Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 131-138

Design and Scenario Development of a Maritime Cybersecurity Training Simulation Platform

Ekaterina Dyankova
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
edyankova@naval-acad.bg

Dilyana Dimitrova
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
di.dimitrova@naval-acad.bg

Evgeni Andreev
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
e.andreev@naval-acad.bg

***Abstract*— This paper presents the design and scenario development of a simulation platform for maritime cybersecurity training. In response to the increasing digitalization of shipboard systems and the growing exposure to cyber threats, the platform provides a web-based environment that simulates a ship bridge and enables hands-on training in cyber incident response. The system supports real-time interaction with key on-board systems, allowing users to observe and respond to unusual behavior under simulated attack conditions. The platform includes three cyber-physical scenarios: GPS spoofing, AIS data injection, and engine control malware. The presented solution is designed to respond to specific training needs - the detection of cyber-physical attacks in conditions that closely simulate real-life scenarios. It is suitable for integration into academic and professional maritime training, enhancing traditional bridge simulators by addressing specific cybersecurity challenges in a controlled and accessible environment.**

Keywords*— *maritime cybersecurity, simulation-based training, ship bridge simulation.

I. INTRODUCTION

The rapid adoption of digital technologies in the maritime sector is transforming the way modern vessels are navigated, operated, and maintained. Systems like Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS) and Integrated Bridge Systems (IBS) are turning ship operations into complex cyber-physical processes in which the human factor interacts with automated digital solutions [1]. This digitalization is leading to a new era of maritime safety, the need for cyber resilience and the ability to respond to digital incidents [2].

At the same time, maritime education is going through a significant change. The integration of simulation technologies as a primary training method provides an opportunity to gain practical experience in performing complex operations in a controlled environment, without risk to personnel or equipment [1], [3]. In parallel, cybersecurity training has become essential for protecting maritime operations, safeguarding sensitive information, ensuring regulatory compliance, and reducing the financial and operational risks associated with cyber threats. As a result, cybersecurity competence is now a key component of the resilience and security of the global maritime industry [4].

The introduction of maritime cyber simulators represents the next stage in the development of simulation technologies. They combine the physical infrastructure of a ship's bridge with virtual cyber scenarios, allowing trainees to study how systems behave when exposed to threats such as malware, GPS spoofing, and unauthorized access to on-board networks [5]. In this way, simulation environments have become a tool for technical training and a means of developing critical thinking, situational awareness, and coordination skills in crisis situations. As a result, they play a dual role in modern maritime education: on the one side, they support the development of professional competencies related to the safety and efficiency of maritime operations, and on the other, they develop the cognitive and social skills necessary for managing cyber risks in the digitalized maritime environment.

Recent studies have examined the issue of maritime cybersecurity training and the need to develop maritime cybersecurity simulators. Publications in the global Scopus database from the past five years were analysed. The search utilized the keywords "maritime", "simulators", and "cybersecurity." Six publications were selected that met the specified criteria and addressed the topic of the problem under consideration.

In paper [6], the authors investigate the vulnerabilities of the ship's main engine lubrication system using a MATLAB Simulink model, simulate various scenarios, and evaluate the system's behavior. The study demonstrates how cyberattacks on sensors and controllers can lead to critical temperature deviations, potentially causing engine damage. This work highlights the need to integrate cyber scenarios into physical simulators for crew

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.116
© 2026 The Author(s). Published by Green Future Technologies.
This is an open-access article under the Creative Commons Attribution 4.0 International License.

training, with the aim of developing critical thinking and incident response capabilities. In [7], ShipNetSim is developed - an open-source simulator that combines aspects of environmental science and cybersecurity, expanding the scope of maritime cybersecurity training, particularly in the assessment of GPS spoofing and route optimization. In [8], the authors present ICoSSiuM, a simulator focused on maritime communications, primarily the AIS. The simulations demonstrate how attacks on communication systems can disrupt maritime operations, adding another aspect to maritime cybersecurity. Through simulated cyberattack scenarios (tabletop exercises), exercises on navigation simulators, and questionnaires, the authors in [9] find that future navigators of unmanned vessels will require training that includes new skills for interacting with digital systems in various activities, such as remote monitoring and others, in order to overcome various challenges, including the management of cyber incidents. In their publication [10], the authors examine autonomous vessels and present a modular warship simulator with artificial intelligence-based monitoring for navigation and network operations. The simulation includes GPS spoofing and attacks on industrial control systems. These technologies aim to train personnel to detect anomalies and protect the ship, demonstrating the potential of artificial intelligence in cyber simulation training. The authors in [11] developed MaCySTe, a project providing a test environment that simulates network infrastructure and the main components of ship cyber-physical systems and integrates with ship simulators. The platform provides realistic training and testing of countermeasures, thereby enhancing the cybersecurity culture among the crew.

