Cyber Security Assessment of An Interoperable Port Call and Voyage Optimization tool

Cyber Security Assessment of An Interoperable Port Call and Voyage Optimization tool

Simon Hacks[1] **and Julia Pahl**[2]

[1] Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden
[2] Section for Engineering Operations Management, University of Southern Denmark, Odense, Denmark

E-mail: simon.hacks@dsv.su.se, julp@sdu.dk

Abstract. The MISSION project aims to revolutionize maritime transport by developing a digital tool for real-time optimization of port calls and voyages, thereby reducing fuel consumption, cutting greenhouse gas emissions, and decreasing waiting times through enhanced coordination and information sharing among stakeholders. However, the security of the involved IT systems is critical to ensure safe and reliable operations.

This paper introduces harborLang, a novel threat modeling language tailored for the maritime sector, built on the Meta Attack Language (MAL) framework. harborLang addresses the unique security challenges in maritime transport by enabling the modeling and mitigation of potential threats through detailed attack simulations. By integrating harborLang with the Yet Another Cybersecurity Risk Assessment Framework (YACRAF), the project enhances its risk analysis capabilities, allowing for precise threat scenarios that reflect the maritime environment's complexities. The combined use of harborLang and YACRAF facilitates comprehensive cybersecurity risk assessments, significantly improving decision-making, operational safety, and the overall cybersecurity posture of maritime and port operations.

1 Introduction

Maritime transport is fundamental for the global economy, as it accounts for over 80% of the world's trade [1]. At the same time, emissions of the world fleet increased by 4,7% from 2020 to 2021, harming the global aim for a carbon-neutral future [2]. One angle to reduce emissions within maritime is to address the "sail-fast-then-wait" syndrome, which shows vessels sailing at a predetermined speed to their destination port to find port resources not ready, forcing them to wait as most ports in the world serve ships on a first-come-first-served basis. Communicating terminal or port readiness early allows ships to adjust speed and save fuel. Besides advances in Information Technology (IT), optimizing cargo within one system is unsolved [3]. In addition, communication between relevant stakeholders in the different port call phases is generally low and disorganized.

To address this, the MaritIme juSt in time optimiSatION (MISSION) project will develop a digitalized voyage and port call optimization system, which enables collaboration among stakeholders, thus allowing the synchronization of ship schedules, optimizing ship operations, and port services to enhance operations efficiency and reduce fuel consumption. The developed system will comprise many components that interact and are used in critical infrastructure. Therefore, ensuring the integrity of the system is of significant importance. To achieve this goal, we plan to assess the overall architecture of the developed solution using state-of-the-art methods. Notably, we will apply our risk assessment

framework [4] and integrate it with domain-specific threat modeling and attack simulations using the Meta Attack Language (MAL) [5, 6].

This work presents the first configurations of the risk assessment framework and its integration with a MAL domain-specific language (DSL), the so-called *harborLang*, to meet the maritime domain's requirements. Thereby, *harborLang* presented in this work presents the second iteration of the language [7] based on a method for developing MAL DSLs [8] and the Unified Process for Ontology building (UPON) lite [9].

The rest of this work is structured as follows. Next, we present the background of the MISSION project and the used frameworks. Before the work is concluded, a presentation of harborLang and a more detailed explanation of how the cybersecurity assessment will be executed.

2 Background

2.1 MISSION Project

The MISSION project aims to tackle the inefficiencies in the maritime supply chain, particularly the "sail-fast-then-wait" syndrome, where ships arrive on schedule but must wait due to unprepared ports. Over a planned period of 42 months, this initiative will develop a digital optimization tool that operates in real-time, facilitating better coordination of port call operations among maritime stakeholders. This tool is expected to reduce waiting times at sea, lower fuel consumption, and minimize environmental impacts while enhancing safety. However, the reliance on digital tools and real-time data exchange necessitates robust cybersecurity measures to ensure the integrity, confidentiality, and availability of the information exchanged. Cybersecurity is important because the system's effectiveness relies on accurate and secure data sharing between various stakeholders, such as shipping companies, terminals, ports, and service providers. A cyber attack could disrupt operations, leading to delays, financial losses, and safety hazards, undermining the project's goals of reducing waiting times and emissions.

