Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27865-cd

Analyzing Interaction Hazards of Battery-Electric Ferries and Hydrogen Fuel Cell Vehicles Using STPA

Donghun Lee, Yiliu Liu and Hyungju Kim

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Norway. E-mail: donghun.lee@ntnu.no

The transportation sector, like many industries, is working to meet the United Nations (UN) net-zero target by 2050. One promising solution is using alternative energy sources, such as hydrogen, batteries, ammonia, and methanol. These solutions introduce hazards distinct from traditional fossil fuels that become increasingly complex when diverse transport modes utilizing unique energy sources operate within shared physical environments. While safety research on individual zero-emission modes is extensive, the interactive risks arising from the convergence of these technologies remain poorly understood. This paper addresses the safety of battery-electric ferries transporting Hydrogen Fuel Cell Vehicles (HFCVs). This research employs System-Theoretic Process Analysis (STPA) to analyze a high-risk Simultaneous Operations (SIMOPs) scenario involving the concurrent loading of an HFCV and shore-side high-voltage charging. The analysis reveals complex interactions involving the ferry's Integrated Bridge System, the shore-side charging controller, and the deck crew. Identified loss scenarios include an HFCV hydrogen leak caused by a vehicle collision during loading. Other scenarios trigger cascading failures, such as when electric arcing from a shoreside charger ignites hydrogen being vented from an HFCV, leading to a catastrophic hazard event. Based on these findings, this study proposes safety guidelines to mitigate these loss scenarios.

Keywords: STPA, Simultaneous Operations, Battery-Electric Ferry, Hydrogen Fuel Cell Vehicle, Risk Analysis, System Safety.

1. Introduction

The transportation sector is transitioning to alternative energy sources to reach the UN net-zero target by 2050 (United Nations, 2025). While adopting high-capacity batteries and hydrogen fuel cells reduces emissions, these carriers introduce safety challenges distinct from fossil fuels, especially when different modes share physical environments. In Norway, battery-electric ferries and hydrogen fuel cell vehicles (HFCVs) are increasingly operational, yet their safety during Simultaneous Operations (SIMOPs) requires urgent analysis.

Current ferry electrification research establishes frameworks for power architecture but acknowledges specific constraints. (Karimi et al., 2020) observed that high-power charging architectures lack comprehensive modeling regarding the complex interactions between shore-side energy management and onboard control functions. This is compounded by regulatory challenges, as (Hsu et al., 2024) identified that the technical complexity of IEC/IEEE 80005-1 standards often leads to operational standard-blindness where crews fail to maintain safety during high-voltage connections. Safety assessments by (Wang et al., 2020) highlighted that traditional tools like Fault Tree Analysis (FTA) struggle with the uncertainty of fire propagation in non-standard battery layouts, while (Johnsen et al., 2022) explicitly described Hazard Identification (HAZID) based approaches as brittle when addressing non-failsafe situations in automated systems where situational awareness is absent. These studies confirm that current maritime electrification research remains component-centric and lacks the capacity to model the dynamic system-wide interactions essential for safe operations.

The safety profile of HFCVs is defined by high-pressure storage and unique combustion characteristics that have been modeled through consequence analysis and physical testing. (Zhu et al., 2025) used quantitative risk assessment to identify jet fires as primary threats in confined spaces but noted that findings are constrained by fixed ventilation scenarios and the omission of dynamic safety system failures. (Cui et al., 2023) pinpointed supply pipelines and valves as critical failure nodes, while admitting that simplified leakage models fail to account for complex thermal interactions with surrounding structural infrastructure. This is supported by (Tamura et al., 2014), who investigated fire spread between vehicles and noted that the exclusion of forced ventilation systems represents a significant gap in maritime safety assessments. However, these studies typically treat the vehicle as an isolated unit within static environments and do not manage initial thermal triggers in complex multi-energy settings as noted by (Han et al., 2024) and (Halder et al., 2024).

