

Securing Digital Maritime Operations: Defense Against Signal Manipulation in Vessel Navigation Systems Integration Through harborLang

Diana Malakhova^{1,*}, Simon Hacks^{2,†} and Anna Alexeeva³

¹Stockholm University, Institutionen för data- och systemvetenskap 164 25 Kista, Sweden

²Stockholm University, Institutionen för data- och systemvetenskap 164 25 Kista, Sweden

³Unaffiliated

Abstract

As maritime operations become increasingly reliant on digital systems, cybersecurity challenges have become a significant concern, particularly regarding GPS and AIS spoofing attacks. These types of cyber threats can compromise navigation and communication systems, leading to operational inefficiencies, safety risks, and financial losses. This paper presents an analysis of the effectiveness of cyber defense mechanisms in the context of the MISSION Project, which aims to optimize maritime operations. By using harborLang, a domain-specific language designed for modeling and simulating cyber-attacks on maritime systems, we analyze vulnerabilities within GPS and AIS systems. Additionally, we leverage the YACRAF framework to perform a comprehensive risk assessment and propose mitigation strategies. The results demonstrate how harborLang can simulate complex attack scenarios, offering actionable insights into the cybersecurity risks facing modern maritime operations. Future developments of harborLang are also discussed, focusing on its extension to address emerging technologies such as AI-driven autonomous vessels and satellite-based communications.

Keywords

Maritime cybersecurity, GPS spoofing, AIS spoofing, harborLang, YACRAF, navigation systems, MISSION Project

1. Introduction

The maritime industry is undergoing a profound digital transformation, with increased reliance on automated navigation and communication systems such as the Global Navigation Satellite System (GNSS) and the Automatic Identification System (AIS). These systems provide crucial data for safe and efficient vessel operations, ensuring accurate positioning, real-time communication, and enhanced coordination between vessels, ports, and other maritime stakeholders. However, this growing dependence on digital technologies has also exposed the maritime sector to significant cybersecurity threats.


Companion Proceedings of the 17th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling Forum, M4S, FACETE, AEM, Tools and Demos co-located with PoEM 2024, Stockholm, Sweden, December 3-5, 2024

*Corresponding author.

†These authors contributed equally.

✉ diana.malakhova@dsv.su.se (D. Malakhova); simon.hacks@dsv.su.se (S. Hacks); anya.alexeeva@gmail.com (A. Alexeeva)

ORCID 0000-0003-4833-1485 (D. Malakhova); 0000-0003-0478-9347 (S. Hacks); 0009-0006-5449-882X (A. Alexeeva)

 © 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

One of the most concerning cyber threats in this context is spoofing attacks on GPS and AIS systems. GPS spoofing involves the transmission of false satellite signals, tricking the vessel's navigation system into believing it is in a different location. Similarly, AIS spoofing involves broadcasting incorrect vessel identity or position data, leading to misidentification and disruptions in maritime traffic management. These attacks can result in severe operational consequences, including vessel misdirection, collisions, or undetected illegal activities such as smuggling or piracy.

To address these threats, the MISSION Project was launched with the aim of enhancing the efficiency, safety, and security of maritime operations through advanced digital solutions. One of the key components of this initiative is the development of harborLang, a domain-specific modeling language designed to simulate and assess cyber-attacks on maritime systems, including GPS and AIS spoofing. By using harborLang to model multi-stage cyber-attacks, the project can evaluate the effectiveness of various defensive strategies and provide a comprehensive assessment of cyber risks in the maritime domain.

This paper presents an analysis of cyber defense effectiveness within the MISSION Project. The analysis includes simulations of potential GPS and AIS spoofing attacks on a vessel's integrated navigation and communication systems using harborLang. These simulations provide critical insights into vulnerabilities in maritime systems and offer recommendations for enhancing cyber resilience. The YACRAF framework is used to evaluate risks and prioritize mitigation strategies, ensuring that the solutions developed are both effective and adaptable to the complex dynamics of maritime operations.