The University of Southern Denmark leads the project consortium with diverse partners, including universities, research institutes, and industry stakeholders across Europe. Together, they will develop and implement innovative IT systems and analytics tools that enable maritime operations interoperability and efficient logistics management. The collaboration of multiple entities increases the attack surface, making cybersecurity measures even more critical. Ensuring the security of these systems protects sensitive data and operations and fosters trust among the stakeholders, which is essential for successful collaboration and data sharing.

By the project's conclusion, the expected outcomes include a robust decision support system that integrates real-time data for optimizing maritime operations, a reduction in the environmental impact of shipping activities, and a model that can be adapted for broader applications in the maritime and transport sectors. The project also aims to influence policy-making and standardization in maritime logistics, offering a blueprint for the digital transformation of the industry and promoting sustainable transport solutions. This aligns with the EU's goals for a competitive and environmentally sustainable transport sector, underscoring the project's commitment to innovation and sustainability. Cybersecurity is integral to achieving these objectives, as it ensures the resilience and reliability of the systems, supports regulatory compliance, and provides a foundation for scalable and adaptable solutions that can be trusted across different contexts and regions.

2.2 YACRAF

YACRAF (Yet Another Cybersecurity Risk Assessment Framework) [4] is a method that aims at enhancing cybersecurity risk assessments. As IT systems increasingly interweave with societal functions, their susceptibility to cyberattacks has become a critical concern. Existing threat modeling methods, while useful, exhibit notable shortcomings in the enterprise IT risk domain, particularly in holistic risk calculation and real-time adaptability.

YACRAF seeks to rectify these issues by integrating model-based security analysis with quantitative risk assessments to foster a comprehensive understanding of cybersecurity threats and their impacts on business operations. This is achieved through a metamodel (cf. Figure 1) that facilitates detailed threat modeling across IT systems and their interactions. The metamodel is structured around three core domains: vulnerability, threat, and impact. Each domain is composed of specific attributes that help evaluate an organization's cybersecurity posture. The vulnerability domain includes attributes such as the system's weaknesses and potential entry points for attackers. The threat domain encompasses various cyber threat types and their likelihood of exploiting the identified vulnerabilities. The impact domain assesses the potential consequences of successful threats on business operations and values, such as financial losses and reputational damage. The interconnections between these domains represent how