Based on the analysis of the literature, it can be concluded that simulation technologies are established as a key tool in the training of maritime personnel, particularly in the context of growing cyber threats to ship systems and communications. They enable the practical learning of a variety of skills in a safe environment, such as responding to cyberattacks on physical and communication systems on board. Combining various aspects of maritime cybersecurity can prepare personnel for real-world operations and incidents.

The main aim of the paper is to present the design and scenario development of a simulation platform for maritime cybersecurity training. The presented solution is designed to respond to specific training needs - the detection of cyber-physical attacks in conditions that closely simulate real-life scenarios.

II. MATERIALS AND METHODS

A. The evolution of maritime simulators over the years

The development of simulation technologies related to maritime education is illustrated in Fig. 1.

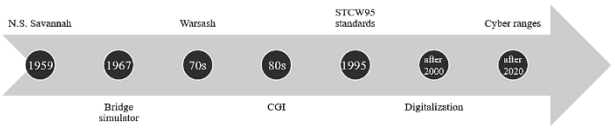

Fig. 1. The development of simulation technologies in maritime education.

The concept of simulation in maritime training goes back to the mid-20th century. A pioneering step can be linked to the world's first nuclear-powered merchant ship, the N.S. Savannah (1959). It is noted that a computer-based training system was used for the crew [12]. However, there is not enough data to confirm that this was a complete computer simulator.

Two key developments emerged in the 1960s. In 1967, the first modern ship bridge simulator was built in Gothenburg, Sweden, to study crew behavior, ship architecture, and port design [13]. By the end of the decade, several countries (Sweden, the Netherlands, the United States, and Japan) had developed their own ship maneuvering simulators, initially intended primarily for scientific research. The first practical training simulators appeared in the early 1970s. The first "bridge" simulator in the United Kingdom was developed at the Warsash School of Maritime Studies and used projected dots of red, green, and white lights to represent approaching ships and buoys [12]. It quickly established itself as a leading innovation in maritime training for its time, proving its effectiveness. Over time, these early analog systems evolved into digital simulators with increasingly realistic graphics and multidisciplinary applications.

During the 1970s and 1980s, simulation technology evolved rapidly. Simulators, such as the one in Warsash, were replaced by computer-controlled systems with black-and-white and, later, color graphics. In 1982, the first simulator with computer-generated imagery (CGI) for day and night graphics was developed in the United Kingdom. At the same time, a simulator based on aviation technology (Computer Aided Operations Research Facility - CAORF) was introduced at the Naval Academy in New York, USA, used for scientific research and for training cadets [12].

At the end of the 20th and beginning of the 21st centuries, advances in computer and graphics processor technology made it possible to integrate complex navigation systems (ECDIS, GPS, radar, and others) into simulators. According to [14], following the adoption of the new STCW95 requirements (1995, effective 1997) and due to technologies from the video game industry, maritime training now utilizes multi-platform solutions: stationary and fully functional navigation simulators, desktop and cloud-based simulators, as well as virtual and augmented reality applications [13], [14]. According to leading manufacturers such as Wärtsilä (NavSim), their simulation systems support training in both traditional classrooms and VR/AR environments, as well as network architectures for distributed learning, all unified under a single software package [15]. High realism is achieved through authentic ship models, classrooms featuring detailed replicas of bridges and engine rooms, dynamic maritime environments, and, when necessary, the movement of simulated ships (dynamic positioning, etc.).

Tracking the evolution of simulation technologies in maritime training reveals a consistent progression from

analog systems with limited visual capabilities to realistic digital environments that integrate navigation and communication components, as well as the inclusion of cyberattack simulations. From the first experimental simulators in the 1960s to modern VR/AR and cloud-based platforms, the trend has been toward increasing the realism, safety, and effectiveness of training. These technologies optimize the training process for maritime professionals, create conditions for adapting to new challenges, and lead to the development of new solutions capable of simulating real-time attacks to improve trainees' decision-making skills.

B. Design of a maritime cybersecurity training simulation platform

The developed web-based training environment simulates the bridge of a cargo ship. The idea is to offer an accessible and easily deployable tool that meets the IMO's requirements for cyber risk management [16] and the NIST cybersecurity framework (CSF) [17]. It operates entirely on the client side, enabling accessibility through standard web browser without requiring dedicated infrastructure. The goal is the trainees to be able to recognize the symptoms of three types of cyber-physical attacks in real time, apply the correct mitigation procedures, see the immediate effect of their actions, and understand what happens when they make the wrong decision.