Effective SIMOPs management is critical, yet current methodologies fail to address system interactivity. (Fan et al., 2021) synthesized risk analysis tools and observed that existing research treats simultaneous activities as parallel rather than interactive, which prevents an accurate understanding of how a failure in one operation alters the risk profile of another. Procedural constraints are also evident as (Baybutt, 2017) demonstrated that traditional siloed techniques often miss complex software or control-logic failures and remain heavily dependent on the experience of the review team. These findings indicate that while SIMOPs management is maturing, the current approaches are frequently static.

This research applies System-Theoretic Process Analysis (STPA) to evaluate risks during concurrent shore charging and HFCVs loading. By using the System-Theoretic Accident Model and Processes (STAMP) model, this study treats safety as a control problem to identify Unsafe Control Actions (UCAs) and loss scenarios stemming from interactions between battery charging interfaces and hydrogen storage.

2. System Description

The adoption of battery-electric ships and HFCVs introduces distinct energy storage mechanisms, such as lithium-ion batteries and high-pressure gas tanks. While individually regulated, integrating these technologies within a shared environment creates a complex safety landscape that necessitates detailed analysis.

To maintain high service frequency on the busy Moss–Horten route, the ferry must minimize quay time by charging its batteries concurrently with vehicle loading and unloading. While this SIMOPs approach is essential for logistical viability, it introduces safety risks by placing high-power electrical activities in close proximity to passenger vehicles.

The MF Bastø Electric is a large fully electric roll-on/roll-off passenger ferry with a 4,300 kWh battery capacity, and its detailed specifications and images are provided in Table 1. Primary technical risks include lithium-ion battery thermal runaway, which causes self-sustaining exothermic states and toxic gas release, and the 7 to 9 MW high-voltage charging infrastructure that can trigger ignition through arcing or component failure during docking.

Table 1. Specification of MF Bastø Electric, (Uavpic, 2022)

Type	Ro-Ro/Passenger Ship
Delivered year	2021
Length (p.p)	144 m
Breadth	20.7 m
Draught	5 m
Gross tonnage	7911 t
Passenger capacity	600
Car capacity	200
Battery capacity	4,300 kWh

HFCVs such as the Hyundai NEXO and Toyota Mirai utilize reinforced tanks to store hydrogen gas at 700 bar, posing risks associated with its small molecular size and wide flammability range. Given that hydrogen is invisible and odorless, any leakage during loading near high-power ferry charging infrastructure could result in ignition from electrical discharges or high-temperature surfaces, making the prevention of hazardous control actions essential during SIMOPs.

3. Methodology

This study utilizes STPA, treating safety as a dynamic control problem rather than a linear chain of failure events. STPA is ideal for multi-energy SIMOPs because it captures risks in software-intensive socio-technical systems where traditional methods often fail. As shown in Figure 1, the analysis follows a four-step procedure based on the STPA Handbook (Leveson & Thomas, 2018): (1) defining losses and hazards to derive safety constraints; (2) modeling the hierarchical control structure through feedback loops; (3) identifying UCAs within their operational context to establish behavioral constraints; and (4) identifying loss scenarios and their causal factors.

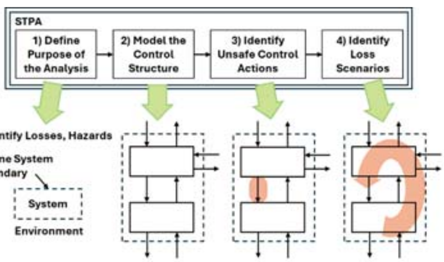

Figure 1. Overview of the basic STPA Method, Adapted from Leveson and Thomas, 2018

4. Results

The application of STPA to the MF Bastø Electric and HFCVs reveals the complex interactions that influence safety. The Results section details the outcomes of applying each STPA step to the target system.

4.1. *Identifying losses and system level hazards*

This analysis defines the following fundamental losses to establish the foundation for subsequent hazard analysis and safety constraint identification.

