydrogen fuel cells for autonomous vessels based on the STPA method are extremely limited. Therefore, the objective of this ongoing study is to ensure adequate safety for the hydrogen fuel cell propulsion on autonomous vessels for long-route vessels with the help of the STPA hazard analysis method. The analysis presents insights into two major controllers which are “emergency shutdown and speed control of the vessel”. The unsafe control actions (UCAs) of these controllers can have a detrimental effect on MASS safety because these are involved not only in preventing collision but also in maintaining autonomous navigation as well as hydrogen propulsion. This study also delineates the potential reasons that lead to the UCAs so that risk mitigation steps can be followed easily.

Section 2 of this article explains the methodology of the study where the STPA method is implemented along with the operational scenario of the whole system based on the concept of operations (CONOPS). Section 3 illustrates the results where UCAs are determined from the two significant control actions’ failures. Section 4 provides a concise as well as precise discussion based on the result and a comparison of the STPA method based on the ongoing study and the existing literature. Section 5 delineates the conclusion of the study, including opportunities for future research.

2. Methodology

This section presents data collection and analysis procedures and a brief discussion of STPA methodology as well as specific safety studies on different terrains based on STPA. The operational procedure of the whole system of this study is also described with the concept of operations (CONOPS).

2.1. Data Collection and Analysis

Primary data collection commenced using the existing literature and the author’s expertise as well as brainstorming. Later, there were meetings with academic researchers and industrial practitioners to develop significant results. This study includes a company that is going to commercialize hydrogen fuel cells onboard ships in the near future. In addition, the author visited the company to observe safety tests and had a discussion with the project members of the company. This company also commissioned an internal risk analysis by a third party and the analysis report was shared with the authors and used as a secondary data source for this ongoing study.

All the data, workshops, and discussions were theorized and used to conduct this study with the STPA method to analyze data.

2.2. STPA

STPA (System Theoretic Process Analysis) is a modern hazard analysis approach to prevent accidents and is more effective in modern and complex systems. It is a hazard analysis technique based on the System-Theoretic Accident Model and Processes (STAMP) theory which is described in detail in [63]. Earlier accidents were mostly attributed to component failures or human errors. At that time, most of the conventional systems were electro-mechanical and relatively simple compared to contemporary software-intensive socio-technical systems [64]. Most modern software-based systems are complex, and they often create unexpected situations or hazards from control-related issues. The main principle of the STPA technique is that “accidents are not failure problems” but “control problems”. That is why the main aim of this method is to analyze unsafe control actions and loss scenarios [63]. According to many authors, STAMP-based approaches are capable enough to identify or predict more possible hazards than conventional methods, from early to advanced stages of system development [63–67]. This method has commonly been used in unmanned systems for safety analysis such as autonomous ship safety [14],

aviation [68,69], and so on. In addition, Zhou et al. [70] conclude that the STPA is the most promising hazard identification method for software-intensive systems compared to traditional methods such as Fault Trees Analysis (FTA) and Failure Modes and Effects Analysis (FMEA). For example, an unidentified event cannot be prevented by HAZID analysis [71] while STPA can prevent it. As autonomous vessels are contemporary as well as software-intensive approaches, the application of hydrogen fuel cell propulsion on a ship creates a new dimension. The STPA method fits the best to assess formal safety because STPA uses a functional model that is based on a holistic representation. Moreover, this method can identify major and maximum possible hazardous contexts with limited information [63]. Another advantage of STPA is that it can generate safety constraints and involved requirements, and the result can be reviewed for feasibility and effectiveness [72]. The STPA method is based on modeling a hierarchical control structure of the system and identifies unsafe situations that lead to accidents.

There are four steps in STPA analysis:

1. Define the purpose of the analysis.
2. Model the control structure.
3. Identify unsafe control actions.
4. Identify loss scenarios.

Step 1: Purpose of the Analysis

The first step of STPA is to define the purpose of the analysis. This step defines the purpose of the whole system. The major purposes of this step are included at the beginning of this analysis along with the system boundary and goal [11]. In this step, a system description is formulated, and based on this, possible losses and system hazards along with system constraints are identified. The system description is presented in Section 2.3 in the CONOPS for a better understanding of the entire system for analysis. System-level hazards during speed change and emergency shutdown actions of the MASS operation are presented in the results section.

Step 2: Model of the Control Structure

This step aims to capture functional relationships and interactions by modeling the system as a set of feedback control loops [63]. The structure is illustrated based on the responsibilities of all model elements and functional requirements. The concepts of the design of hydrogen propulsion on remotely controlled ships (no seafarers onboard) are still being developed. Hence, the final structure of the diagram is based on the brainstorming workshop with experts and a few earlier published studies.

Step 3: Unsafe Control Actions

Unsafe control actions (UCAs) generally define the control actions in the control structure and how they lead to losses which are presented in Step 1 [11]. Leveson and Thomas report [64] that “an unsafe control action is a control action that, in a particular context and worst-case environment, will lead to a hazard”. In this study, the Central Control Unit (CCU) and Human Operator (HO) are two controllers whose wrong control actions for different actions can create UCAs.

Step 4: Loss Scenarios

A loss scenario represents the specific and structured reasons that lead to unsafe control actions and hazards [63]. Moreover, loss scenarios also show why the control actions are executed improperly or not executed. Two types of loss scenarios need to be accounted for.

1. The reasons for the unsafe control actions.
2. The reasons for not executing or wrong execution of control actions that lead to hazards.

The probable reasons why and how CCU and HO create the UCAs are the loss scenarios for this analysis.

2.3. Concepts of Operations (CONOPS)

Through CONOPS, the operational procedure of the whole system along with the components of the system and system illustration have been presented for clear conception.

2.3.1. System Descriptions

This study focuses on the risk analysis of a hydrogen propulsion system through a fuel cell where supplied hydrogen fuel is stored in the cryogenic tank in liquid form. More significantly, the whole system is controlled under an autonomous system (Autonomy degree 3—remotely controlled ship with no seafarers onboard).

The very first step of the system begins with the production of liquid hydrogen (LH2). The electrolysis process is used for production which is not part of this analysis. The liquid form of hydrogen on board is stored in a cryogenic tank as it requires a very low temperature (-253°C). This study commenced with the cryogenic storage tank. Integrating the system in the vessel design, combining technical aspects with a safety barrier analysis, a cryogenic tank is placed under the deck [73]. Next, there is a tank connection space (TCS) that encloses the valves coming from a liquid hydrogen (LH2) tank in a ventilated box. It allows for hydrogen venting in a controlled space able to withstand cryogenic temperatures. After that, hydrogen passes through the vaporizer which turns the liquid hydrogen into a gaseous state to feed into the fuel cell. A sufficient amount of pressure of hydrogen flow is regulated by a regulator that is included as a part of the internal sensors. Later, hydrogen enters the fuel cell where all the required components are combined to produce electric power for the propulsion system. All the internal and external components are controlled under the internal sensors of the autonomous system. The fuel cell is located at the top of the board inside a fuel cell frame where a series of fuel cells are included parallelly as per the power required for the ship. On top of the fuel cell, a vent mast is included so that excessive or unused hydrogen gas can exit. With the fuel cell, an external circuit is connected and the purpose of it is to convert AC/DC as well as to pass electricity for propulsion. The system ends with the propulsion motor that rotates the propeller of the vessel. As a part of the autonomous system, there are a few external sensors that control the vessel's navigation and maintain communication with the shore operator through the satellite.

Although primary power is derived from the battery to initiate the whole system, this study specifically focuses on hydrogen fuel cell propulsion as well as the autonomous system. Analysis of the battery is not within the scope of this study and is left for future discussion. It is also to be considered that the study is partially conceptual, especially with the design and placement of the major elements of the vessel.

2.3.2. System Configuration

This section is included for the clear visualization of the aforementioned system description. The visualization is presented in Figure 1 where the configuration starts with the production of hydrogen and ends with the propulsion system along with autonomous system operation. Though the current study does not focus on every step, components are illustrated for clear conception and visualization.