The platform is developed for cadets, students and officers at the Nikola Vaptsarov Naval Academy in Varna, Bulgaria, but it is also applicable in other maritime higher education institutions or corporate crew training programs.

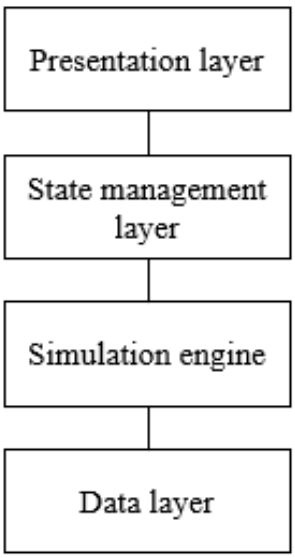

Fig. 2. System architecture.

The system architecture is presented in Fig. 2. It is organized into four logical layers:

- presentation layer - it consists of interactive user interface components that visually represent ship systems and operational conditions;
- state management layer - maintains the global simulation state, which includes system integrity, active threats, user progress, and event logs;
- simulation engine - it controls the execution of cyberattack scenarios, handling user interactions, validating responses, and updating system behavior;
- data layer - provides configurable definitions of attack scenarios and enables flexibility and extensibility without modifying core application logic.

Following the description of the four architectural layers, the technological foundation of each layer is presented to provide a complete picture of the implementation. The platform is developed as a single-page application using React 19 with TypeScript, with Vite serving as the build toolchain. TypeScript is selected to ensure static type safety across the simulation state model, where typed interfaces define system statuses, challenge-step structures, and attack scenario configurations.

The presentation layer is styled with Tailwind CSS as a utility-first framework and includes Framer Motion for animated transitions, including alert pulsations, radar scan-line effects, and modal interactions, while Lucide React supplies consistent SVG iconography across the interface. The state management layer is implemented through React's built-in hooks (useState, useEffect), maintaining a single SimulationState object that encapsulates active attack references, ship system parameters, event logs, score, elapsed time, and integrity values. The simulation engine operates through a one-second interval timer that decrements vessel integrity during active attacks, applies pseudorandom fluctuations to compromised sensor readings, and evaluates termination conditions. The data layer is implemented as a declarative TypeScript module defining scenario parameters, challenge steps, valid responses, and penalty structures.

At the core of the platform is a centralized simulation controller that orchestrates the execution flow. Each training scenario is modelled as a sequence of structured steps representing different stages of a cyberattack. Users interact with the system through decision panels, where their actions are evaluated in real time. Correct responses advance the simulation and improve performance metrics, while incorrect actions result in penalties such as reduced system integrity or degraded system functionality. The application runs entirely client-side without server-side components or external API dependencies, requiring only Node.js (version 18 or higher) as a development-time dependency. This deployment model ensures accessibility in maritime training environments with limited or restricted network connectivity.

The platform also includes a system visualization module that mimics real maritime interfaces and includes radar displays and subsystem panels. These components dynamically reflect the effects of cyberattacks, enhancing situational awareness. An event logging mechanism

records all actions and system changes, providing immediate feedback during execution and supporting post-simulation analysis.

The system workflow (Fig. 3) begins with scenario initialization, followed by stepwise user interaction, real-time evaluation, and continuous feedback. The simulation terminates either upon successful completion of all steps or when system integrity falls below a defined threshold. The current design emphasizes simplicity and accessibility. The interface of the simulation platform is presented in Fig. 4.

A key design feature is the use of a configurable data model for defining attack scenarios. Each scenario specifies targeted systems, ordered challenge steps, and possible incorrect actions with associated consequences. This approach allows domain experts to extend the platform with new threat scenarios without altering the underlying implementation, improving maintainability and scalability.