- L-1 Loss of life or injury to people
- L-2 Loss of or damage to physical assets
- L-3 Loss of operational continuity or mission
- L-4 Environmental loss or pollution

Based on the identified losses, the hazards for the target system are defined as follows.

- H-1: [The integrated ferry-vehicle system] [contains hydrogen gas concentrations exceeding the Lower Explosive Limit (LEL) within the semi-enclosed deck] [during SIMOPs] [L-1, L-2, L-4].
- H-2: [The integrated ferry-vehicle system] [maintains a separation distance below the predefined safety buffer between moving vehicles and charging infrastructure] [during loading operations] [L-1, L-2, L-3].
- H-3: [The integrated ferry-vehicle system] [maintains energized high-voltage charging equipment within a hazardous zone containing hydrogen gas concentrations] [during SIMOPs] [L-1, L-2, L-3, L-4].
- H-4: [The integrated ferry-vehicle system] [permits uncontrolled thermal energy transfer between the ship's battery compartment and HFCVs sufficient to trigger pressure relief or ignition] [L-1, L-2, L-3, L-4].
- H-5: [The integrated ferry-vehicle system] [enters a non-synchronized safety state between the shore-side and ship-side controllers] [following an emergency detection] [L-1, L-2, L-3].

4.2. *Modeling the control structure*

The control structure models the functional relationships and feedback loops that maintain safety within the integrated maritime and automotive system. Each control loop consists of a controller that utilizes a control algorithm and a process model to issue control actions based on feedback from the controlled process. Figure 2 and Figure 3 illustrate the respective control structures for the MF Bastø Electric and the HFCVs.

The ferry and vehicle control systems operate independently, with interactions mediated solely by the deck crew. For the MF Bastø Electric, the Integrated Bridge System (IBS) manages fire safety and off-gas ducts, the Integrated Automation System (IAS) governs autonomous docking, and the Energy Management System (EMS) monitors battery safety and shore-side charging.

During SIMOPs, HFCV drivers drive their vehicles onto or off the ferry under the guidance of the deck crew. The Vehicle Control Unit

(VCU) regulates energy and propulsion including the motor, braking, Battery Management System (BMS), and Fuel Cell Control Unit (FCCU) based on driver inputs. The deck crew facilitates this by relaying bridge instructions to drivers for vehicle positioning, subsequently reporting the deck status back to the bridge to complete the feedback loop.