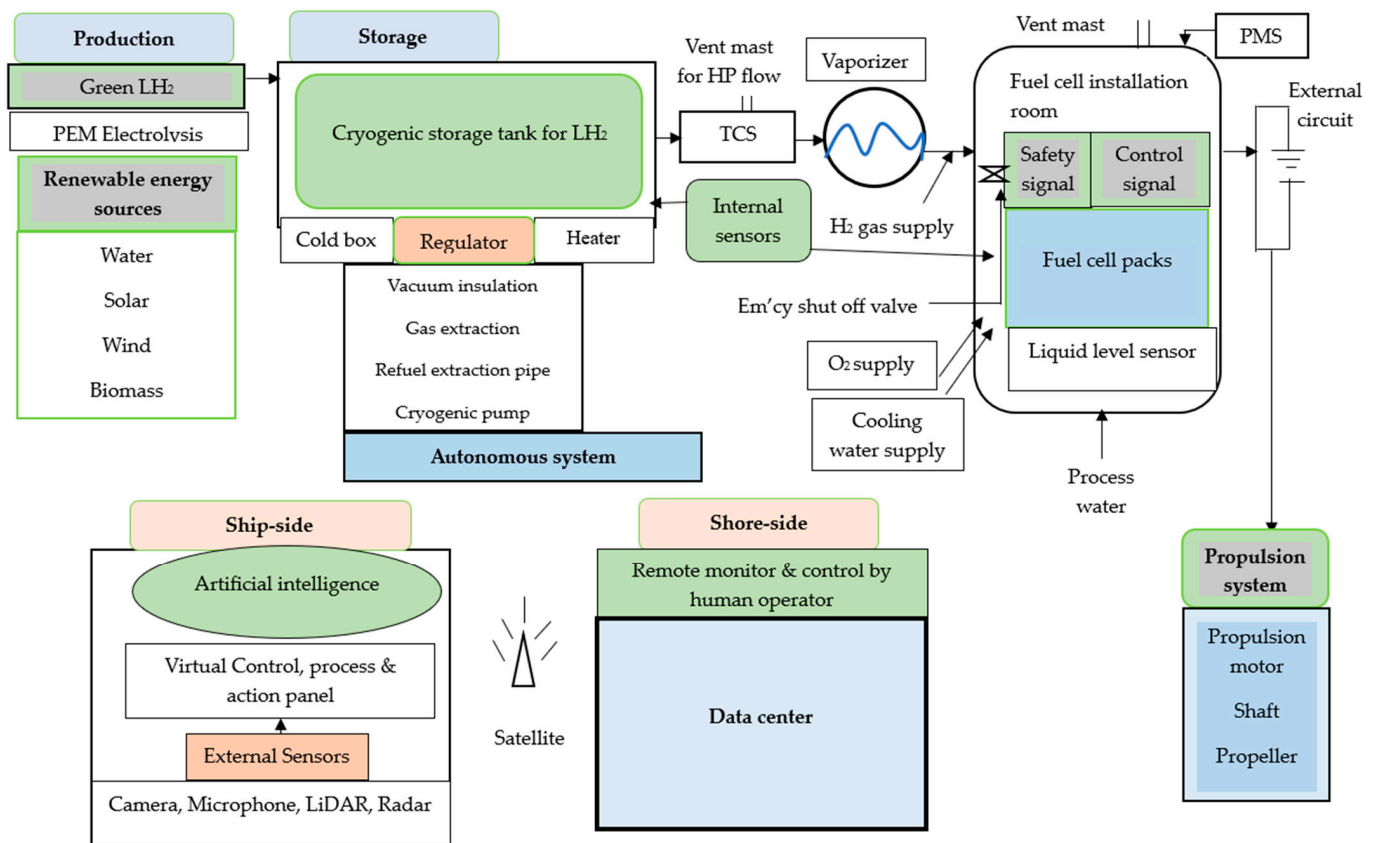


Figure 1. Illustration of the system configuration.

3. Result

3.1. STPA: Step 1

In this study, the system boundary is associated with the hydrogen fuel cell propulsion system on a remotely controlled ship with no seafarers onboard (autonomous level 3). As an alternative fuel, the use of liquid hydrogen with a fuel cell onboard is new and the same context applies to the autonomous vessel, hence the purpose is to carry out the safety analysis of the whole system so that risk-free as well as cost-effective operations are performed. In this step, at first, the possible losses that can occur from the operation of the whole system are pointed out. Individual loss is identified with the letter “L”. The losses are not limited to the autonomous ship itself but also to other ships. After that, system-level hazards that lead to these losses and system-level constraints that restrict these losses are established and presented in Table 1.

Table 1. System-level hazards and system-level constraints.

System-Level Hazards	System-Level Constraints
H-1: Vessel generates inappropriate propulsion (thrust) power. (L-1, L-2, L-3, L-4, L-5)	SC-1: The vessel must generate appropriate propulsion (thrust) power to run the engine appropriately.
H-2: The vessel approaches being approached too close to an obstacle or other vessel. (L-1, L-2, L-3, L-4, L-5, L-6, L-7)	SC-2: The vessel should always keep a minimum distance from obstacles or other vessels to avoid collision.
H-3: The vessel loses its intact stability. (L-2, L-3, L-4)	SC-3: The vessel should never lose its intact stability.
H-4: Human operation is inactive or inappropriate while needed. (L-1, L-2, L-3, L-4, L-5, L-7).	SC-4: Human operator/s should take active and appropriate action as per the requirement to maintain a smooth voyage.
H-5: Unauthorized access to the vessel. (L-1, L-2, L-3, L-5, L-7, L-8)	SC-5: Unauthorized access must be prevented.

Losses:

L-1: Loss of life or serious injury to people of another vessel.

L-2: Loss of or damage to the ship.

L-3: Loss of or damage to objects outside the ship.

L-4: Loss of time.

L-5: Loss of acceptance and approval of the autonomous ships.

L-6: Environmental pollution or damage.

L-7: Loss of cargo.

L-8: Loss of confidential information about the vessel and the mission.

3.2. Step 2: Model the Control Structure

The functional control structure during the voyage is shown in Figure 2. The control structure mainly acts in four specific sections of the model. These are (1) the remote-control center (RCC), (2) internal control system (ICS), (3) energy system, and (4) propulsion system.

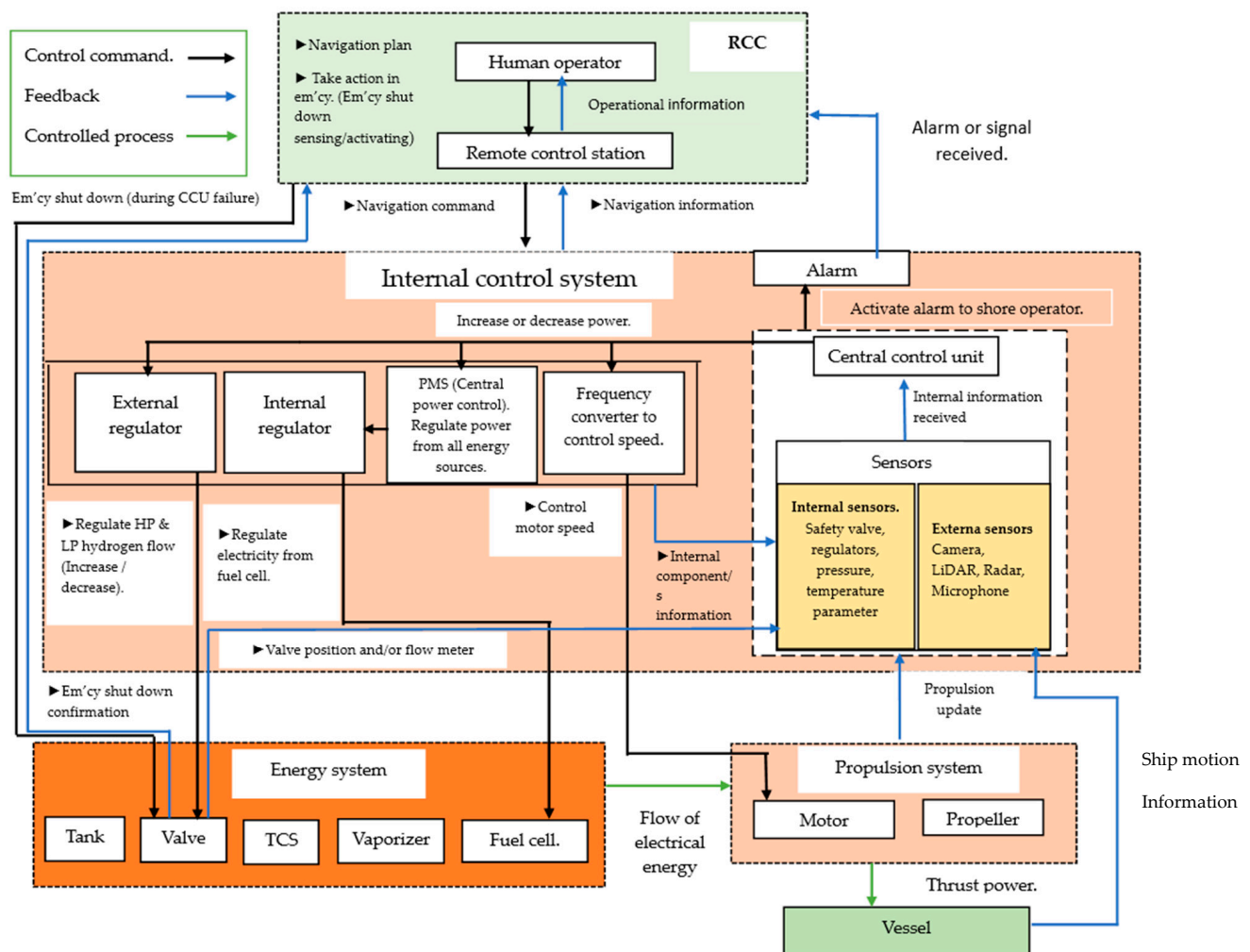


Figure 2. Control structure model of the system.