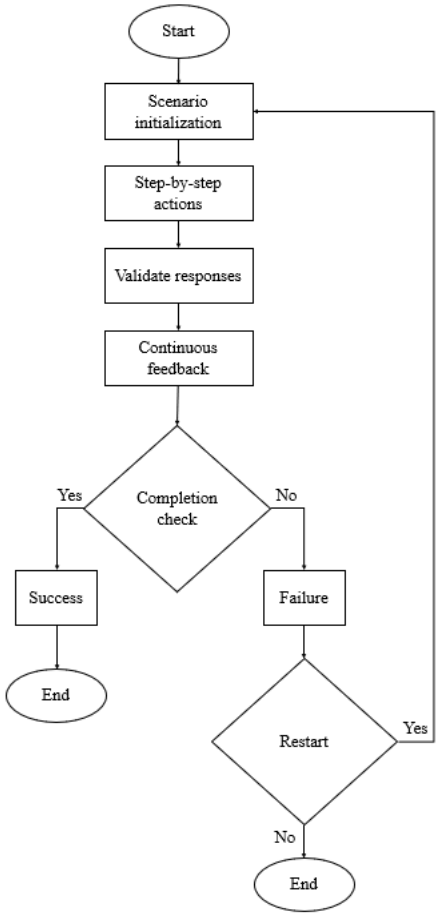

Fig. 3. System workflow.

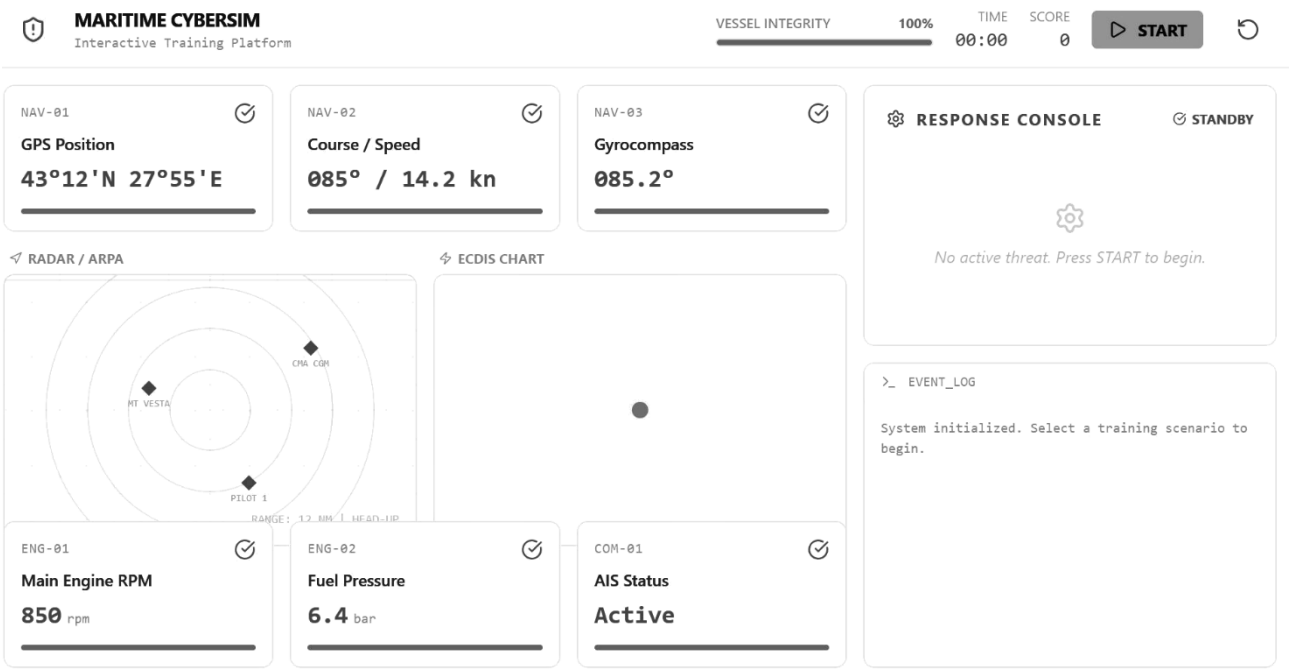

Fig. 4. The interface of the simulation platform.

III. Results and Discussion

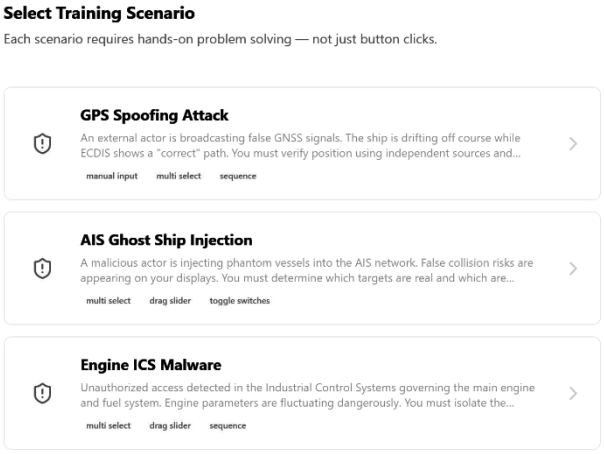

Fig. 5. Scenario options.