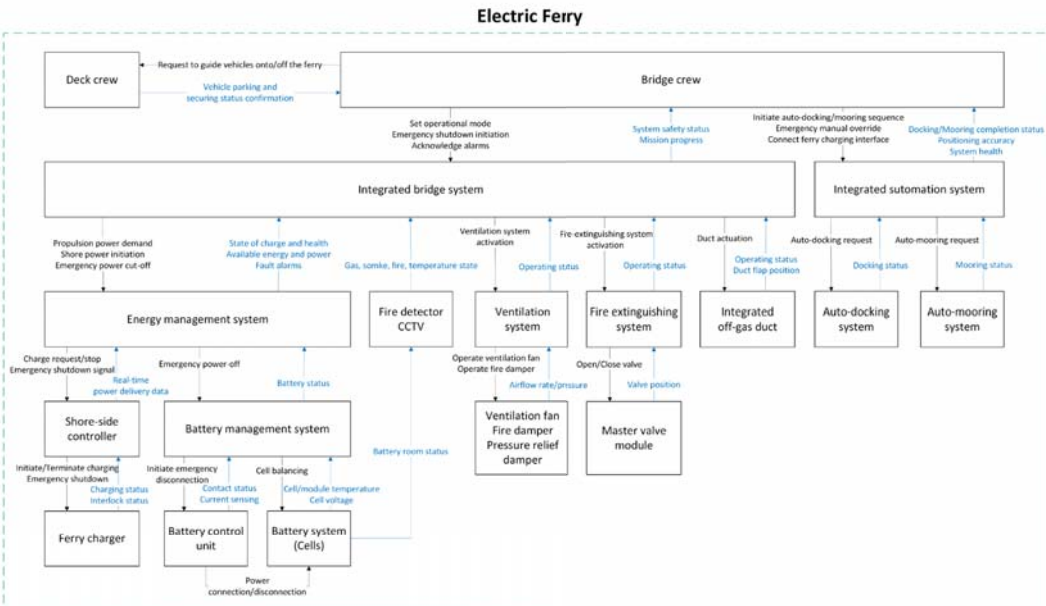

Figure 2. Control structure of the electric ferry

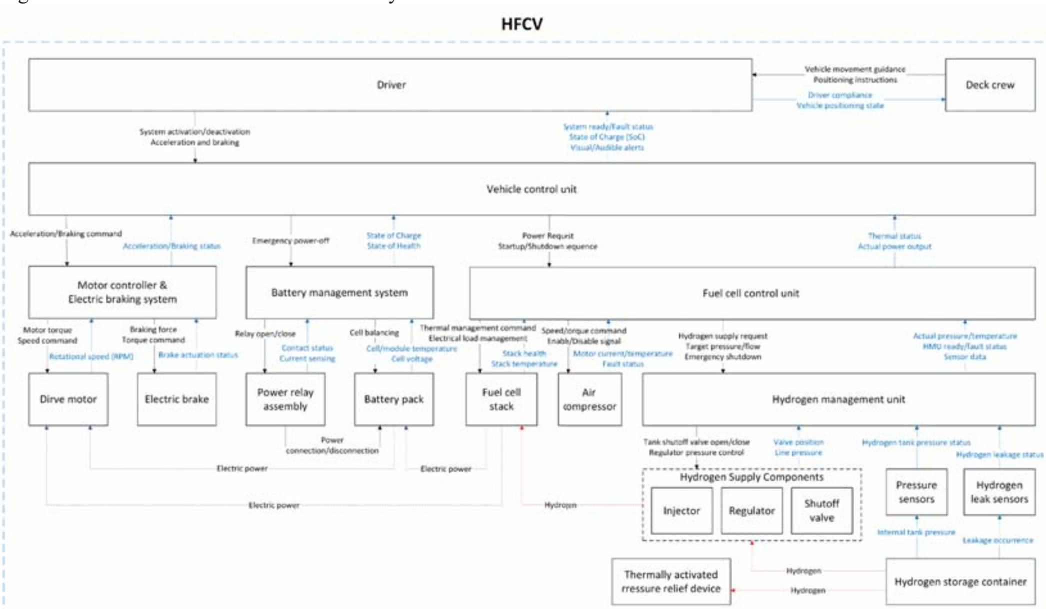

Figure 3. Control structure of a HFCV

4.3. *Identifying Unsafe Control Actions*

Once the system-level hazards and the control structure are established, UCAs can be identified. A UCA is defined as a control action that leads to a hazard when provided in a given operational context or system state. Table 2 presents examples of the UCAs identified in this analysis. For instance, in the context of a hydrogen leak from an HFCV, not providing or providing too late an emergency shutdown initiation by the bridge crew constitutes an UCAs. This systematic process was applied to all controllers identified in the control structure.

Table 2. Identifying UCAs of the bridge crew

Controller: Bridge crew

No.	Control action	Context	Not providing	Providing	Too early	Too late	Stopped too soon	Applied too long
1	Emergency shutdown initiation	when electric arcs or overcurrents occur at the ferry's charging interface	*Unsafe*	Safe	Safe	*Unsafe*	N/A	N/A
2		when a hydrogen leak occurs in a hydrogen fuel cell vehicle	*Unsafe*	Safe	Safe	*Unsafe*	N/A	N/A
3		when a fire occurs in the ferry's battery room	*Unsafe*	Safe	Safe	*Unsafe*	N/A	N/A
4		when seawater ingress occurs into the ferry	*Unsafe*	Safe	Safe	*Unsafe*	N/A	N/A
5		when a fire originates from another vehicle on the ferry	*Unsafe*	Safe	Safe	*Unsafe*	N/A	N/A
6	Acknowledge alarms	when an emergency alarm is triggered by the ferry's integrated alarm system	*Unsafe*	Safe	N/A	*Unsafe*	*Unsafe*	*Unsafe*
7	Emergency manual override	when a failure occurs in the ferry's auto-docking or auto-mooring system	*Unsafe*	Safe	Safe	*Unsafe*	*Unsafe*	Safe
8	Request to guide vehicles off the ferry	when an emergency alarm is triggered by the ferry's integrated alarm system	*Unsafe*	Safe	N/A	*Unsafe*	*Unsafe*	*Unsafe*