The remainder of this paper is structured as follows: Section 2 provides an overview of the background and related work, including the MISSION Project, GPS and AIS spoofing, the YACRAF framework, and the Meta Attack Language (MAL). Section 3 introduces harborLang, detailing its components and its role in addressing cyber threats in the maritime sector. Section 4 assesses the effectiveness of cyber defenses through use case simulations, and Section 5 presents conclusions and future research directions.

2. Background

2.1. MISSION Project

The Maritime Integrated Software-based Solution for Interoperable Networks (MISSION) Project is an EU-funded initiative that addresses inefficiencies in the maritime supply chain, particularly the "hurry-up-and-wait" scenario, where vessels arrive on time at ports only to be delayed due to unprepared facilities. Over a planned period of 42 months, the project will develop a digital optimization tool that operates in real-time, improving the coordination of port call operations among key maritime stakeholders, including shipping companies, ports, terminals, and service providers.

This optimization tool aims to reduce waiting times at sea, which, in turn, lowers fuel consumption, cuts greenhouse gas emissions, and enhances operational safety. A key feature of the project is its ability to increase transparency and improve real-time communication between maritime entities. By enabling vessels to adjust their speed based on terminal readiness, the MISSION Project anticipates fuel savings of up to 23% and a significant reduction in environmental

impacts. Moreover, it aims to decrease the average annual waiting time at anchor, benefiting a variety of vessel types.

Led by the University of Southern Denmark, the project consortium includes universities, research institutes, and industry stakeholders from across Europe, working together to develop and implement innovative IT systems and analytics tools. These tools will improve the interoperability of maritime operations and enable more efficient logistics management. The project also emphasizes real-time decision support systems, ensuring better integration of data and optimizing maritime operations at a higher level.

By the end of the project, the expected outcomes include a robust decision support system that incorporates real-time data for optimizing maritime operations, reducing the environmental impact of shipping activities, and promoting greater efficiency. The project also seeks to provide a model adaptable to broader applications in the maritime and transport sectors, offering a blueprint for digital transformation in maritime logistics. It aims to influence policy-making and standardization, aligning with the EU's goals for a competitive and environmentally sustainable transport sector, reinforcing the project's commitment to innovation and sustainability.

2.2. GPS and AIS Spoofing in Maritime Systems

As modern maritime operations increasingly rely on digital navigation and communication systems, GPS (Global Positioning System) and AIS (Automatic Identification System) have become critical for ensuring safe and efficient vessel movement. The Automatic Identification System (AIS) is a cyber-physical system that is required to be installed on ships since 2004 according to the Safety of Life at Sea (SOLAS) regulation V/19 (IMO,2000)[1]. However, this reliance also exposes vessels to significant cybersecurity threats, particularly spoofing attacks, where malicious actors manipulate these systems to mislead ships, port authorities, and coastal monitoring stations. GPS and AIS spoofing are two of the most concerning cyber threats in this domain, with the potential to cause substantial operational and security disruptions.

GPS spoofing involves the alteration or falsification of the satellite signals that a vessel's GPS receiver uses to determine its position. By injecting false signals, attackers can deceive the navigation system into believing the vessel is located elsewhere. This can lead to incorrect course plotting, which might cause vessels to enter restricted or dangerous areas, or deviate from their intended routes, potentially resulting in collisions or grounding. A notable example occurred in 2017, when numerous vessels in the Black Sea reported GPS anomalies, later identified as spoofing attacks, which caused ships to display false positions far from their actual locations[2].

GPS signals are an easy attack target. Due to the low signal strength at the Earth's surface, the signals can be effortlessly blocked[3] or manipulated. The civil GPS lacks encryption, authentication, or any further security measures to protect the signal integrity. In fact, the data structure, modulation schemes, and spreading codes are publicly available[4]. Altogether, these peculiarities enable jamming and spoofing[5].

Similarly, AIS spoofing targets the Automatic Identification System, which broadcasts a vessel's identity, position, speed, and course to other ships and coastal authorities. Attackers can manipulate this system to transmit false data, disguising a ship's true identity or location. AIS spoofing has been used in illegal activities, such as smuggling, illegal fishing, and sanctions evasion, by making vessels appear to be in different locations or hiding their presence entirely.