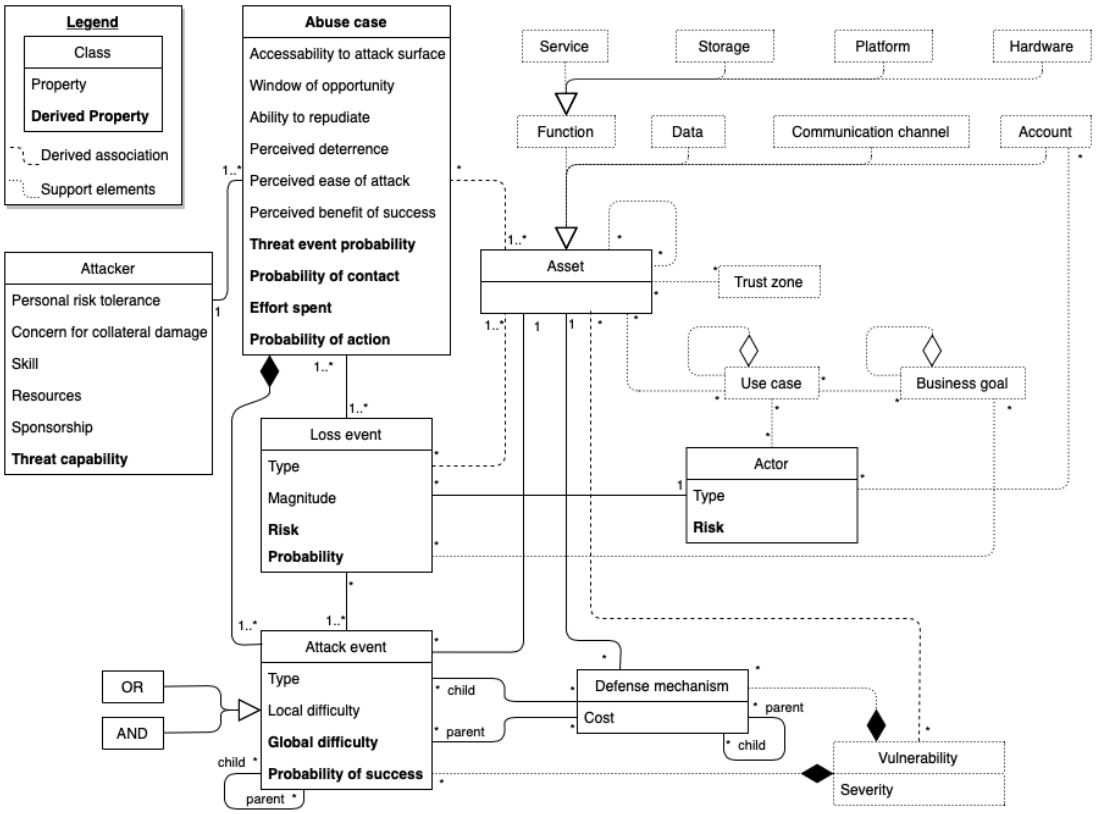


Figure 1: YACRAF Metamodel [4]

vulnerabilities can lead to threats, which, in turn, can have significant impacts. The metamodel supports detailed threat modeling by integrating these elements into simulated attack scenarios, allowing for dynamic risk assessment as conditions evolve. Doing so provides a clearer picture of possible risks and informs the implementation of targeted mitigation strategies, ensuring that organizations can prioritize security measures that align with business objectives.

The framework also includes a formalized approach for calculating risks (cf. Figure 2), which formalizes assessing cybersecurity risks by quantifying threat probabilities, vulnerability exposures, and the potential impacts on business values. This framework introduces a mathematical approach to calculating risk scores, where risk is expressed as a function of these three factors. The probability of a threat event occurring is assessed based on historical data and expert analysis. At the same time, the vulnerability exposure is evaluated by examining the system's security measures and potential weaknesses. The impact is measured by estimating the potential consequences of a successful attack on business operations, including financial, reputational, and operational impacts. This quantitative assessment allows organizations to prioritize risks based on severity and likelihood, facilitating informed decision-making. The framework includes feedback loops for continuously updating risk assessments in response to new information and changing threat landscapes.

The metamodel is organized around three core domains: vulnerability, threat, and impact, each with defined attributes that aid in assessing the cybersecurity posture of an organization. YACRAF's approach identifies vulnerabilities and ties them to potential business impacts through simulated attack scenarios, thus providing a clearer picture of possible risks.

Moreover, the framework emphasizes the importance of real-world application by including a detailed example of how an organization can apply YACRAF to enhance its risk assessment processes. This practical application demonstrates YACRAF's utility in identifying critical vulnerabilities and assessing their potential impact on business continuity and security.