3.2.1. Remote Control Center (RCC)

RCC is controlled by one or more human operators depending on the job functions. Human operator/s practically command the navigation where the major control actions are included in the navigation plan and emergency shutdown. The navigation plan means specifying the voyage routes as well as the port of arrival and departure. This action also includes speeding up and speeding down the vessel depending on the stakeholder's

requirement as well as collision or piracy avoidance. Next, another vital action is the emergency shutdown of the vessel during a critical situation.

3.2.2. Internal Control System (ICS)

This system receives a command from the RCC and executes it to the next system by a few specific control action units of the internal system. The Central control unit, also known as the virtual captain, is a software algorithm that commands the other sub-control action units to increase or decrease the power of the vessel. Increasing and decreasing the power means speeding up or speeding down the vessel as per the navigation plan. It also shuts down the system or vessel during an emergency by decreasing the power supply to zero level. The Power Management System (PMS) of this control unit plays a vast role which mainly includes commanding the internal regulator of this section to regulate the electricity flow of the fuel cell. PMS not only commands the internal regulator but also controls the power distribution system of the entire vessel.

3.2.3. Energy System

The energy system executes the command actions received from the ICU by controlling the flow of energy. Initially, the valve regulates the fuel supply amount depending on the required speed. When high speed or low speed is required, it increases or decreases the fuel supply, respectively. The valve also receives the emergency shutdown command directly from the RCC when there is a malfunction in the central control unit. It executes the command by directly cutting off the fuel supply to the fuel cell, and therefore, no power is produced from the fuel cell for propulsion. The emergency shutdown confirmation feedback is also directly sent to the RCC through a flow meter sensor. In this system, the fuel cell performs a significant role because the internal regulator commands the fuel cell unit to speed up or speed down as well as perform emergency shutdowns. In an emergency shutdown situation, the produced power is supplied to the battery. During the speed-down situation, extra power is also supplied to the battery. During the speed-up situation, the fuel cell receives additional fuel from the storage tank through the valve or takes additional power from the battery (which is not part of this analysis).

3.2.4. Propulsion System

The propulsion system performs straightforward functions. Motor rotation speeds up or speeds down or stops as per the functional command. This system is synchronized by the “frequency converter to control speed” command. Hence, low, high, or no thrust power is generated.

3.2.5. Responsibility, Process Model, and Feedback

This section presents the responsibilities of the human operator and central control unit (CCU) controllers in a structured way in Tables 2–4. In addition, when these responsibilities need functioning is also included with the identification of the process model along with the feedback.

Table 2. Responsibility, process model, and feedback of human operator during speed change.

Human Operator		
Responsibility	Process Model	Feedback
Speed up the vessel with a feasible propulsion system (SC 2) (SC 4) (SC 5).	• Unexpected obstacles. • Approaching unauthorized entry towards the vessel. • Required to maintain voyage plan. • Heavy weather conditions.	Location/heading/increase energy or power supply.

Table 2. *Cont.*

Human Operator		
Responsibility	Process Model	Feedback
Speed down the vessel (SC 2) (SC 4) (SC 5).	• Unexpected obstacles. • Approaching unauthorized entry towards the vessel. • Required to maintain voyage plan. • Heavy weather conditions. • Propulsion equipment (fuel cell, motor, etc.) is overheated or overloaded.	Location/heading/decrease energy or power supply.

Table 3. Responsibility, process model, and feedback of Central Control Unit during emergency shutdown.

Central Control Unit (CCU)		
Responsibility	Process Model	Feedback
Activate the emergency shutdown (SC 1) (SC 3)	• Fuel cell is overloaded or overheated (due to fire). • The intact stability of the vessel is lost. • Uncontrollable fire onboard • Vital internal equipment is damaged by the external substance. • Fuel storage tank leakages or damages.	Fuel or power supply cut off.
Deactivate the emergency shutdown or start the vessel (SC 1) (SC 3).	• Intact stability of the vessel is maintained after an emergency. • Emergency situation is controlled.	Fuel or power supply flow.

Table 4. Responsibility, process model, and feedback of Human operator during emergency shutdown.

Human Operator		
Responsibility	Process Control	Feedback
Activate the emergency shutdown directly via the valve (SC 1) (SC 3).	The intact stability of the vessel is lost, uncontrollable fire, fuel cell overload or overheated, storage tank leakages along with the internal control system (ICS) failure.	Fuel supply cut off.

3.3. Step 3: Identifying Unsafe Control Actions (UCAs)

This step identifies UCAs that originate from emergency shutdown and speed-related control actions. The human operator and CCU perform the responsibility of the system. Control actions are structured at different conditions initially. Later, all the unsafe control actions related to those two control actions are determined according to the varied conditions in a structured way. Table 5 demonstrates an example of how the UCAs are identified while the “Emergency shutdown” action is executed by the “CCU” under varied conditions (not provided, provided, too early, too late too short, and too long). In Table 5, there are four major columns. The first column contains the ID numbers related to the specific controller’s actions. The second column mentions the specific action of that controller (such as CCU here). The third column is for the two different conditions during the execution of the control action. The column has two sub-conditions such as whether the execution of the control action is required or not and whether the power supply is favorable or not. The fourth column is used to identify the unsafe control actions (UCAs), which is the

aim of this analysis. The column has six sub-columns that are the varied context of the control action (emergency shutdown activate) execution. Based on the two conditions, in some contexts the execution of the control action is unsafe while in some contexts the execution is safe, or execution is not applicable. For example, at “CA.CCU.009”, control action “Emergency shutdown activation” is required and there is no power, but the control action is not provided. Hence, it is unsafe (UCA). In the next slot, in the same condition, the action is provided as it is required, so it is a safe action. The red marking written as “Unsafe” slots are our investigated UCAs. The entire analysis is presented in Appendix A.

Table 5. Identification of UCAs.

Controller: CCU									
ID	Control Action	Condition		Unsafe Control Actions					
		Activation Required	Fuel or Power Supply Cut Off?	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.CCU.009	Emergency shutdown activate	Yes	Yes	Unsafe (H1)	Safe	N/A	N/A	Unsafe (H1)	Unsafe (H3)
CA.CCU.010		Yes	No	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A	Unsafe (H1)
CA.CCU.011		No	Yes	Safe	Unsafe (H1)	N/A	N/A	N/A	N/A
CA.CCU.012		No	No	Safe	Unsafe (H3)	N/A	N/A	N/A	N/A

Similarly, three more control actions which are “speed up, down, and emergency shutdown directly via valve” of the human operator and one control action (shut down, deactivate, or start the vessel) of CCU are analyzed, and UCAs that evolve from those are determined. The number and percentage of UCAs from the two controllers during the specific control actions are presented in the following Tables 6–8, and Figure 3a,b, and Figure 4. In Table 6, the number of UCAs from human operator/s during “speed up, down, and emergency shutdown” actions are presented. The number of UCAs from individual actions is almost the same. In the same way, Table 7 presents the number of UCAs from the CCU during two control actions (emergency shutdown activate and deactivate) and the numbers of UCAs are exactly the same. Figure 3a,b compares the percentage difference of UCAs from the individual control actions of human operator/s and CCU, respectively.

Table 6. Total unsafe control actions from human operator/s.

UCAs from Human Operator	
Control Actions	No. of UCAs
Speed up	10
Speed down	9
Emergency shutdown directly via valve	9

Table 7. Total unsafe control actions from the central control unit.

UCAs from CCU	
Control Actions	No. of UCAs
Emergency shutdown activated	8
Emergency shutdown deactivated or start the vessel	8

Table 8. Combined UCAs from HO and CCU.