The proposed solution includes three cyber-physical attack scenarios presented in Fig. 5, each reflecting a distinct category of maritime cybersecurity threat and grounded in both real-world incidents and documented vulnerabilities in the literature. They are designed to simulate realistic on-board conditions, requiring trainees to detect anomalies, assess system reliability, and execute appropriate mitigation procedures. The scenarios provide structured learning progression from navigation data manipulation to direct compromise of critical control systems.

A. GPS spoofing attack scenario

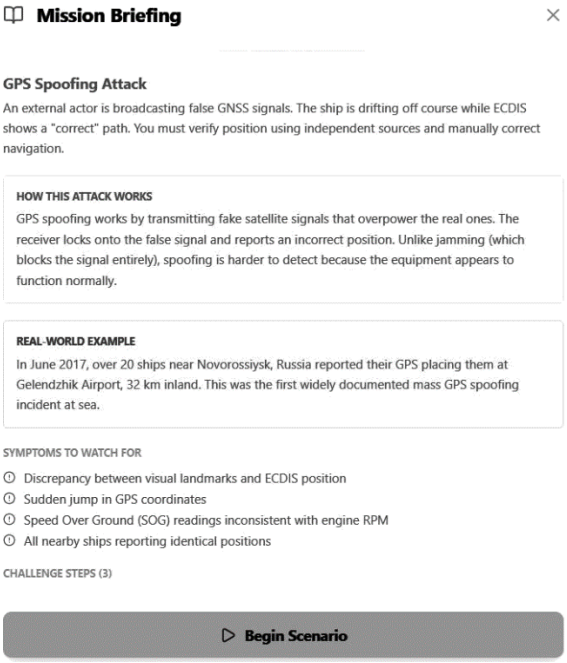

Fig. 6. Scenario 1 overview.

The first scenario models a GPS (Global Positioning System) spoofing attack, in which spoofed satellite signals are transmitted to override legitimate positioning data. As a result, the vessel appears to maintain a valid position on the Electronic Chart Display and Information System (ECDIS), while it deviates from its intended course. This type of attack has been documented in operational environments, most notably in the Black Sea incident in June 2017, where more than 20 vessels near Novorossiysk reported false GPS positions directing them inland toward Gelendzhik airport [18]. More recent observations in the period 2023-2024 further confirm that GNSS (Global Navigation Satellite System) spoofing has evolved into an operational threat [19]. Fig. 6 presents an overview of a GPS spoofing attack scenario. The panel includes a real-world example, lists warning signs, and outlines steps to verify and correct navigation before starting the scenario.

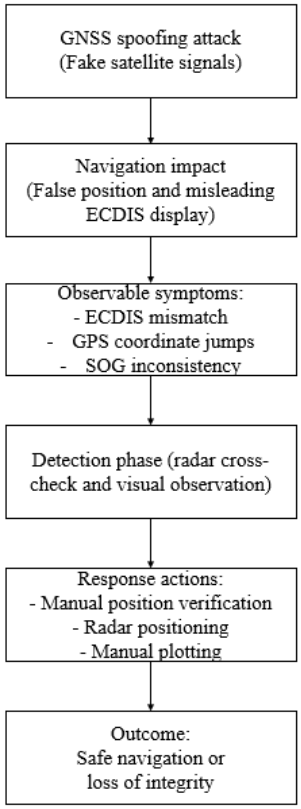

Fig. 7. GPS spoofing attack workflow.

Within the simulation, a GNSS spoofing attack causes false position data, coordinate jumps, and inconsistencies in course over ground (COG) and speed over ground (SOG). As shown in Fig. 7, trainees must detect discrepancies between GNSS data and independent sources to maintain situational awareness and safe navigation.

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.116
© 2026 The Author(s). Published by Green Future Technologies.
This is an open-access article under the Creative Commons Attribution 4.0 International License.

B. AIS ghost ship injection scenario

The second scenario presented in Fig.8 simulates an AIS data injection attack, where an adversary introduces altered vessel information into the communication network, resulting in the appearance of non-existent targets ("ghost ships"). This type of manipulation exploits the lack of authentication and encryption in AIS protocols, making them inherently vulnerable to spoofing and data injection attacks.