In essence, YACRAF represents a significant advancement in cybersecurity risk management, offering a structured, transparent, and detailed method for organizations to assess and mitigate potential threats. This comprehensive approach enables more informed decision-making and better alignment of

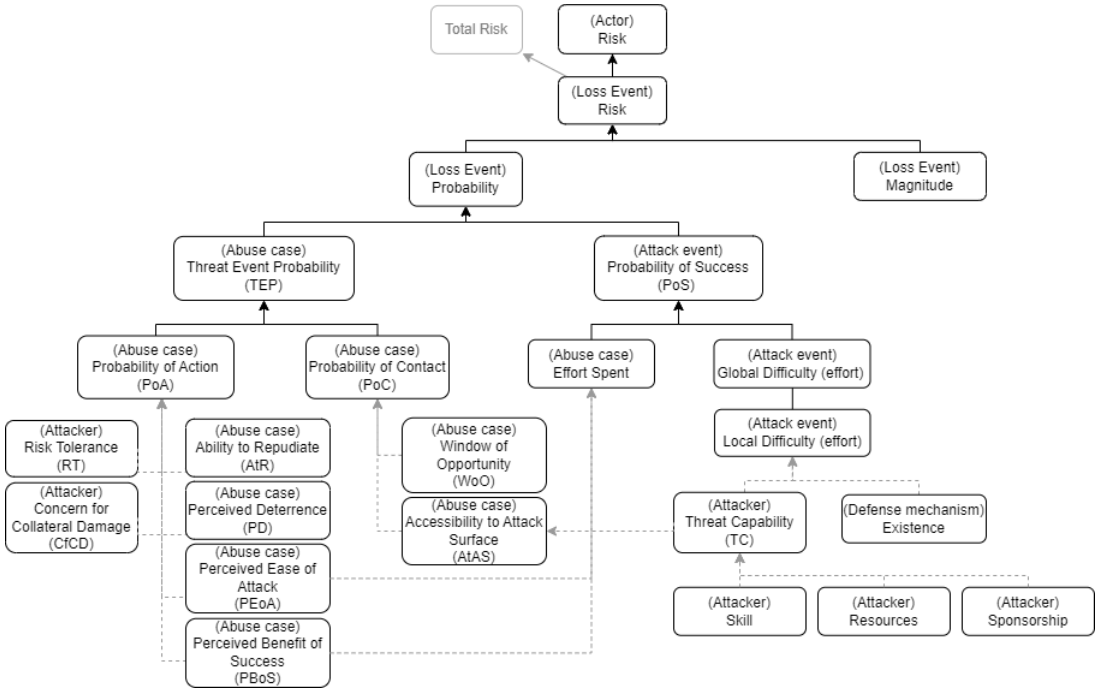


Figure 2: YACRAF Risk Calculation [4]

security measures with business objectives.

2.3 The Meta Attack Language

```
category System {
  asset Network {
    | access
      -> hosts.connect
  }
  asset Host {
    | connect
      -> access
    | authenticate
      -> access
    | guessPwd
      -> guessedPwd
    | guessedPwd [Exp(0.02)]
      -> authenticate
    & access
  }
  asset User {
    | attemptPhishing
      -> phish
    | phish [Exp(0.1)]
      -> passwords.obtain
  }
  asset Password extends Data {
    | obtain
      -> host.authenticate
  }
}

associations {
  Network [networks] *
    <-- NetworkAccess --> * [hosts] Host
  Host [host] 1
    <-- Credentials --> * [passwords] Password
  User [user] 1
    <-- Credentials --> * [passwords] Password
}
```

List. 1: Exemplary MAL Code

A MAL DSL contains the main elements encountered on the domain under study, so-called `assets`. The assets contain `attack steps`, representing the possible attacks.

An `attack step` can be connected with the succeeding `attack steps` so that an attack path is created. Those attack paths comprise attack graphs facilitated in attack simulation. An `attack step` can be either OR or AND, respectively indicating that performing any individual parental `attack step` is required (OR) or performing all parental `attack steps` is required (AND) for the current step to be performed. Attack steps of type OR are defined by the symbol — while AND attack steps are defined by the symbol & before their names.

Furthermore, `defenses` do not allow connected `attack steps` to be performed if they have the value TRUE, which represents them as enabled. Finally, `probability distributions` can be assigned to `attack steps` to represent the effort needed to complete the related `attack step` or the probability of the `attack step` to be possible.