UCAs from Both Controllers	
Controller	No. of UCAs
Human Operator	28
CCU	16

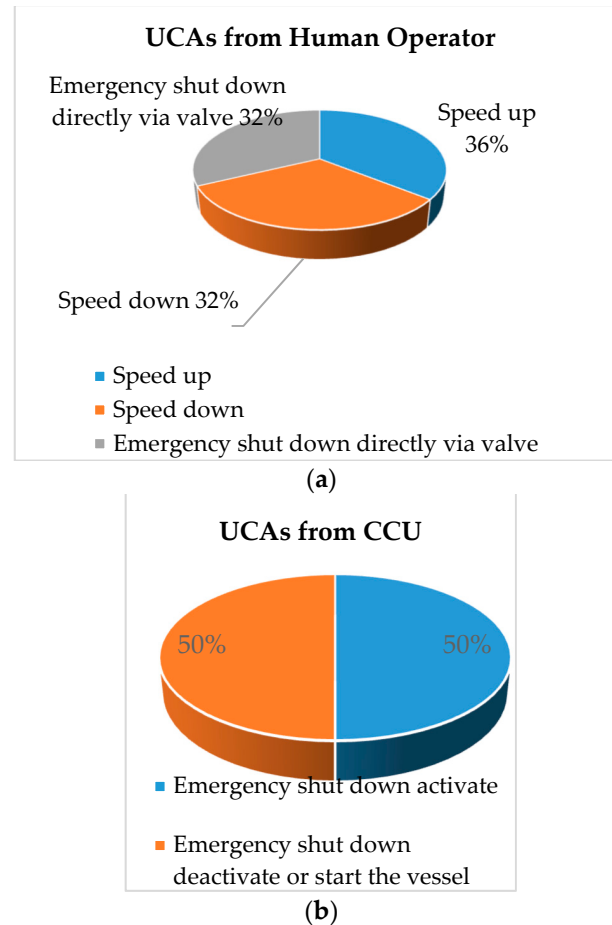
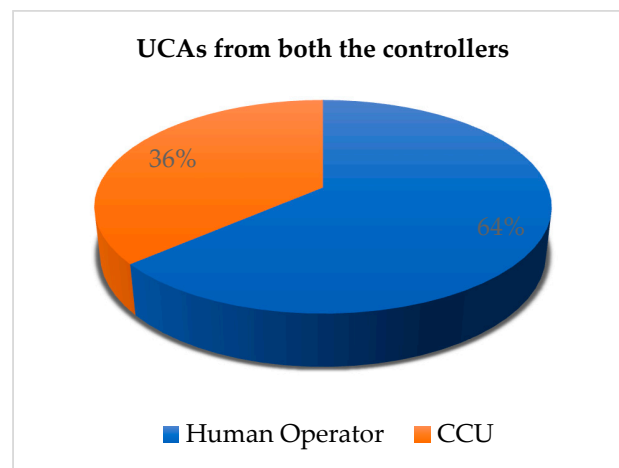
**Figure 3.** (a) Percentage of UCAs of HO from individual control actions. (b) Percentage of UCAs of CCU from individual control actions.**Figure 4.** Percentage of UCAs from both CCU and HO.

Table 8 represents the total number of UCAs from the human operator/s and CCU and Figure 4 compares their percentage difference. The number of UCAs from HO is significantly more than the number of UCAs from the CCU. HO (3) also executes more control actions than CCU (2).

3.4. Step 4: Loss Scenarios

In this section, major possible loss scenarios that lead to unsafe control actions regarding the two discussed controllers are presented. The loss scenarios are demonstrated systematically with the following Table 9 and Figures 5 and 6. In Table 6, four reasons for loss scenarios are specified, and the number of loss scenarios that may arise due to these reasons is also mentioned. Figures 5 and 6 illustrate the specified number of loss scenarios and compare their percentage for better understanding.

Table 9. Number of loss scenarios from individual factors.

Loss Scenarios	
Reasons for Loss Scenarios	No. of Loss Scenarios
Physical failure	9
Power failure	8
Sensor failure	29
Flawed algorithm	5

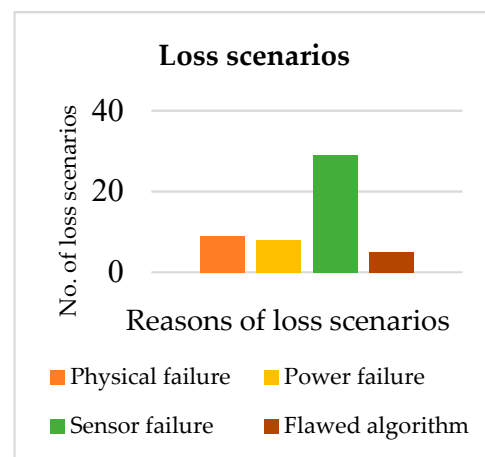


Figure 5. Number of LSs from individual factors.

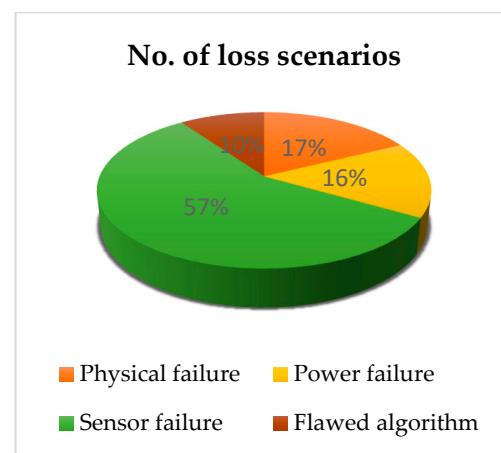


Figure 6. Percentage of LSs from individual factors.

CCU is the controller of the onboard autonomous system and creates UCAs by giving the wrong command to the hydrogen fuel supply. Hence, the major focus of this study is CCU which performs the fully autonomous functions along with the alternative fuel. CCU creates a total of 16 UCAs, where 8 are activated during emergency shutdown activate actions and 8 are during emergency shutdown deactivate or start the vessel actions. The prime reasons for UCAs from CCU are presented in Table 10 in a structured manner.

Table 10. Loss scenarios leading to UCAs from CCU.

Unsafe Control Action ID	No. of UCAs	Reasons for UCAs & Wrong or Not Execution of Control Actions	Loss Scenarios
UCA.CCU.009 (H, H3)	3	(a) Physical failure	LS.HO.009.001: CCU does not activate emergency shutdown when it is required because of the physical damage to the internal system though the fuel or power supply is cut off.
		(b) Power failure	LS.HO.009.002: Due to power failure in the control or internal system, CCU fails to activate emergency shutdown when it is required.
		(c) Wrong execution of the command.	LS.HO.009.003: CCU provides the emergency shutdown command for too long or too short a period due to the wrong execution of the internal system.
UCA.CCU.010 (H1)	3	(a) Power failure	LS.CCU.010.001: Power failure restricts CCU from activating emergency shutdown when it is required.
		(b) Wrong interpretation of the feedback.	LS.CCU.010.002: CCU commands to activate emergency shutdown but the internal valve makes wrong interpretation and does not cut the fuel or power supply.
UCA.CCU.011 (H1)	1	(a) Wrong interpretation	LS.CCU.011.001: CCU provides the wrong command of emergency shutdown by cutting off fuel or power supply due to the wrong interpretation of the feedback
UCA.CCU.012 (H1)	1	(a) Flawed algorithm.	LS.CCU.012.001: CCU provides emergency shutdown without fuel or power supply cut off flawed algorithm of the specified system when shutdown is not required.
UCA.CCU.013 (H1, H3)	2	(a) Controller does not receive feedback.	LS.CCU.013.001: CCU does not start the operation after an emergency shutdown when it is required because CCU does not receive any feedback from the internal sensors.
		(b) Controller receives incorrect feedback.	LS.CCU.013.002: CCU receives wrong feedback and as a result deactivates the emergency shutdown too early when there is a flow of fuel or power supply.
UCA.CCU.014 (H1, H3)	2	(a) Power failure.	LS.CCU.014.001: Due to central power failure, CCU does not start the vessel with the flow of fuel or power supply after an emergency shutdown.
		(b) Physical failure.	LS.CCU.014.002: Due to external damage to the internal system, CCU does not deactivate the emergency shutdown when it is required.
		(c) Controller receives incorrect feedback.	LS.CCU.014.003: CCU deactivates the emergency shutdown too early because it receives the wrong feedback from the internal system.

Table 10. Cont.

Unsafe Control Action ID	No. of UCAs	Reasons for UCAs & Wrong or Not Execution of Control Actions	Loss Scenarios
UCA.CCU.015 (H1)	3	(a) Incorrect execution of the control action.	LS.CCU.015.001: CCU deactivates the emergency shutdown or starts the vessel operation in the emergency shutdown situation with the flow of fuel or power supply because CCU provides the correct information, but the internal actuator responds incorrectly.
UCA.CCU.016 (H1)	1	(a) Incorrect interpretation of the feedback.	LS.CCU.016.001: CCU provides emergency shutdown deactivation, or the vessel operation start command when it is required but fuel or power supply is not started due to the wrong interpretation of the feedback by the storage tank valve.

4. Discussions

This study was conducted to determine major possible UCAs and loss scenarios that derive from STPA risk analysis methods associated with the hydrogen fuel cell propulsion on a third-degree autonomous vessel (remotely operated vessel with no seafarers on board). The purpose was to ensure safety and create reliability by introducing and mitigating the UCAs. Ghaderi [73] concludes with the necessity of advanced technology and competencies to design, build, and operate unmanned vessels. He also indicates the challenges in maintenance, navigation systems, and cyber security. This study analyzes the specific competencies for operation and extends the maintenance area. Specific components are also discussed to implement a risk-free design and cyber security is taken into consideration through STPA.