For example, vessels involved in oil smuggling have used AIS spoofing to evade detection by port authorities and maritime law enforcement, appearing to be outside restricted zones when they were not.

The impact of GPS and AIS spoofing on maritime systems is profound. These attacks not only threaten operational efficiency but also pose serious risks to navigational safety, particularly in congested or high-risk waters. The analysis of selected case studies confirmed that these systems could easily be spoofed and become a subject of data manipulation with significant consequences for the safety of navigation.[6] As these spoofing incidents grow more frequent and sophisticated, the maritime industry is pressed to adopt advanced methods of detection, defense, and simulation to mitigate their impact. In response to these evolving threats, the MISSION Project aims to enhance the cyber resilience of maritime navigation systems. By integrating advanced tools such as harborLang and YACRAF, the project focuses on simulating and assessing the risks posed by spoofing attacks, providing robust defenses to ensure vessels can continue to operate safely and efficiently even in the face of cyber threats.

2.3. YACRAF

The Yet Another Cyber Risk Assessment Framework (YACRAF)[7] was designed to address the increasing complexities of cybersecurity risk management, particularly in IT and cyber-physical systems. As organizations continue to expand their reliance on digital infrastructure, the risk of cyberattacks becomes a critical concern. YACRAF provides a structured and model-based approach for conducting quantitative risk assessments in these environments. It combines the strengths of threat modeling and risk calculation frameworks, aiming to improve the decision-making process for security controls.

YACRAF introduces a metamodel that defines how assets, vulnerabilities, threats, and impacts should be modeled to perform a comprehensive risk assessment. This metamodel is one of the key innovations of YACRAF, as it allows users to model specific attack vectors, vulnerabilities, and defense mechanisms associated with IT systems. In contrast to other frameworks, YACRAF integrates model-based security analysis with quantitative risk assessment, providing more precise decision support. The framework emphasizes the importance of considering the system architecture, highlighting how the context and location of vulnerabilities influence the overall risk to the organization.

YACRAF's risk calculation methodology is grounded in formalized risk assessment techniques that calculate risk based on threat probabilities, system vulnerabilities, and the potential impacts of successful attacks. By applying attack graphs, YACRAF maps attack events to specific assets and their defense mechanisms. This approach supports the evaluation of both individual risks and system-wide vulnerabilities. Moreover, the framework provides a mechanism to analyze the cost-effectiveness of different defense strategies, allowing organizations to prioritize mitigation efforts according to their available resources.

2.4. The Meta Attack Language

The Meta Attack Language (MAL) is a versatile framework designed to model and simulate cyber-attacks across a variety of domains. MAL enables users to create detailed representations

of system architectures and map out potential attack paths, allowing for in-depth analysis of cybersecurity risks. The core idea behind MAL is to define assets and their relationships in a way that simulates how an attacker might exploit vulnerabilities within a system to compromise critical components. By simulating attack scenarios, analysts can identify weak points in the system and evaluate the effectiveness of security defenses.

MAL's true strength lies in its extensibility—it provides a base structure that can be adapted into domain-specific languages, each tailored to the unique requirements of different industries. This modular approach allows for highly specialized modeling, ensuring that the language can accurately reflect the specific types of assets, attack vectors, and defensive measures relevant to a given sector. For example, MAL has been extended to model cyber-attacks in fields like IT infrastructures, energy grids, and industrial control systems, each with its own domain-specific version of MAL.

In the context of maritime cybersecurity, MAL has been extended to create harborLang, a language specifically designed to model cyber-attacks on maritime systems. While harborLang will be discussed in detail in the following section, it is important to note that MAL's adaptability made it an ideal foundation for developing a specialized language to incorporate GPS spoofing, AIS spoofing, and other cyber threats unique to the maritime sector. These represent specific attack vectors added to harborLang, which is capable of simulating cyber-attacks targeting the digital and operational systems that vessels and ports rely on. harborLang leverages MAL's attack simulation capabilities to represent complex attack scenarios and assess cyber risks in this critical domain.