`Asset`s have relations between them that are used to create a model. Those relations are called `associations` and are defined by the <- - and - -> symbols. When associations are specified, a name for the association and cardinalities for both assets should be defined. Inheritance between `asset`s is also possible, and each child `asset` inherits all the `attack step`s of the parent `asset`. Additionally, the `asset`s can be organized into `categories` for purely organization reasons.

Listing 1 presents a domain-agnostic example of a MAL DSL to ease understanding. In this example, four modeled assets can be seen together with the connections of attack steps from one asset to another. In the `Host` asset on line 6, the *connect* attack step is an OR attack step while *access* is an AND attack step. Then, the -> symbol denotes the connected next attack step.

For example, if an attacker performs *phish* on the `User`, it is possible to reach *obtain* on the associated `Password` and, as a result, finally perform *authenticate* on the associated `Host`. In lines 29 to 39, the `associations` between the assets are defined.

2.4 Related Work

Maritime transport, responsible for over 80% of world trade volume, faces significant cybersecurity challenges that can disrupt operations and compromise safety. Various studies have explored these challenges, offering solutions through advanced risk assessment frameworks and threat modeling languages developed to safeguard maritime operations.

For example, Bayesian networks [10] assess cybersecurity risks in maritime operations models by probabilistically modeling relationships between cyber threats and vulnerabilities, allowing for a dynamic assessment of risks as conditions change. Integrating expert knowledge and empirical data provides a risk assessment that guides the implementation of mitigation strategies.

Another work [11] explores the unique cybersecurity challenges faced by maritime logistics and presents a comprehensive framework for addressing these issues. The framework includes best practices for securing communication networks, protecting sensitive data, and ensuring the integrity of maritime operations. It also discusses the importance of international collaboration and the role of policy in enhancing cybersecurity in the maritime sector. The framework emphasizes securing communication networks and protecting sensitive data, highlighting the need for international collaboration and robust policy measures to enhance cybersecurity in maritime logistics.

Xu and Zhu [12] demonstrate the potential of blockchains to secure data exchanges, ensure transparency, and prevent unauthorized access. Blockchain's decentralized and immutable ledger provides a robust mechanism for securing data exchanges, ensuring transparency, and preventing unauthorized access. The study presents case studies demonstrating the effectiveness of blockchain in protecting maritime communications and logistics.

The work by Lee and Kim [13] presents an effective approach to analyzing network traffic patterns and identifying anomalies in real-time. The machine learning models enhance threat detection and response capabilities by leveraging supervised and unsupervised learning techniques within the maritime domain.

Brown and Jones [14] examine the current state of cybersecurity policies and regulations in the maritime industry, identifying gaps and challenges in the existing regulatory framework and suggesting improvements to enhance the industry's cybersecurity posture. It discusses the role of international organizations and the need for coordinated efforts to develop comprehensive cybersecurity standards. Effective cybersecurity policies and regulations are crucial for the maritime industry, requiring coordinated efforts and comprehensive standards to address existing gaps and challenges.

Besides those general works relevant to the overall risk assessment within the MISSION project, harborLang, as a tool for assessing cybersecurity, has two foundations. On the one hand, we base the language on existing MAL DSLs and situate it accordingly in the ecosystem of MAL DSLs [15] with concepts from the IT domain, such as classical office environments and with concepts from the Operational Technology, such as the cyber-physical systems controlling the vessels or the machinery in the harbor. coreLang [16] will cover the IT parts, which provide the basic concepts to model IT systems like applications, related hardware, and communication infrastructure. The operational technology parts will stem from icsLang [17], a language designed for industrial control systems.