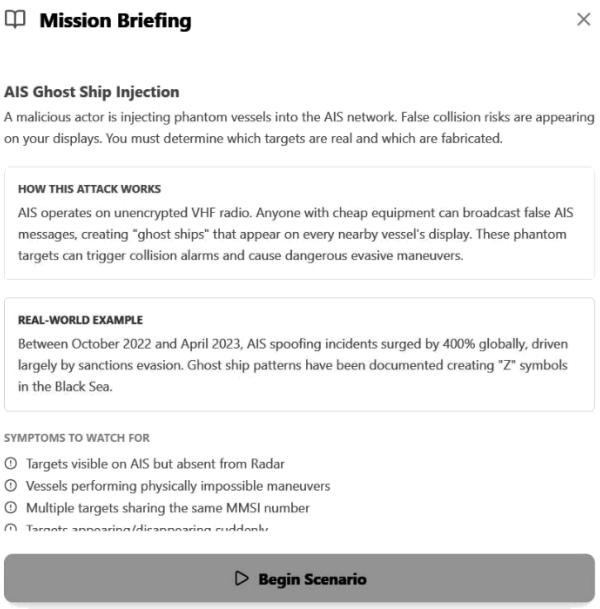

Fig. 8. Scenario 2 overview.

Such incidents are reported in practice. For example, analyses of maritime traffic data indicate a significant rise in AIS spoofing events, with reported cases increasing by up to 400% between late 2022 and early 2023. Other studies further confirm that AIS messages can be easily forged, allowing attackers to create phantom vessels, duplicate identities, or manipulate vessel trajectories [20].

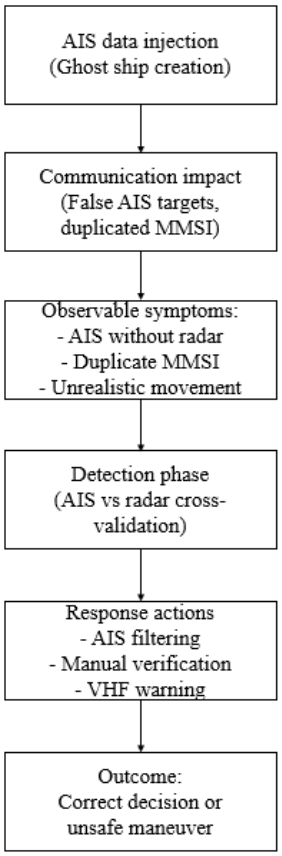

Fig. 9. AIS ghost ship injection workflow.

In the simulation, ghost targets appear on the AIS display without corresponding radar echoes or exhibit anomalies such as duplicated Maritime Mobile Service Identity (MMSI) numbers and unrealistic movements (Fig. 9). Trainees must identify these inconsistencies by correlating AIS data with radar and visual observations. The scenario trains users to apply filtering mechanisms, switch to manual verification modes, and prioritize trusted sensor inputs. It also incorporates communication procedures, such as issuing navigational warnings. The objective is to prevent unsafe decisions, particularly unnecessary evasive maneuvers triggered by falsified information.

C. Engine ICS malware scenario

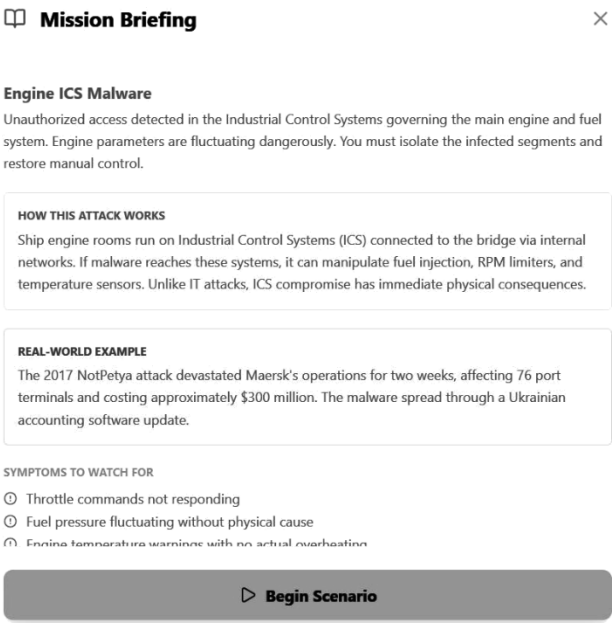

Fig. 10. Scenario 3 overview.

The third scenario addresses a malware attack targeting industrial control systems (ICS) within the vessel's engine and propulsion subsystem (Fig. 10). This case represents a direct compromise of operational control, posing an immediate risk to vessel safety.