4.1. STPA Risk Factors

At the very beginning, this analysis introduced a total of eight losses that can evolve from the whole system. After that, five system-level hazards were introduced which led to those losses. As STPA discusses control failure, control actions of human operator/s and autonomous systems are analyzed. The onboard central control unit (CCU) is the main controller of the autonomous system. Two major control actions are analyzed by these controllers. The control actions are (1) speed control and (2) emergency shutdown.

Due to uncontrollable external natural environments, currents, uncertainties, wrong actions, and executions, risks to MASS operations can arise [74]. To reduce this type of uncertainty, speed control plays a vital role. Therefore, speeding up and down was one of the major control actions for this study.

A total of 44 unsafe control actions were identified from the two controllers. Among these, 19 unsafe control actions were determined from the wrong control actions of the human operator (HO) during speed up and speed down and 9 unsafe control actions were identified during emergency shutdown via valve. Sixteen unsafe control actions were identified by the wrong control actions of the central control unit during the emergency shutdown. These unsafe control actions arise due to various loss scenarios. A total of 51 fundamental loss scenarios are discussed which lead to the earlier mentioned UCAs. Most of the reasons behind these loss scenarios are physical failure, power failure, incorrect feedback, wrong interpretation, and so on.

From STPA, all 44 unsafe control actions are potential risks. These UCAs are probable depending on the loss scenarios. Fifty-one loss scenarios presented in the result section are the fundamental loss scenarios that have the highest probability of being directed toward the UCAs. Depending on the circumstances, there can be a huge number of loss scenarios. However, maximum UCAs are related to “providing” the command when not required and “not providing the command” when required or making late or long-

duration commands. These UCAs can lead to five potential hazards. These hazards are related to the “inappropriate propulsion power, collision, loss of intact stability, inactive HO and unauthorized access to the vessel” and arise due to the wrong control actions of HO and CCU.

From the analyses, CCU failure or UCAs of CCU are the potential risks or hazards as they take the primary and majority of the automatic control actions.

From STPA, CCU is analyzed for the emergency shutdown action. During emergency shutdown and deactivation of shutdown or operation start, CCU may command a total of 16 UCAs which are marked with the ID numbers UCA.CCU.009 to UCA.CCU.016. Fourteen loss scenarios are discussed which lead to these UCAs by the CCU. The main reasons for these loss scenarios are (1) physical failure (2), power failure (3), wrong execution of the command by the actuator, (4) wrong interpretation of the feedback (5), flawed algorithm, and (6) controller receives incorrect feedback from the sensors.

Hence, theorizing the analysis, the common reasons for CCU failure, or UCAs of CCU are:

1. Power failure.
2. Wrong or flawed algorithm.
3. Sensor/s failure.

This study combines two novel processes where a recent as well as effective analysis method has been applied that produces more accurate and significant results. The safety analysis of autonomous ships and hydrogen fuel cells with the STPA method creates unique results that need to be considered while implementing this combination. Some unique results are:

- Human operator/s lead to two-thirds of the unsafe control actions compared to the software.
- The addition of CCU is one of the major differences between autonomous vessels and manual vessels. The number of UCAs from CCU and HO related to emergency shutdown is almost similar, even slightly less.
- Most of the UCAs are evolved due to the sensor failure of the autonomous system that must be taken care of with correct monitoring and maintenance.
- Availability of hydrogen fuel supply has a significant role in maintaining adequate safety. Compared to conventional fuel, hydrogen is more prone to leakage. Hence, a lack of hydrogen supply to the fuel cell may arise now and then.
- Analysis with STPA helps to identify all possible control-related failures that are very difficult to detect with the help of conventional methods. Furthermore, traditional methods, for instance, FMEA, focus on hazards from single-component failure whereas STPA focuses on hazards that are caused by and without component failure or multiple-component failure in addition to the single-component failure. For example, H5 of this study is that unauthorized access to the vessel may arise without any component failure.

4.2. Limitations of the Study

The major limitation of this study is the unforeseen hazards that can evolve because of this unique system. The hydrogen fuel cell propulsion system on autonomous vessels is fairly new. Though parts of this whole system are under trial, the whole system is still in the conceptual stage. So, during the trial period or practical operation, unknown hazards may arise. In addition, the power management system plays a vital role in the whole system and power failure is a major detrimental reason for the hazard to the whole system. This study is not sufficient to identify the depth analysis of PMS. Finally, the battery power system also has a significant role in this whole analyzed system. Without battery support, this system cannot be completed. However, a detailed analysis of the battery system is yet to be conducted.

Another limitation is associated with the STPA method. This method is qualitatively prone and needs enough brainstorming. Hence, quantification of the losses is challenging.

Moreover, even though STPA has been shown to identify possible accident causes, they have not been demonstrated in controlled experiments [72]. The method also needs a huge team of experts for the execution [75].

5. Conclusions

This study explores possible control failure-related risk factors associated with hydrogen fuel cell propulsion on autonomous vessels using a system-based hazard analysis method. The aim was to provide sufficient operational safety and create reliability, which is one of the challenges because of the wide acceptance of hydrogen fuel cell propulsion autonomous vessels by a group of stakeholders based on this point.

UCAs related to two major control actions, “emergency shutdown and speed control”, have been manifested with the aid of the STPA analysis method. UCAs take place mostly when an action needs to be provided but it is not provided and vice versa. Power or fuel supply also plays an important role, especially when there is no or inadequate fuel or power supply. The identified control action failures arise due to some particular loss scenarios that obstruct the execution of the specific control actions. Apart from physical failure, other loss scenarios are mostly technical such as sensor failure, incorrect feedback, flawed algorithm, etc. UCAs evolving from HO at RCC are foreseeable and some unforeseen hazards with the addition of CCU can be overcome with strict monitoring, maintenance, and awareness. In some cases, redundancy is quite an effective remedy. The result of the study shows that compared to the conventional vessel and fuel, an autonomous vessel with a hydrogen fuel cell is also acceptable but needs additional training and awareness for the operators from RCC.

Normally, traditional, and established methods have been mandated or recommended for risk analysis of autonomous vessels, and the use of the STPA method has been limited to academia only. However, the 107th Maritime Safety Committee (MSC) in 2023 agreed to allow flexible use of various risk analysis methods for autonomous ships, so this study is expected to open the door to apply it in the maritime industry.

Further research on the same framework can make the whole system more widely reliable and acceptable. For example,

- The study is fully qualitative. So, with the availability of sufficient specific data and other convenient methods (such as Failure Mode and Effect Analysis, Fault Tree Analysis, Event Tree Analysis, and so on), quantitative analysis can be conducted to quantify the UCAs based on the intensity of hazards and establish numerical loss scenarios.
- As the whole system is also strongly dependent on the battery system, in-depth quantitative as well as qualitative risk analysis is required further for the battery application as a part of the whole system.
- The use of liquid hydrogen as an alternative fuel and hydrogen fuel cell for autonomous ships require more focus on analyzing individual components and sub-components to create adequate and subsequent safety.
- For hydrogen fuel cell propulsion vessels, a bunker station in the designated port is solely required. A lot of known and unknown risk factors can evolve during the bunker operation. Hence, risk analysis for the establishment of hydrogen fuel stations and bunker operations is important.
- “Pilot” operation plays a significant role for the autonomous vessel. Pilotage operation can be safer and acceptable with the combined analysis of HAZID and STPA.

Author Contributions: M.M.A.S.: plan for the whole paper. Introduction, methodology, data collection, analysis, result, discussion, writing. H.K.: methodology, review and editing, discussion, supervision. S.N. and C.C.: project administration, validation. E.K.: data curation, validation. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are grateful for the research and publication support from the Development of Autonomous Ship Technology project (20200615), funded by the Ministry of Oceans and Fisheries of Korea. The APC is also funded by the same project.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article and further inquiries can be directed to the corresponding author.

Acknowledgments: We are grateful to the “Corvus Energy” company and its hydrogen fuel cell project members for their unparalleled support to make this study more valid and convenient.

Conflicts of Interest: Author Elisabeth Kjøsberg was employed by the “Corvus Energy” company. The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish results.

Appendix A

In this section, the entire analysis along with the structured presentation of the analysis is represented.