4.4. *Identifying loss scenarios*

This step focuses on explaining why a controller might issue an unsafe command or why a safe command might fail to achieve its objective. The analysis considers the entire control loop including the controller and the feedback sensors and the communication links between the ship and the shore. The following list shows the loss scenarios identified for UCAs item 2 from Table 2, which involves the failure to provide or the late provision of an emergency shutdown initiation during a hydrogen leak in an HFCV. This process was performed for all UCAs.

- Scenario 1: Feedback failure and unawareness
  The bridge crew fails to initiate a shutdown because they are unaware of the leak due to sensor or communication failures. This leads to a flawed process model where the crew incorrectly assumes the system is safe.
- Scenario 2: Information overload and delayed processing
  The shutdown is delayed as the crew prioritizes charging parameters over leak notifications during SIMOPs. This cognitive overload is worsened if the IBS interface does not prioritize safety alerts over routine data.
- Scenario 3: Signal mistrust and delayed confirmation
  The bridge crew receives the leak signal but mistakes it for sensor noise due to past

calibration issues. They deliberately delay the shutdown command until physical evidence of the hazard is observed.

5 Discussion

In this study, a total of 133 high-level UCAs have been identified for the integrated battery-electric ferry and HFCV system. The Bridge Crew and the FCCU of HFCV are associated with the highest number of UCAs (26 and 15, respectively). Out of the 133 identified UCAs, 43 are related to H-4, which involves uncontrolled thermal energy transfer between the ship's battery and the HFCV, while 13 UCAs are related to H-3, maintaining energized equipment within a hazardous hydrogen zone. The distribution of UCAs for each controller and their relevance to system-level hazards are summarized in Table 3.

Table 3. Total number of identified UCAs

Controller	Total UCAs	H1	H2	H3	H4	H5
Bridge Crew	26	2	7	7	6	4
Integrated Bridge System	13			2	9	2
Integrated Automation System	10			4		6
Energy Management System	4					4
Ventilation System	3				3	
Fire-extinguishing System	3				3	
Shore-side Controller	2					2
Battery Management System (Ferry)	8				8	
Deck Crew	8		8			
HFCV Driver	10		10			
Vehicle Control Unit	10	4	4		2	
Motor Controller & Electric Braking System	8		8			
Battery Management System (HFCV)	10				8	2
Fuel Cell Control Unit	15	8			4	3
Hydrogen Management Unit	3	3				
Total	133	17	37	13	43	23

The most significant finding of this analysis is the asymmetric information flow between the HFCV and the ferry. While the ferry's EMS and IBS monitor internal battery states and charging parameters, there is a total absence of feedback regarding the status of the HFCVs hydrogen storage and venting systems. As identified in Scenario 1, if a vehicle's hydrogen system fails and initiates venting, the ferry's controllers are currently blind to this hazard (H-1). This lack of feedback directly leads to UCAs, where the Bridge Crew fails to initiate an emergency shutdown because their process model incorrectly reflects the environment as safe. For SIMOPs to be reliable, safety architectures must move beyond isolated units toward an integrated data-sharing protocol where critical vehicle safety alerts, such as leak detection or pressure relief triggers, are relayed directly to the IBS of ferry.