The relevance of such attacks is supported by increasing concerns in the maritime domain regarding vulnerabilities in operational technology (OT) systems. International guidelines, including those issued by the International Maritime Organization (IMO), highlight the growing risk of cyber incidents affecting shipboard control systems [16].

In the simulation, the attack results in unstable engine behaviour - fluctuating revolutions per minute (RPM), irregular fuel pressure, and unresponsive control inputs (Fig. 11). Trainees must identify compromised network segments based on abnormal traffic patterns and they need to isolate affected systems so they can prevent further propagation. The response process includes transitioning to manual control, verifying system states through local instrumentation, and executing a controlled recovery sequence. The scenario emphasizes important cybersecurity principles such as network segmentation, incident containment, and staged system restoration and illustrates the risks associated with improper actions during an active attack.

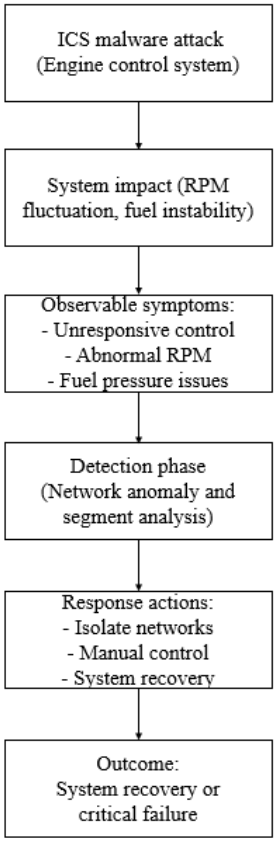

Fig. 11. Engine ICS malware scenario workflow.

The platform provides an accessible and flexible training solution compared to existing large-scale simulators. Its main advantage is the web-based architecture and ease of deployment. Despite its advantages, the current implementation has certain limitations which include the absence of real hardware integration and a limited set of training scenarios. The platform does not claim to replace full-scale bridge simulators, but it fills a niche that they don't cover - training in responding to cyber incidents in which navigation sensors malfunction, engine controllers fail to respond, and simulated ships threaten to collide. Possible directions for future development include adding new scenarios, introducing difficulty levels, a multiplayer mode, and integration with real NMEA data from navigation simulators.

IV. CONCLUSIONS

The paper presents the design and scenario development of a web-based maritime cybersecurity training simulation platform aimed at improving the preparedness of maritime personnel for cyber-physical incidents. The proposed solution provides an accessible and interactive environment that enables users to observe, analyze, and respond to cybersecurity threats affecting critical shipboard systems.

The platform integrates a modular architecture and a configurable scenario model, allowing the simulation of realistic cyberattack situations without the need for

specialized hardware. Three scenarios (GPS spoofing, AIS data injection, and engine ICS malware) were implemented to reflect key categories of maritime cyber threats, ranging from navigation manipulation to direct control system compromise. They support the development of essential skills such as anomaly detection, decision-making under uncertainty, and application of mitigation procedures.

The results demonstrate that the platform can serve as a valuable addition to traditional maritime simulators by introducing training focused on cybersecurity in a flexible and scalable format. Its web-based nature enables easy deployment in both academic and professional training environments, making it particularly suitable for institutions with limited access to full-scale simulators.

Future work will focus on expanding the scenario library, including multi-user and collaborative training capabilities, and integrating performance tracking and adaptive learning mechanisms. The proposed platform contributes to bridging the gap between theoretical cybersecurity knowledge and practical maritime training, supporting the development of cyber-resilient maritime operations in an increasingly digitalized industry.

ACKNOWLEDGMENTS

This report was financed by the Ministry of Education and Science under the National Science Program "Security and Defense", carried out in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and adopted by Decision of the Council of Ministers No. 731 of October 21, 2021. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

REFERENCES

[1] E. Demirel, "Maritime Education and Training in the Digital Era," Universal J ournal of Educational Research, vol. 8, no. 9, pp. 4129–4142, Sep. 2020, https://doi.org/10.13189/UJER.2020.080939.

[2] F. Martínez, L. E. Sànchez, A. Santos-Olmo, D. G. Rosado, and E. Fernàndez-Medina, "Maritime cybersecurity: protecting digital seas," International Jo urnal of Information Security, vol. 23, no. 2, pp. 1429–1457, Jan. 2024, https://doi.org/10.1007/S10207-023-00800-0.

[3] B. Nikolov, "Approach to developing a maritime cybersecurity virtual training environment," in Proc. Int. Sci. Practical Conf. Environment. Technology. Resources, Rezekne, Latvia, Jun. 2024, pp. 220–225, https://doi.org/10.17770/ETR2024VOL2.8039.