All MAL DSLs rely heavily on the concept of threat modeling. Xiong and Lagerström [18] conducted a comprehensive review of the methodologies and tools used in threat modeling to assess security threats. The review categorizes existing threat modeling approaches into several main types, each with distinct methodologies and applications. STRIDE [19], developed by Microsoft, is one of the most widely used frameworks, focusing on Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. PASTA (Process for Attack Simulation and Threat Analysis) [20] is another comprehensive methodology emphasizing a risk-centric approach to evaluating threats based

on business objectives. Attack Trees [21] visually represent potential threats in a tree structure, allowing for intuitive analysis of attack scenarios and their consequences. LINDDUN [22] focuses on privacy threats, helping identify and mitigate privacy risks through a structured approach.

Moreover, harborLang aims to integrate real-time indicators. This has already been applied in different fields, such as financial market data analysis, social media analytics, and IoT sensor data, to improve risk assessment accuracy and timeliness. For instance, a study by Dorfleitner and Rößle [23] explored the incorporation of high-frequency financial data into credit risk models, demonstrating improved predictive accuracy compared to traditional methods. Caldarelli et al. [24] focused on leveraging social media data to predict financial market volatility, showing how sentiment analysis can serve as a real-time indicator of market movements. In cybersecurity, Haque et al. [25] examined real-time network traffic data to identify potential threats, highlighting the role of machine learning algorithms in swiftly processing large volumes of data. The integration of IoT data into risk models has also been explored by Chui and Glover [26], who discussed the benefits of using sensor data for real-time monitoring of physical assets, providing timely alerts to prevent equipment failures.

3 harboLang

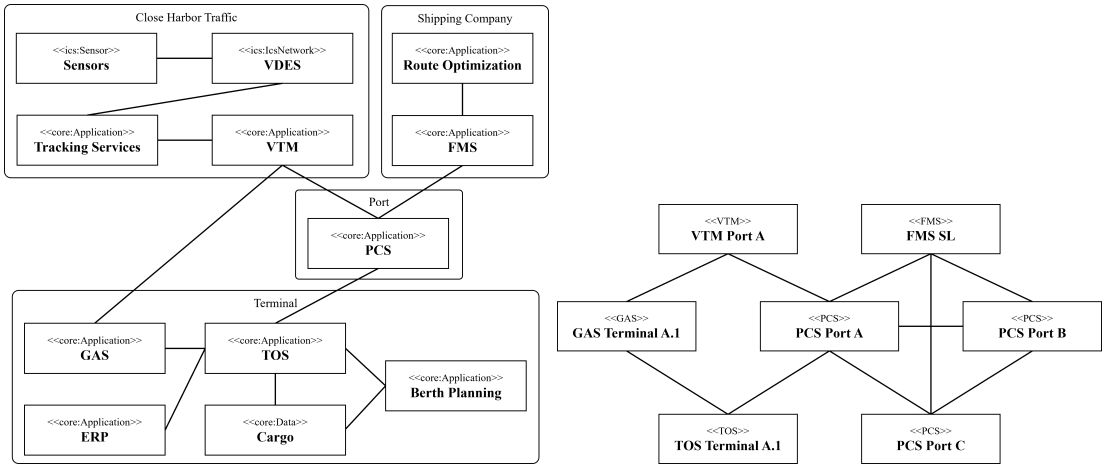
To integrate harborLang with YACRAF, harborLang provides a structured approach to identifying and analyzing potential cybersecurity threats within maritime operations. YACRAF utilizes the detailed threat models generated by harborLang to enhance its risk analysis capabilities. By incorporating harborLang's maritime-specific assets and attack steps into YACRAF, organizations can create precise and detailed threat scenarios that reflect the unique challenges of the maritime environment. This integration enables the simulation of complex attack paths and the evaluation of their impacts, leading to more accurate and actionable risk assessments. Consequently, the combined use of harborLang and YACRAF can significantly improve decision-making, operational safety, and the overall cybersecurity posture of maritime and port operations.

Hacks et al. [8] suggest following an Action Design Research (ADR) [27] approach to create MAL DSLs, and we follow this suggestion as harborLang will be developed in close exchange with the industrial partners of the MISSION project.