2.5. Related Work

Maritime transport, responsible for over 80% of world trade volume[8], faces significant cybersecurity challenges that can disrupt operations and compromise safety. Various studies have proposed solutions, including advanced risk assessment frameworks and threat modeling languages to protect maritime operations. For example, Bayesian networks [9] have been employed to assess cybersecurity risks by probabilistically modeling relationships between threats and vulnerabilities, allowing for dynamic assessments as conditions evolve. Another study[10] presents a comprehensive framework for maritime logistics, focusing on securing communication networks and protecting sensitive data, while emphasizing the need for international collaboration to enhance cybersecurity.

The application of blockchain technology in maritime cybersecurity has also been explored, with research highlighting its potential to secure data exchanges and ensure transparency. Xu and Zhu[11] demonstrate how blockchain's decentralized ledger prevents unauthorized access, improving the security of maritime communications. Additionally, machine learning has been used to enhance threat detection, with studies exploring real-time analysis of network traffic patterns using supervised and unsupervised learning models, which strengthen anomaly detection capabilities.

Research into cybersecurity regulations further underscores the importance of a strong policy framework. Studies highlight gaps in the current regulatory landscape, emphasizing the role of international organizations in developing comprehensive cybersecurity standards for the maritime sector. Effective policies are critical for addressing the increasing sophistication of

cyber threats.

While substantial work has been done to assess individual risks like GPS and AIS spoofing, fewer studies have explored their combined impact. Although tools like securiCAD simulate general cyber-attacks across critical infrastructures, they are often limited when applied to the maritime domain, lacking the specificity needed to model the complex dynamics of maritime operations. Moreover, existing tools generally do not account for multi-vector attacks, where GPS and AIS systems are targeted simultaneously.

To address these gaps, harborLang, developed within the MISSION project, builds upon existing MAL DSLs[12]. harborLang extends MAL by incorporating concepts from both IT and Operational Technology (OT), allowing for the modeling of cyber-attacks on cyber-physical systems that are crucial in maritime operations. harborLang's integration of IT concepts from coreLang[13] and OT concepts from icsLang[14] enables the detailed simulation of GPS and AIS spoofing attacks, addressing the limitations of existing simulation tools in the maritime sector.

3. harborLang

harborLang is a domain-specific language (DSL) designed to model and simulate cyber-attacks targeting the maritime sector. Built as an extension of the Meta Attack Language (MAL), harborLang is specifically tailored to address the unique cybersecurity challenges faced by maritime operations, including vessels, ports, and communication networks. harborLang integrates both Information Technology (IT) and Operational Technology (OT) components, reflecting the diverse cyber-physical systems that operate in modern maritime environments.

As maritime systems become increasingly dependent on digital technologies for navigation, communication, and logistics, the need for robust cybersecurity measures has grown. harborLang is designed to simulate a range of cyber-attacks, including GPS and AIS spoofing, while considering the specific dynamics of maritime operations. The language extends the core concepts of MAL to include maritime-specific assets, attack vectors, and defensive measures, enabling comprehensive risk assessments and threat modeling within the maritime context.

harborLang's ability to model cyber-physical systems—such as navigation systems, vessel management systems, and port infrastructures—makes it an essential tool for assessing vulnerabilities and optimizing defensive strategies against evolving threats. By simulating multi-vector attacks, such as GPS jamming combined with AIS spoofing, harborLang provides a detailed view of how such attacks propagate through interconnected maritime systems and how different defensive measures can mitigate them.

3.1. Components of harborLang

harborLang is designed to model and simulate cyberattacks on critical systems within the maritime sector, addressing both information systems and operational technologies (OT) used in vessel navigation, port operations, and cyber-physical systems (CPS). Within the MISSION project, harborLang serves as a structured framework for assessing security vulnerabilities in key maritime components.