[4] B. Nikolov and D. Nikolov, "A Scenario-based approach to cybersecurity training for Seafarers," in Proceedings of the International Association of Maritime Universities Conference, Buzzards Bay: International Association of Maritime Universities, 2024, pp. 385–390. Accessed: May 21, 2026. [Online]. Available: https://aga24.maritime.edu/wp-content/uploads/IAMUC-2024-proceedings-final-corrected.pdf

[5] G. Potamos, E. Stavrou, and S. Stavrou, "Enhancing Maritime Cybersecurity through Operational Technol ogy Sensor Data Fusion: A Comprehensive Survey and Analysis," Sensors, vol. 24, no. 11, May 2024, https://doi.org/10.3390/S24113458.

[6] Y. Gülmez, O. Konur, M. Erbas, and S. Bauk, "Identifying cyber attack vulnerabilities in the main lubricating oil system of marine propulsion units," International Journal of Critic al Infrastructure Protection, vol. 51, Dec. 2025, https://doi.org/10.1016/j.ijcip.2025.100810.

[7] A. Aredah and H. A. Rakha, "ShipNetSim: An Open-Source Simulator for Real-Time Energy Consumption and Emission Analysis in Large-Scale Maritime Networks," J. Mar. Sci. Eng., vol. 13, no. 3, Mar. 2025, https://doi.org/10.3390/jmse13030518.

[8] L. Bayou, A. Awarkeh, M. E. H. Haouari, R. Yaich, and M. A. Faillon, "ICoSSiuM: An integrated communication security simulator for maritime operations," Lecture Notes in Computer Science, vol. 15532, pp. 58–73, 2025, https://doi.org/10.1007/978-3-031-87499-4_5.

[9] J. D. Palbar Misas, R. Hopcraft, K. Tam, and K. Jones, "Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness," Journal of Marine Engineering and Techno logy, vol. 23, no. 3, pp. 224–235, May 2024, https://doi.org/10.1080/20464177.2024.2330176.

[10] L. Rivas et al., "Assuring Safe Navigation and Network Operations of Autonomo us Ships," IEEE 14th Annu. Comput. Commun. Workshop Conf. (CCWC), 2024, pp. 138–143, 2024, https://doi.org/10.1109/CCWC60891.2024.10427933.

[11] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," SoftwareX, vol. 23, p. 101426, Jul. 2023, https://doi.org/10.1016/j.softx.2023.101426.

[12] Nautilus International Maritime Union, "Simulators: 45 years of development and debate." Accessed: Apr. 21, 2026. [Online]. Available: https://web.archive.org/web/20251216032850/https://www.nautilusint.org/en/news-insight/telegraph/simulators-45-years-of-development-and-debate/

[13] M. H. Dewan, R. Godina, M. R. K. Chowdhury, C. W. M. Noor, W. M. N. Wan Nik, and M. Man, " "Immersive and non-immersive simulators for the education and training in maritime domain-A review"," J. Mar. Sci. Eng., vol. 11, no. 1, p. 147, 2023, https://doi.org/10.3390/jmse11010147.

[14] B. Lintott, "The History and Heritage of the Age of Simulation," Human Fact ors and Simulation, vol. 83, 2023, https://doi.org/10.54941/ahfe1003581.

[15] Wärtsilä, "Wärtsilä Navigational simulators." Accessed: Apr. 21, 2026. [Online]. Available: https://web.archive.org/web/20250905015437/https://www.wartsila.com/marine/products/simulation-and-training/navigational-simulators

[16] IMO, "Maritime cyber risk." Accessed: Apr. 22, 2026. [Online]. Available: https://web.archive.org/web/20260419071845/https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

[17] NIST, "The NIST Cybersecurity Framework." Accessed: Apr. 22, 2026. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[18] M. Jones, "Spoofing in the Black Sea: What really happened? - GPS World." Accessed: Apr. 22, 2026. [Online]. Available: https://web.archive.org/web/20250928103644/https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

[19] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and Mitigating Attacks on GPS Devices," Sensors, vol. 24, no. 17, Aug. 2024, https://doi.org/10.3390/S24175529.

[20] D. Ampatzidis, "AIS Spoofing in the Maritime Industry: A Growing Risk and Compliance Challenge." Accessed: Apr. 22, 2026. [Online]. Available: https://www.marinetraffic.com/ru/maritime-news/34/risk-and%20compliance/2024/11316/ais-spoofing-in-the-maritime-industry-a-growing-risk-and-com