Identifying Unsafe Control Actions by STPA Analysis

Controller: Human Operator									
ID	Control Action	Condition		Unsafe Control Actions					
		Speed Up Needed	Speed Up Feasible	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.HO.001	Speed up	Yes	Yes	Unsafe (H2)	Safe	Unsafe (H2)	Unsafe (H2)	N/A	N/A
CA.HO.002		Yes	No	Unsafe (H2)	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A
CA.HO.003		No	Yes	Safe	Unsafe (H2)	Unsafe (H2)	N/A	N/A	N/A
CA.HO.004		No	No	Safe	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A
Controller: Human Operator									
ID	Control Action	Condition		Unsafe Control Actions					
		Speed Down Needed	Energy or Power Supply	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.HO.005	Speed down	Yes	Increase	Unsafe (H2)	Unsafe (H1)	Unsafe (H1)	N/A	N/A	Unsafe (H1)
CA.HO.006		Yes	Decrease	Unsafe (H2)	Safe	Unsafe (H3)	N/A	N/A	N/A
CA.HO.007		No	Increase	Safe	Unsafe (H2)	N/A	N/A	N/A	N/A
CA.HO.008		No	Decrease	Safe	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A
Controller: CCU									
ID	Control Action	Condition		Unsafe Control Actions					
		Activation Required	Fuel or Power Supply Cut Off?	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.HO.009	Emergency shutdown activate	Yes	Yes	Unsafe (H1)	Safe	N/A	N/A	Unsafe (H1)	Unsafe (H3)
CA.HO.010		Yes	No	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A	Unsafe (H1)
CA.HO.011		No	Yes	Safe	Unsafe (H1)	N/A	N/A	N/A	N/A
CA.HO.012		No	No	Safe	Unsafe (H3)	N/A	N/A	N/A	N/A

Controller: CCU									
ID	Control Action	Condition		Unsafe Control Actions					
		Deactivation Required	Fuel or Power Supply Flow?	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.HO.013	Emergency shutdown deactivate or start the vessel	Yes	Yes	Unsafe (H3)	Safe	Unsafe (H1)	N/A	N/A	N/A
CA.HO.014		Yes	No	Unsafe (H3)	Unsafe (H1)	N/A	N/A	N/A	N/A
CA.HO.015		No	Yes	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A	Unsafe (H1)
CA.HO.016		No	No	Safe	Unsafe (H1)	N/A	N/A	N/A	N/A
Controller: Human Operator									
ID	Control Action	Condition		Unsafe Control Actions					
		Shutdown Is Required?	Fuel Supply Cut Off??	Not Provided	Provided	Too Early	Too Late	Too Short	Too Long
CA.HO.017	Emergency shutdown directly via valve.	Yes	Yes	Unsafe (H1)	Safe	N/A	N/A	Unsafe (H1)	Unsafe (H3)
CA.HO.018		Yes	No	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A	Unsafe (H1)
CA.HO.019		No	Yes	Unsafe (H1)	Unsafe (H1)	N/A	N/A	N/A	N/A
CA.HO.020		No	No	Safe	Unsafe (H3)	N/A	N/A	N/A	N/A

Unsafe control actions: All the unsafe control actions that are determined from the above systematic identification table are mentioned in full sentences with UCAs code.

UCA.HO.001:

- Human operator does not provide the speed-up command when speed-up is required within a feasible context. (H2, H5).
- Human operator provides the speed-up command too early when speed-up is required within a feasible context. (H2).
- Human operator provides the speed-up command after a long-time delay when speed-up is required within a feasible context. (H2)

UCA.HO.002

- Human operator does not provide the speed-up command when speed-up is required but speed-up is not feasible. (H2)
- Human operator provides the speed-up command when speed-up is required but speed-up is not feasible. (H1)
- Human operator provides the speed-up command too early when speed-up is required but speed-up is not feasible. (H1)

UCA.HO.003

- Human operator provides the speed-up command when speed-up is not required within a feasible context. (H2).
- Human operator provides the speed-up command too early when speed-up is not required within a feasible context. (H2).

UCA.HO.004

- Human operator provides the speed-up command when speed-up is not required and feasible. (H1)
- Human operator provides the speed-up command too early when speed-up is not required and feasible. (H1)

UCA.HO.005

- Human operator does not provide the speed-down command when speed-down is required and energy or power supply is increased. (H2)

- Human operator provides the speed-down command when speed-down is required but energy or power supply is increased. (H1)
- Human operator provides the speed-down command too early by increasing energy or power supply when speed-down is required. (H1)
- Human operator provides the speed-down command for a long time by increasing energy or power supply when speed-down is required. (H1)

UCA.HO.006

- Human operator does not provide the speed-down command by decreasing energy or power supply when speed-down is required. (H2)
- Human operator provides the speed-down command too early by decreasing energy or power supply when speed-down is required. (H3)

UCA.HO.007

- Human operator provides the speed-down command by increasing energy or power supply when speed-down is not required. (H2)

UCA.HO.008

- Human operator provides the speed-down command by decreasing energy or power supply when speed down is not required. (H1)
- Human operator provides the speed-down command too early by decreasing energy or power supply when speed-down is not required. (H1)

UCA.CCU.009

- Central control unit does not provide emergency shutdown activation when the activation is required, and fuel or power supply is also cut off. (H1)
- Central control unit provides emergency shutdown activation for a too short period when the activation is required, and fuel or power supply is also cut off. (H1)
- Central control unit provides emergency shutdown activation for a too long period when the activation is required, and fuel or power supply is also cut off. (H3)

UCA.CCU.010

- Central control unit does not provide emergency shutdown activation when the activation is required and also fuel, or power supply is not cut off. (H1)
- Central control unit provides emergency shutdown activation when the activation is required but fuel or power supply is not cut off. (H1)
- Central control unit provides emergency shutdown activation for a too long period when the activation is required, and fuel or power supply is also not cut off. (H1)

UCA.CCU.011

- Central control unit provides emergency shutdown activation by fuel or power supply cut off when the activation is not required. (H1)

UCA.CCU.012

- Central control unit provides emergency shutdown activation when the activation is not required, and fuel or power supply is also not cut off. (H1)

UCA.CCU.013

- Central control unit does not provide emergency shutdown deactivation or start the vessel when deactivation is required and there is a flow of fuel or power supply. (H3)
- Central control unit provides emergency shutdown deactivation command too early when deactivation is required and there is a flow of fuel or power supply. (H1)

UCA.CCU.014

- Central control unit does not provide emergency shutdown deactivation command or start the vessel when deactivation is required and also there is no flow of fuel or power supply. (H3)

- Central control unit provides emergency shutdown deactivation or starts the vessel when deactivation is required but there is no flow of fuel or power supply. (H1)
UCA.CCU.015
- Central control unit does not provide emergency shutdown deactivation or start the vessel when deactivation is not required but there is a flow of fuel or power supply. (H1)
- Central control unit provides emergency shutdown deactivate or start the vessel when deactivation is not required and also there is a flow of fuel or power supply. (H1)
- Central control unit provides emergency shutdown deactivation or starts the vessel for a too long period when deactivation is not required and there is a flow of fuel or power supply. (H1)
UCA.CCU.016
- Central control unit provides emergency shutdown deactivation or start the vessel when deactivation is not required and there is no flow of fuel or power supply. (H1)
UCA.HO.017
- Human operator does not provide emergency shutdown command directly via valve when shutdown is required, and fuel supply is also cut off. (H1)
- Human operator provides emergency shutdown command directly via valve for a too short period when shutdown is required, and fuel supply is also cut off. (H1)
- Human operator provides emergency shutdown command directly via valve for a too long period when shutdown is required, and fuel supply is also cut off. (H3)
UCA.HO.018
- Human operator does not provide emergency shutdown command directly via valve when shutdown is required, and fuel supply is also not cut off. (H1)
- Human operator provides emergency shutdown command directly via valve when shutdown is required but fuel supply is not cut off. (H1)
- Human operator provides emergency shutdown command directly via valve for a too long period when shutdown is required, and fuel supply is also not cut off. (H1)
UCA.HO.019
- Human operator does not provide emergency shutdown command directly via valve and shutdown also is not required but fuel supply is also cut off. (H1)
- Human operator provides emergency shutdown command directly via valve when shutdown is not required, and fuel supply is also cut off. (H1)
UCA.HO.020
- Human operator provides emergency shutdown command directly via valve when shutdown is not required, and fuel supply is also not cut off. (H3)

References

1. IMO. IMO Takes First Steps to Address Autonomous Ships. Available online: <https://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-mass-scoping.aspx> (accessed on 3 August 2023).
2. LR. ShipRight Design and Construction. Liod's Register. Available online: <https://www.lr.org/en/knowledge/shipright/procedures/> (accessed on 26 July 2023).
3. Sheridan, T.; Verplank, W.; Brooks, T. Human and Computer Control of Undersea Teleoperators. December 1978. Available online: https://www.researchgate.net/publication/23882567_Human_and_Computer_Control_of_Undersea_Teleoperators (accessed on 26 July 2023).
4. IMO. Autonomous Ships: Regulatory Scoping Exercise Completed. Available online: <https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx> (accessed on 10 May 2023).
5. Heij, C.; Knapp, S. Predictive power of inspection outcomes for future shipping accidents—An empirical appraisal with special attention for human factor aspects. *Marit. Policy Manag.* **2018**, *45*, 604–621. [CrossRef]
6. Burmeister, H.-C.; Bruhn, W.C.; Rødseth, Ø.J.; Porathe, T. Can Unmanned Ships Improve Navigational Safety? 2014. Available online: https://folk.ntnu.no/thomaspo/webbprofil/hfunmanned/TRA2014_Fpaper_17909.pdf (accessed on 3 August 2023).