The STPA results highlight that human controllers are particularly vulnerable to information overload during simultaneous charging and loading operations. Traditional safety assessments often label these events as human error. However, this study reveals that these are systemic failures caused by inadequate interface design. When the IBS does not prioritize high-risk safety alerts over routine charging data, the crew's ability to maintain situational awareness is compromised. Furthermore, Scenario 3 suggests that signal mistrust can lead to delayed shutdowns, even when alerts are received, highlighting a need for more robust, high-integrity sensor calibration and clear, unambiguous alarm hierarchies. To address these risks, the safety constraints derived in this study (SC-1 through SC-5) provide maritime safety guidelines. We propose the following requirements for zero-emission SIMOPs:

(SC-1) Integrated Detection and Active Ventilation

- H2 sensors: The ferry's car deck must be equipped with high-sensitivity hydrogen gas detectors capable of sensing concentrations at 10% of the LEL to provide early warning before a hazardous state is reached.
- Ventilation: Upon detection of hydrogen by the ship-side sensors, the IBS must automatically trigger maximum forced ventilation in the affected deck zone to disperse the gas and prevent the formation of explosive pockets in semi-enclosed spaces.

(SC-2) Dynamic Spatial Management and Collision Prevention

- Buffer zones: A physical exclusion zone must be maintained around the 7–9 MW high-voltage charging interface. This zone should be dynamically managed by the Deck Crew and visualized via digital overlays on the IBS.
- Loading protocols: The Deck Crew must enforce a sequential loading protocol that ensures HFCVs are parked in designated high-ventilation zones, away from energized charging cabinets or potential ignition sources like electric arcing.

(SC-3) High-Integrity Ignition Prevention

- EMS Cut-off: The EMS must be programmed to execute an immediate emergency cut-off if hydrogen gas is detected within the hazardous zone of the shore-side charger.
- Arc Resistant design: Charging interfaces should utilize arc-containment technology to minimize the risk of electrical discharge acting as an ignition source during the connection/disconnection phase.

(SC-4) Thermal Isolation and Proactive Cooling

- Thermal Barriers: Structural fire insulation (A-60 class or higher) must be maintained between the ship's battery compartment and the car deck to prevent thermal runaway propagation from the ferry to HFCV hydrogen tanks.
- Active Cooling: In the event of a ferry battery fire, the Fire-extinguishing system must initiate a drenching protocol for the HFCV parking zone to maintain hydrogen tank temperatures below the activation threshold of Thermally Activated Pressure Relief Devices (TPRD).

(SC-5) Cross-Platform Communication and Synchronized Shutdown

- Unified E-Stop: A synchronized shutdown protocol must link the Shore-side Controller, the ship's IBS, and the loading ramp control. Activating any Emergency-Stop must simultaneously cease the power transfer and freeze all vehicle movements to prevent escalating scenarios.
- V2S Feedback: To address the identified feedback gap, an industry-standard Vehicle-to-Ship (V2S) communication protocol is recommended. This would allow the vehicle's FCCU or Hydrogen Management Unit (HMU) to broadcast its status directly to the bridge, ensuring the crew's process model is updated instantly if a vehicle-side leak occurs.

6. Conclusion

This research provides an examination of the emergent risks inherent in the convergence of diverse zero-emission energy systems within maritime environments. By applying STPA to the SIMOPs of high-power shore charging and HFCV loading on the MF Bastø Electric, this study successfully identified 133 UCAs that traditional hazard analysis method might overlook. The pivotal finding is the existence of a critical feedback gap between the vehicle's hydrogen management systems and the ferry's IBS. This research contributes to the field by shifting the safety paradigm from component reliability to system-theoretic control, resulting in a framework of five safety constraints (SC-1 to SC-5) designed to govern complex functional interactions in multi-energy SIMOPs.

While STPA proved highly effective at identifying non-linear causal factors and software-logic failures, the analysis also highlighted significant methodological challenges. The technique remains inherently qualitative, relying heavily on the subjective expertise of the research team to model the control structure and identify potential loss scenarios. Furthermore, while STPA identifies that a hazard exists, it does not inherently provide the physical or temporal quantification needed to define exact safety distances or maximum allowable shutdown latencies. This limitation underscores the need for supplementary analytical tools to move from identifying unsafe states to defining precise engineering tolerances.