Currently, harborLang focuses on simulating attacks on close harbor traffic systems such as sensors and VHF Data Exchange Systems (VDES), which manage communication between

ships and ports, and Vessel Traffic Management (VTM) systems, responsible for tracking and ensuring the safe flow of vessel traffic. Shipping companies rely on Route Optimization systems, which adjust routes based on real-time conditions, and Fleet Management Systems, which coordinate vessel operations, including maintenance, crew management, and logistics. In port operations, the Port Community System (PCS) enables real-time data exchange among stakeholders, streamlining port activities[15, 16]. Meanwhile, Terminal Operating Systems (TOS) manage logistics at the terminal level, coordinating with systems such as Gate Appointment Systems, Enterprise Resource Planning (ERP), and Berth Planning tools to ensure smooth cargo handling and operational efficiency.

By this work, harborLang is being extended to incorporate new components, expanding upon the concepts proposed by Simon Hacks and Julia Pahl [17], to address future maritime cybersecurity challenges. The Voyage Planning System is one such addition, dynamically adjusting vessel routes based on factors like port readiness, weather conditions, and fuel efficiency. Integrating this system into harborLang enables the modeling of cyber-attacks where compromised route data could mislead vessel navigation, resulting in inefficient routes or navigational hazards. Additionally, with the maritime sector's increasing reliance on Artificial Intelligence (AI) and Machine Learning (ML), harborLang will be enhanced to simulate attacks targeting these technologies. By including AI & ML in the simulation environment, harborLang will model adversarial attacks like data poisoning, potentially leading to inaccurate predictions or navigation errors within autonomous decision-making systems.

Satellite communication is also a critical system to be integrated into harborLang. Vessels depend heavily on satellite data for real-time communication and coordination, making it a prime target for signal jamming or spoofing attacks. By modeling satellite communication, harborLang will allow for a more detailed analysis of how these disruptions affect not only navigation but also the entire flow of data between vessels, ports, and shipping companies. Additionally, harborLang will incorporate Global Positioning System (GPS) and Automatic Identification System (AIS) data, essential for vessel positioning and identification. Attacks on GPS, such as GPS spoofing, or on AIS, where vessel identity or position can be falsified, will be simulated to understand how such attacks can lead to dangerous consequences like collisions or the masking of illicit activities[18].

In summary, the ongoing work in extending harborLang aims to build a more comprehensive tool for simulating cyber-attacks that target interconnected maritime systems. By incorporating these new components, harborLang can provide a robust framework for simulating complex multi-vector cyber-attacks and evaluating their impact on maritime safety and security. As seen in Figure X, these systems are highly interconnected, and attacks on one can cascade through others, emphasizing the need for holistic cyber resilience strategies across the maritime sector.

3.2. Potential communication manipulation attacks on GPS/INS integration

In this section, the focus is on the Route Optimization Sector within harborLang, outlining the potential steps involved in jamming and spoofing attacks (signal manipulations) targeting GPS/INS integration. In this setup, GPS serves as an external system, while INS functions as the internal navigation system within the vessel, crucial for route optimization.

Jamming Attacks disrupt the reception of GNSS signals by emitting signals on the same

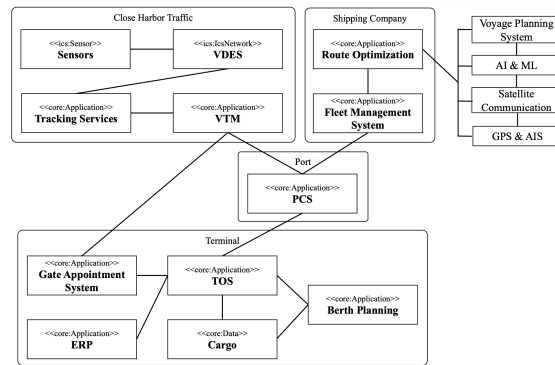


Figure 1: Main Components of Future harborLang

frequency as the GPS, effectively "blinding" the vessel's navigation system. In such cases, the Inertial Navigation System (INS) becomes the fallback solution. The INS, which does not rely on external signals, continues providing time, position, and velocity estimates based on internal sensors. However, these estimates degrade over time due to natural sensor inaccuracies, leading to navigation drift. This drift worsens the longer the jamming attack persists, gradually reducing the reliability of the vessel's navigational data.