7. Burmeister, H.-C.; Bruhn, W.; Rødseth, Ø.J.; Porathe, T. Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective. *Int. J. E-Navig. Marit. Econ.* **2014**, *1*, 1–13. [CrossRef]
8. Komianos, A. The Autonomous Shipping Era. Operational, Regulatory, and Quality Challenges. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2018**, *12*, 335–348. Available online: http://www.transnav.eu/Article_The_Autonomous_Shipping_Era_Operational_Regulatory_and_Quality_Challenges_Komianos,46,818.html (accessed on 3 August 2023). [CrossRef]
9. Knowledge Group. Yara Birkeland. The First Zero Emission, Autonomous Ship. Yara International. Yara None. Available online: <https://www.yara.com/knowledge-grows/game-changer-for-the-environment/> (accessed on 3 August 2023).
10. Jalonen, R.; Tuominen, R.; Wahlström, M. Safety and security in autonomous shipping: Challenges for research and development. In *Remote and Autonomous Ship*; AAWA: London, UK, 2016. Available online: <http://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf> (accessed on 3 August 2023).
11. Zhou, X.-Y.; Liu, Z.-J.; Wang, F.-W.; Wu, Z.-L. A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Eng.* **2021**, *222*, 108569. [CrossRef]
12. Vakil, S.S. Overview of Autonomous Ships Classification. *J. Inst. Eng. India Ser. C* **2022**, *103*, 889–893. [CrossRef]
13. Yang, R.; Vatn, J.; Utne, I.B. Dynamic maintenance planning for autonomous marine systems (AMS) and operations. *Ocean Eng.* **2023**, *278*, 114492. [CrossRef]
14. Wróbel, K.; Montewka, J.; Kujala, P. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliab. Eng. Syst. Saf.* **2018**, *178*, 209–224. [CrossRef]
15. IMO. IMO and the Republic of Korea Symposium on IMO MASS Code. Available online: <https://www.imo.org/en/About/Events/Pages/IMO-MASS-Code-Symposium.aspx> (accessed on 31 July 2023).
16. Mandra, J.O. Japan Takes Its Autonomous Shipping to the Next Level. Offshore Energy. Available online: <https://www.offshore-energy.biz/japan-takes-its-autonomous-shipping-to-the-next-level/> (accessed on 3 August 2023).
17. Haworth, C.; Evans, J.; Ji, Z.; Taylor, R.; Martin, D. An open software framework for adaptive, autonomous operation of maritime autonomous systems. In Proceedings of the OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, USA, 19–23 September 2016; pp. 1–7. [CrossRef]
18. Norris, J.N. Human Factors in Military Maritime and Expeditionary Settings: Opportunity for Autonomous Systems? In *Advances in Human Factors in Robots and Unmanned Systems*; Chen, J., Ed.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2018; pp. 139–147. [CrossRef]
19. Porathe, T.; Hoem, Å.; Rødseth, Ø.; Fjortoft, K.; Johnsen, S.O. At least as safe as manned shipping? Autonomous shipping, safety and “human error”. In *Safety and Reliability—Safe Societies in a Changing World*; CRC Press: Boca Raton, FL, USA, 2018. Available online: <https://www.taylorfrancis-com.ezproxy2.usn.no/chapters/oa-edit/10.1201/9781351174664-53/computerized-procedure-system-framework-utilities-lew-boring-ulrich?context=ubx> (accessed on 19 February 2023).
20. Hagaseth, M.; Jan Rødseth, Ø.; Meland, P.H.; Wille, E.; Murray, B.; Meling, P. Methodology for Approval of Autonomous Ship Systems CONOPS. Zenodo (CERN European Organization for Nuclear Research). June 2022. Available online: https://www.academia.edu/109255625/Methodology_for_Approval_of_Autonomous_Ship_Systems_CONOPS (accessed on 20 February 2024).
21. Rødseth, Ø.J.; Wennersberg, L.A.L.; Nordahl, H. Towards approval of autonomous ship systems by their operational envelope. *J. Mar. Sci. Technol.* **2022**, *27*, 67–76. [CrossRef] [PubMed]
22. Chang, C.-H.; Wijeratne, I.B.; Kontovas, C.A.; Yang, Z. COLREG and MASS: Analytical review to identify research trends and gaps in the Development of Autonomous Collision Avoidance. *Ocean Eng.* **2024**, *302*, 117652. [CrossRef]
23. Tjora, Å. A risk-based approach to the design of unmanned ship control systems. In *Maritime-Port Technology and Development*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2014. Available online: <https://www.taylorfrancis-com.ezproxy2.usn.no/chapters/edit/10.1201/b17517-20/risk-based-approach-design-unmanned-ship-control-systems-r%C3%B8dseth-tjora> (accessed on 11 February 2023).
24. IMO. Autonomous Shipping. Available online: <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx> (accessed on 24 February 2023).
25. Fan, C.; Wróbel, K.; Montewka, J.; Gil, M.; Wan, C.; Zhang, D. A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. *Ocean Eng.* **2020**, *202*, 107188. [CrossRef]
26. Chae, C.-J.; Kim, M.; Kim, H.-J. A study on identification of development status of MASS technologies and directions of improvement. *Appl. Sci.* **2020**, *10*, 4564. [CrossRef]
27. Ventikos, N.P.; Chmurski, A.; Louzis, K. A systems-based application for autonomous vessels safety: Hazard identification as a function of increasing autonomy levels. *Saf. Sci.* **2020**, *131*, 104919. [CrossRef]
28. Veitch, E.; Alsos, O.A. A systematic review of human-AI interaction in autonomous ship systems. *Saf. Sci.* **2022**, *152*, 105778. [CrossRef]
29. Jokioinen, E. *Remote and Autonomous Ships: The Next Steps*; AAWA: Advanced Autonomous Waterborne Applications, Rolls-Royce: London, UK, 2016.
30. Wróbel, K.; Montewka, J.; Kujala, P. System-theoretic approach to safety of remotely-controlled merchant vessel. *Ocean Eng.* **2018**, *152*, 334–345. [CrossRef]
31. Chang, C.-H.; Kontovas, C.; Yu, Q.; Yang, Z. Risk assessment of the operations of maritime autonomous surface ships. *Reliab. Eng. Syst. Saf.* **2021**, *207*, 107324. [CrossRef]