References

Baybutt, P. (2017). Simultaneous Operation (SIMOP) Review: An Important Hazard Analysis Tool. Process Safety Progress, 36(1), 62–66. https://doi.org/10.1002/prs.11866

Cui, S., Zhu, G., He, L., Wang, X., & Zhang, X. (2023). Analysis of the fire hazard and leakage explosion simulation of hydrogen fuel cell vehicles. Thermal Science and Engineering Progress, 41, 101754. https://doi.org/10.1016/j.tsep.2023.101754

Fan, H., Enshaei, H., & Gamini Jayasinghe, S. (2021). Safety philosophy and risk analysis methodology for LNG bunkering simultaneous operations (SIMOPs): A literature review. Safety Science, 136, 105150. https://doi.org/10.1016/j.ssci.2020.105150

Halder, P., Babaie, M., Salek, F., Haque, N., Savage, R., Stevanovic, S., Bodisco, T. A., & Zare, A. (2024). Advancements in hydrogen production, storage, distribution and refuelling for a sustainable transport sector: Hydrogen fuel cell vehicles. International Journal of Hydrogen Energy, 52, 973–1004. https://doi.org/10.1016/j.ijhydene.2023.07.204

Han, H., Kim, S., Park, J., Kim, G., & Jung, S. (2024). Risk mitigation study for hydrogen releases from hydrogen fuel cell vehicles. INTERNATIONAL JOURNAL OF HYDROGEN ENERGY, 54, 1593–1602. (WOS:001161128300001). https://doi.org/10.1016/j.ijhydene.2023.11.208

Hsu, S.-H., Tzu, F.-M., Chen, Y.-D., & Huang, C.-W. (2024). Navigating Safety and Compliance in High-Voltage Shore Connection Systems: A Comprehensive Exploration of IEC/IEEE 80005-1 Standards and the Guidelines of Ship Classification Societies. Journal of Marine Science and Engineering, 12(2), 322. https://doi.org/10.3390/jmse12020322

Johnsen, S., Thieme, C., Myklebust, T., Holte, E., Fjørtoft, K., & Jan Rødseth, Ø. (2022). Hazards and Risks of Automated Passenger Ferry Operations in Norway. 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022). https://doi.org/10.54941/ahfe1002312

Karimi, S., Zadeh, M., & Suul, J. A. (2020). Shore Charging for Plug-In Battery-Powered Ships: Power System Architecture, infrastructure, and Control. IEEE Electrification Magazine, 8(3), 47–61. https://doi.org/10.1109/MELE.2020.3005699

Leveson, N., & Thomas, J. (2018). STPA Handbook.

Tamura, Y., Takabayashi, M., & Takeuchi, M. (2014). The spread of fire from adjoining vehicles to a hydrogen fuel cell vehicle. International Journal of Hydrogen Energy, 39(11), 6169–6175. https://doi.org/10.1016/j.ijhydene.2014.01.140

Uavpic. (2022, April 18). Bastø Electric. Uavpic. https://uavpic.com/basto-electric/

United Nations. (2025). Emissions Gap Report 2024 (DEW/2672/NA; p. 100). United Nations Environment Programme. https://www.unep.org/resources/emissions-gap-report-2024

Wang, H., Boulougouris, E., Theotokatos, G., Priftis, A., Shi, G., Dahle, M., & Tolo, E. (2020). Risk Assessment of a Battery-Powered High-Speed Ferry Using Formal Safety Assessment. Safety, 6(3), 39. https://doi.org/10.3390/safety6030039

Zhu, X., Wang, C., Xie, Q., & Zhang, A. (2025). A quantitative risk assessment method for hydrogen fuel cell vehicles in residential garages. International Journal of Hydrogen Energy, 157. Scopus. https://doi.org/10.1016/j.ijhydene.2025.150250