Spoofing Attacks, on the other hand, involve the manipulation of GPS signals to deceive the system with false position or time data. Unlike jamming, where the system recognizes the loss of signal, spoofing attacks are insidious because they can introduce false corrections into the system without detection. The vessel's navigation system may interpret these false signals as legitimate, causing it to make erroneous course adjustments. These errors can result in vessels navigating off-course while still believing they are following the correct route.

In the case of a jamming attack, the INS can continue to provide navigational data, although its accuracy deteriorates over time. However, during a spoofing attack, any corrections made based on the falsified GPS data can lead to dangerously incorrect navigation.

Figure 2 illustrates the attack paths affecting time estimates, position, and velocity corrections in GPS and INS systems. It shows how jamming causes transition interruptions while spoofing leads to false information transmission that results in inaccurate corrections. This figure demonstrates the potential impact of these attacks on maritime navigation systems.

By modeling these attacks, harborLang offers a comprehensive framework for simulating spoofing and jamming scenarios. This simulation capability allows maritime organizations to better understand the vulnerabilities of their navigation systems and develop more effective defense strategies.

4. Assessing Cyber Defense Effectiveness in MISSION

In this section, we present the results of simulations conducted using harborLang within the context of the MISSION Project, which focuses on optimising maritime operations while ensuring robust cybersecurity defenses. The simulations evaluate the impact of various cyber-attacks, including GPS spoofing, AIS spoofing, spoofing and communication jamming in GPS-INS

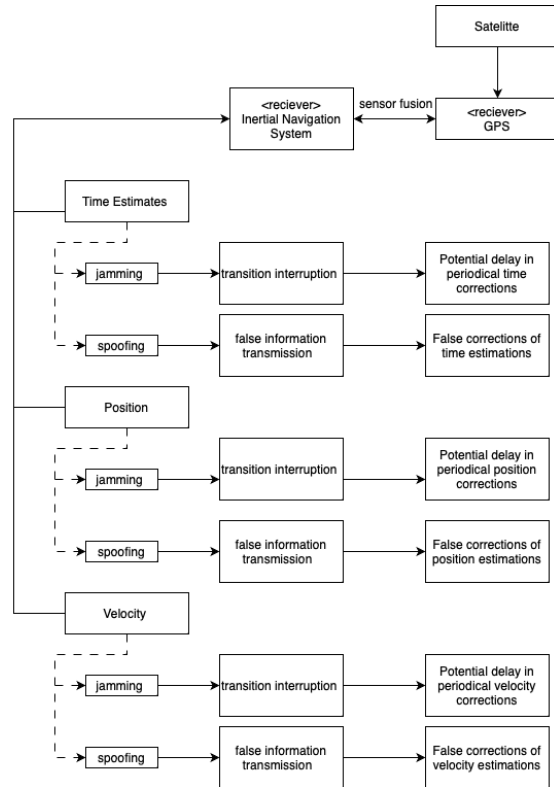


Figure 2: Simulation of potential attack paths in INS/GPS integration

integration. We also assess the effectiveness of different defensive strategies in mitigating these attacks.

4.1. Use Case Description

To evaluate the cybersecurity posture within the MISSION Project, we examine a maritime scenario involving a vessel using advanced integrated navigation and communication systems. The vessel operates between two key ports, Port X and Port Y, under the control of the Vessel Management System (VMS) and communicates in real-time with the Port Management Information Systems (PMIS) at both ports. The vessel’s navigation relies on an Inertial Navigation System (INS) integrated with GPS for accurate positioning.

The system depends on continuous satellite communication to exchange data between the vessel and the ports, including ETA updates, weather forecasts, and port readiness status. Automated data exchange helps optimize port call schedules, reduce fuel consumption, and ensure efficient cargo handling. The vessel’s systems also utilize AIS to broadcast identity and location data to nearby vessels and coastal authorities.