32. NMA. Guidance in Connection with the Construction or Installation of Automated Functionality Aimed at Performing Unmanned or Partially Unmanned Operations—Norwegian Maritime Authority. Available online: <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/> (accessed on 3 April 2023).
33. EMSA. Risk Based Assessment Tool (RBAT). Available online: <https://emsa.europa.eu/mass/rbat.html> (accessed on 3 April 2023).
34. Asariotis, R.; Assaf, M.; Benamara, H.; Hoffmann, J. *Review of Maritime Transport 2018*; United Nations: New York, NY, USA; Geneva, Switzerland, 2018. Available online: https://unctad.org/system/files/official-document/rmt2018_en.pdf (accessed on 26 July 2023).
35. Müller-Casseres, E.; Edelenbosch, O.Y.; Szklo, A.; Schaeffer, R.; van Vuuren, D.P. Global futures of trade impacting the challenge to decarbonize the international shipping sector. *Energy* **2021**, *237*, 121547. [CrossRef]
36. IMO. Revised GHG Reduction Strategy for Global Shipping Adopted. Available online: <https://www.imo.org/en/MediaCentre/PressBriefings/pages/Revised-GHG-reduction-strategy-for-global-shipping-adopted-.aspx> (accessed on 31 July 2023).
37. Valentin, L. Different Ways to Reduce CO₂ Emissions from Sea Freight. Available online: <https://sinay.ai/en/different-ways-to-reduce-co2-emissions-from-sea-freight/> (accessed on 4 August 2023).
38. DNV. Alternative Fuels: The Options—DNV. DNV GL. Available online: <https://www.dnv.com/expert-story/maritime-impact/alternative-fuels/> (accessed on 11 February 2023).
39. Foretich, A.; Zaimes, G.G.; Hawkins, T.R.; Newes, E. Challenges and opportunities for alternative fuels in the maritime sector. *Marit. Transp. Res.* **2021**, *2*, 100033. [CrossRef]
40. Ustolin, F.; Campari, A.; Taccani, R. An Extensive Review of Liquid Hydrogen in Transportation with Focus on the Maritime Sector. *J. Mar. Sci. Eng.* **2022**, *10*, 1222. [CrossRef]
41. Cotrell, J.; Pratt, W. *Modeling the Feasibility of Using Fuel Cells and Hydrogen Internal Combustion Engines in Remote Renewable Energy Systems*; NREL/TP-500-34648; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2003. [CrossRef]
42. Dincer, I.; Rosen, M.A. Sustainability aspects of hydrogen and fuel cell systems. *Energy Sustain. Dev.* **2011**, *15*, 137–146. [CrossRef]
43. American Bureau of Shipping. Fuel Cell Power Systems for Marine and Offshore Applications. 2019. Available online: <https://img.fuelcellworks.com/wp-content/uploads/2019/12/Fuel-Cell-Power-Systems-For-Marine-and-Offshore-Applications.pdf> (accessed on 12 February 2023).
44. Vogler, F.; Würsig, G. New Developments for Maritime Fuel Cell Systems. In Proceedings of the 18th World Hydrogen Energy Conference 2010—WHEC 2010, Essen, Germany, 19 May 2010. Available online: https://user.fz-juelich.de/record/135685/files/SM3_3_Vogler.pdf (accessed on 6 February 2023).
45. Xu, X.-J.; Yang, R.; Ji, Y.-B.; Zhang, X.-Y.; Jiang, L.; Li, K. Review on key technologies of hydrogen fuel cell powered vessels. *Jiaotong Yunshu Gongcheng Xuebao J. Traffic Transp. Eng.* **2022**, *22*, 47–67. [CrossRef]
46. Hansen, S.Ø. #PoweredByBallard: The First Hydrogen-Powered Vessels Set Sail. Ballard. Available online: <https://blog.ballard.com/marine/first-hydrogen-powered-vessels-marine> (accessed on 26 July 2023).
47. IRENA. Renewable Energy Statistics 2022. Available online: <https://www.irena.org/publications/2022/Jul/Renewable-Energy-Statistics-2022> (accessed on 2 April 2023).
48. Wijayanta, A.T.; Oda, T.; Purnomo, C.W.; Kashiwagi, T.; Aziz, M. Liquid hydrogen, methylcyclohexane, and ammonia as potential hydrogen storage: Comparison review. *Int. J. Hydrogen Energy* **2019**, *44*, 15026–15044. [CrossRef]
49. IREANA. Geopolitics of the Energy Transformation: The Hydrogen Factor. Available online: <https://www.irena.org/publications/2022/Jan/Geopolitics-of-the-Energy-Transformation-Hydrogen> (accessed on 4 May 2023).
50. Aarskog, F.G.; Hansen, O.R.; Strømgren, T.; Ulleberg, Ø. Concept risk assessment of a hydrogen driven high speed passenger ferry. *Int. J. Hydrogen Energy* **2020**, *45*, 1359–1372. [CrossRef]
51. IMO. International Code of Safety for Ship Using Gases or Other Low-Flashpoint Fuels (IGF Code). Available online: <https://www.imo.org/en/OurWork/Safety/Pages/IGF-Code.aspx> (accessed on 27 April 2023).
52. Cui, S.; Zhu, G.; He, L.; Wang, X.; Zhang, X. Analysis of the fire hazard and leakage explosion simulation of hydrogen fuel cell vehicles. *Therm. Sci. Eng. Prog.* **2023**, *41*, 101754. [CrossRef]
53. Shen, Y.; Lv, H.; Hu, Y.; Li, J.; Lan, H.; Zhang, C. Preliminary hazard identification for qualitative risk assessment on onboard hydrogen storage and supply systems of hydrogen fuel cell vehicles. *Renew. Energy* **2023**, *212*, 834–854. [CrossRef]
54. Groth, K.; Hecht, E.; Reynolds, J.T.; Blaylock, M.L.; Carrier, E.E. *Methodology for Assessing the Safety of Hydrogen Systems: HyRAM; 1.1 Technical Reference Manual*; SAND2017-2998; Sandia National Lab. (SNL-NM): Albuquerque, NM, USA; Livermore, CA, USA, 2017. [CrossRef]
55. Yuan, Y.-P.; Cui, W.-Y.; Shen, H.; Zou, Z.-X.; Guo, W.Y. Numerical simulation of leakage and diffusion of hydrogen in cabin of fuel cell ship. *J. Transp. Eng.* **2022**, *22*, 196–209. [CrossRef]
56. Balestra, L.; Yang, R.; Schjøberg, I.; Utne, I.B.; Ulleberg, Ø. *Towards Safety Barrier Analysis of Hydrogen Powered Maritime Vessels*; ASME: New York, NY, USA, 2021. [CrossRef]
57. Giannissi, S.G.; Venetsanos, A.G. Study of key parameters in modeling liquid hydrogen release and dispersion in open environment. *Int. J. Hydrogen Energy* **2018**, *43*, 455–467. [CrossRef]
58. Winters, W.S. *Modeling Leaks from Liquid Hydrogen Storage Systems*; SAND2009-0035; Sandia National Laboratories (SNL): Albuquerque, NM, USA; Livermore, CA, USA, 2009. [CrossRef]

59. Millet, P. 14—Hydrogen storage in hydride-forming materials. In *Advances in Hydrogen Production, Storage and Distribution*; Basile, A., Iulianelli, A., Eds.; Woodhead Publishing: Sawston, UK, 2014; pp. 368–409. [\[CrossRef\]](#)
60. Jovanović, I.; Vladimir, N.; Perčić, M.; Koričan, M. The feasibility of autonomous low-emission ro-ro passenger shipping in the Adriatic Sea. *Ocean Eng.* **2022**, *247*, 110712. [\[CrossRef\]](#)
61. NIST. NIST Chemistry WebBook. Available online: <https://webbook.nist.gov/chemistry/> (accessed on 26 July 2023).
62. DNV. Rules and Standards Explorer. Available online: <https://standards.dnv.com/explorer/> (accessed on 28 April 2023).
63. Leveson, N.G.; Thomas, J.P. *STPA Handbook*; MIT Partnership for Systems Approaches to Safety and Security (PSASS): Cambridge, MA, USA, 2018.
64. Chaal, M.; Banda, O.A.V.; Glomsrud, J.A.; Basnet, S.; Hirdaris, S.; Kujala, P. A framework to model the STPA hierarchical control structure of an autonomous ship. *Saf. Sci.* **2020**, *132*, 104939. [\[CrossRef\]](#)
65. Leveson, N.G. *Engineering a Safer World: Systems Thinking Applied to Safety*; The MIT Press: Cambridge, MA, USA, 2016. Available online: <https://library.oapen.org/handle/20.500.12657/26043> (accessed on 19 February 2023).
66. Salmon, P.M.; Cornelissen, M.; Trotter, M. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Saf. Sci.* **2012**, *50*, 1158–1170. [\[CrossRef\]](#)
67. Banda, O.A.V.; Goerlandt, F. A STAMP-based approach for designing maritime safety management systems. *Saf. Sci.* **2018**, *109*, 109–129. [\[CrossRef\]](#)
68. Castilho, D.S.; Urbina, L.M.S.; de Andrade, D. STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs. *Saf. Sci.* **2018**, *108*, 129–139. [\[CrossRef\]](#)
69. Aps, R.; Fetissov, M.; Goerlandt, F.; Kujala, P.; Piel, A. Systems-Theoretic Process Analysis of Maritime Traffic Safety Management in the Gulf of Finland (Baltic Sea). *Procedia Eng.* **2017**, *179*, 2–12. [\[CrossRef\]](#)
70. Zhou, X.-Y.; Liu, Z.-J.; Wang, F.-W.; Wu, Z.-L.; Cui, R.-D. Towards applicability evaluation of hazard analysis methods for autonomous ships. *Ocean Eng.* **2020**, *214*, 107773. Available online: <https://trid.trb.org/view/1732545> (accessed on 2 May 2023). [\[CrossRef\]](#)
71. Paltrinieri, N.; Tugnoli, A.; Buston, J.; Wardman, M.; Cozzani, V. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. *J. Loss Prev. Process Ind.* **2013**, *26*, 683–695. [\[CrossRef\]](#)
72. Harkleroad, E.P.; Vela, A.E.; Kuchar, J.K. Review of Systems-Theoretic Process Analysis (STPA) Method and Results to Support NextGen Concept Assessment and Validation. MIT Lincoln Laboratory. Available online: <https://www.ll.mit.edu/r-d/publications/review-systems-theoretic-process-analysis-stpa-method-and-results-support-nextgen> (accessed on 4 December 2022).
73. Ghaderi, H. Autonomous technologies in short sea shipping: Trends, feasibility and implications. *Transp. Rev.* **2018**, *39*, 152–173. [\[CrossRef\]](#)
74. Li, X.; Oh, P.; Zhou, Y.; Yuen, K.F. Operational risk identification of maritime surface autonomous ship: A network analysis approach. *Transp. Policy* **2023**, *130*, 1–14. [\[CrossRef\]](#)
75. Bensaci, C.; Zennir, Y.; Pomorski, D.; Innal, F.; Liu, Y.; Tolba, C. STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison. *Alex. Eng. J.* **2020**, *59*, 3799–3816. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.