During the voyage, the vessel must maintain positioning accuracy, ensure secure and reliable data transmission, and respond to real-time changes in port schedules or environmental factors. A failure in GPS or AIS data integrity could disrupt the voyage, leading to delays, inefficiencies,

Vulnerability	Severity	Defense Mechanisms
Lack of GPS signal authentication	High	GPS signal integrity monitoring, multi-source navigation (INS)
Dependency on single-source navigation data (INS/GPS)	High	Multi-source navigation (INS, radar), redundant systems
Unencrypted AIS message transmission	Medium	AIS message encryption, message authentication
Weak satellite communication encryption	High	Encrypted satellite communication, frequency hopping

Table 1
Identified Vulnerabilities

or increased risks of collisions in congested areas.

4.2. Potential Cybersecurity Attack Scenario

Based on the previously described use case, we present the following potential attack scenario and its subsequent analysis using YACRAF. The attack involves a multi-stage strategy targeting the vessel's integrated communication and navigation systems, with the aim of disrupting port operations, manipulating navigational data, and causing delays and financial losses. A more detailed attack simulation is performed using harborLang, which serves as input for our risk assessment.

In this scenario, a cyber attacker uses GPS spoofing to mislead the vessel's navigation system, followed by AIS spoofing to broadcast false identity and location data. Additionally, the attacker jams satellite communication, preventing real-time data exchange between the vessel and external systems, further escalating the operational impact. Finally, the vessel's INS begins to drift due to reliance on falsified GPS data, leading to further navigational inaccuracies in velocity, positioning and time estimates.

Based on this attack scenario, we present the following YACRAF-based risk assessment. This analysis evaluates the system's vulnerabilities, the likelihood and impact of threat events, and the overall consequences of the attack. Moreover, we include a set of Tables 1–3, which present an excerpt of the overall risk assessment and will be developed further throughout the project.

5. Conclusions

The MISSION Project significantly advances the optimization of maritime transport by integrating digital real-time port call and voyage optimization tools. By improving coordination and data exchange between vessels and ports, the project aims to reduce fuel consumption, cut greenhouse gas emissions, and enhance overall operational efficiency. However, securing these digital systems against emerging cyber threats is equally crucial to maintaining safe and reliable operations.

Threat Event	Probability of Occurrence (PoO)	Defense Mechanisms
GPS spoofing attack causing misrepresentation of vessel position	High	GPS signal integrity monitoring, multi-source navigation (INS)
AIS spoofing attack resulting in falsified vessel identity	Medium	AIS message encryption, AIS message authentication
Satellite communication jamming disrupting data exchange	Medium	Encrypted satellite communication, frequency hopping

Table 2
Identified Threat Events

Impact	Magnitude	Mitigation Strategies
Vessel misrouting leading to potential collisions	High	Multi-source navigation (INS, radar), GPS integrity monitoring
Falsified AIS messages allowing illegal activities	Medium	AIS message encryption, message authentication, satellite tracking
Disruption of real-time communication between vessel and port	High	Encrypted satellite communication, redundant communication channels

Table 3
Identified Impact

harborLang provides a robust framework for simulating cyber-attacks, including threats like GPS and AIS spoofing, which are particularly relevant to maritime navigation systems. Combined with the YACRAF framework, harborLang enhances risk assessments through model-based security analysis, ensuring that vulnerabilities are identified, evaluated, and mitigated efficiently. This approach enables maritime stakeholders to assess the security of their systems and develop appropriate defenses against potential cyberattacks.

This work contributes to the scientific community by bridging the gap between general IT security frameworks and the specific cybersecurity needs of the maritime sector. By simulating complex cyber-attack scenarios, harborLang and YACRAF provide maritime organizations with advanced tools for risk assessment, helping to safeguard critical infrastructure and improve operational resilience.

Extending harborLang for Future Challenges As the maritime sector continues to adopt new technologies, such as AI-driven autonomous vessels and satellite-based communication systems, harborLang will evolve to address these emerging cybersecurity challenges. The integration of AI & ML components will be particularly important as more vessels rely on these technologies for autonomous navigation and decision-making. harborLang will continue to

assist maritime stakeholders in assessing the risks posed by new technological innovations and developing robust defenses against increasingly sophisticated cyber-attacks.

In conclusion, the MISSION Project, through the integration of harborLang and YACRAF, provides a powerful approach to securing modern maritime operations. By addressing both the operational and cybersecurity challenges of digital transformation, the project contributes to a safer, more efficient, and more sustainable maritime transport system.

Acknowledgement

This work has received funding from European Union's HORIZON research and innovation programme under the Grant Agreement no. 101138583.

References

- [1] International Maritime Organization, Automatic identification systems (ais), International Maritime Organization Website, 2024. URL: <https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx>, accessed: 2024-10-01.
- [2] M. Jones, Spoofing in the black sea: What really happened?, GPS World, 2017. URL: <https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>, accessed: 2024-10-01.
- [3] J. Warner, R. Johnston, GPS Spoofing Countermeasures, Technical Report LAUR-03-6163, Los Alamos National Laboratory, Los Alamos, NM, USA, 2003.
- [4] A. Ranganathan, H. Ólafsdóttir, S. Capkun, SPREE: A Spoofing Resistant GPS Receiver, in: Proceedings of the Conference on Mobile Computing and Networking (MobiCom), New York, NY, USA, 2016, pp. 348–360. URL: <https://doi.org/10.1145/2973750.2973754>. doi:10.1145/2973750.2973754.
- [5] J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, J. Bauer, Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring, Journal of Marine Science and Engineering 11 (2023) 928. URL: <https://doi.org/10.3390/jmse11050928>. doi:10.3390/jmse11050928.
- [6] A. Androjna, M. Perkovič, Impact of spoofing of navigation systems on maritime situational awareness, Transactions on Maritime Science 10 (2021) 361–373. doi:10.7225/toms.v10.n02.w08.
- [7] M. Ekstedt, Z. Afzal, P. Mukherjee, S. Hacks, R. Lagerström, Yet another cybersecurity risk assessment framework, International Journal of Information Security 22 (2023) 1713–1729.
- [8] United Nations, Review of maritime transport 2023, 2023.
- [9] A. Gokce, E. Erturk, A bayesian network-based approach for maritime cybersecurity risk assessment, Ocean Engineering 219 (2021) 110164. doi:10.1016/j.oceaneng.2021.110164.
- [10] M. Schermer, M. van der Vlist, Cybersecurity challenges and solutions in maritime logistics, Journal of Operations Management 68 (2020) 101123. doi:10.1016/j.jom.2020.101123.
- [11] X. Xu, K. Zhu, Blockchain technology for enhancing maritime cybersecurity, Marine Policy 103 (2019) 103670. doi:10.1016/j.marpol.2019.103670.

- [12] S. Hacks, S. Katsikeas, Towards an ecosystem of domain specific languages for threat modeling, in: International Conference on Advanced Information Systems Engineering, Springer, 2021, pp. 3–18.
- [13] S. Katsikeas, S. Hacks, P. Johnson, M. Ekstedt, R. Lagerström, J. Jacobsson, M. Wällstedt, P. Eliasson, An attack simulation language for the it domain, in: H. Eades III, O. Gadyatskaya (Eds.), Graphical Models for Security, Springer International Publishing, Cham, 2020, pp. 67–86.
- [14] S. Hacks, S. Katsikeas, E. Ling, R. Lagerström, M. Ekstedt, powerlang: a probabilistic attack simulation language for the power domain, Energy Informatics 3 (2020).
- [15] V. Caldeirinha, J. L. Nabais, C. Pinto, Port community systems: accelerating the transition of seaports toward the physical internet—the portuguese case, Journal of Marine Science and Engineering 10 (2022) 152.
- [16] A. Moros-Daza, R. Amaya-Mier, C. Paternina-Arboleda, Port community systems: A structured literature review, Transportation Research Part A: Policy and Practice 133 (2020) 27–46.
- [17] S. Hacks, J. Pahl, Cyber security assessment of an interoperable port call and voyage optimization tool, IOP Journal of Physics: Conference Series (to be published) (2024).
- [18] A. Androjna, M. Perkovič, I. Pavić, Cyber security challenges for safe navigation at sea, in: Proceedings of the 14th Annual Baska GNSS Conference, 2022.