ADR structures research projects in four phases: (1) Problem formulation. (2) Building, Intervention, and Evaluation. (3) Reflection and Learning. (4) Formalization of Learning. This work is currently in its initial stages. Here, we are focusing on building harborLang, which is achieved by following the method of UPON lite [9]. The other phases will be performed throughout the project later on. We plan to assess the effectiveness of the developed tools and methodologies, gather stakeholder feedback, and refine the models to meet the project's objectives better. Evaluation will involve systematic testing of the harborLang and YACRAF integration in simulated environments to identify strengths and areas for improvement. Reflection will focus on analyzing the outcomes of these evaluations, considering stakeholder feedback, and understanding the impact of the tools on cybersecurity. This reflective process will help recognize gaps or challenges during the initial implementation, allowing for adjustments and enhancements. Learning will continue throughout the project, leveraging insights gained from evaluation and reflection to refine methodologies, update threat models, and improve overall system resilience. This iterative approach ensures the project adapts to emerging cybersecurity threats and evolving maritime industry requirements. As the project matures, these activities will not only enhance the robustness of harborLang and YACRAF but also contribute valuable knowledge to the maritime cybersecurity field.

UPON lite suggests the following six steps to create ontologies representing domain knowledge: *(1) Lexicon:* In the first step, a lexicon of all terms in the domain is created, including synonyms. To create this lexicon, we rely on existing research in the field and the partners' codified knowledge in the project proposal. For example, Port Community Systems (PCS) are electronic platforms that support communication and integration among various stakeholders within the port community. PCS focuses on improving service levels, partner networks, maritime and freight services, and fostering horizontal collaboration between seaport community partners [28, 29]. Another component is Terminal Operating Systems (TOS), a critical component of port and terminal operations, serving as the backbone for managing the day-to-day activities within a maritime terminal or port [30]. Moreover, there are systems to optimize the routes of the vessels, the (un)loading, and ensure the successful communication between the different parts [31].

The maritime supply chain IT landscape with seaports as intermodal hubs consists of various IT-systems [31] that support the different actors, e.g., vessel traffic management **(VTM)** service providers ensuring incoming/entering traffic based on **sensors** and **tracking services** communicating via very high frequency (VHF) data exchange system (**VDES**) [32]. Shipping companies use fleet



(a) Main Components of Future harborLang (b) Excerpt of an Instance of harborLang

Figure 3: harborLang Excerpt and Illustrative Instance

management systems **(FMS)**, which can include different customized modules such as planned maintenance systems, ship safety management systems, crew management systems, etc., and **route optimization** services which use weather forecasts, sea conditions, and ship's profile to help optimize the route to provide better-informed decisions on routes, ensure crew safety, and reduce voyage costs [33]. It helps to create route options based on time, cost, or fuel constraints, either with or without a given ETA.

Ports employ port community systems **(PCS)**. These are unique platforms that automate data, link individual existing systems of distinct stakeholders, and enable real-time data sharing for interaction and to reduce the administrative burden on ships [34].

Terminals use terminal operating systems **(TOS)** to plan and execute terminal operations, providing functionalities to control storage movement of various **cargo** types and planning of asset usage, labor, and equipment workload, i.e., enterprise resource planning **(ERP)**. **Berth planning** is frequently done using spreadsheet solutions and updating plans in a work-intense and time-consuming endeavor. Gate appointment systems **(GAS)** help orchestrate port-bound cargo traffic.

(2) Glossary: The second step aims to unify the lexicon by identifying synonyms and providing a textual description of the single terms. Here, we restrict ourselves to identifying the synonyms in this iteration, as a detailed description of the different concepts is not yet needed beyond the descriptions provided in the first step.

(3) Taxonomy: The third step focuses on defining a taxonomy of the terms within the glossary. Additionally to this activity, we identify possible hierarchies of harborLang concepts with coreLang [16] and icsLang [17]. This leads to the first outline for harborLang represented in Figure 3a, which can be facilitated by domain experts to assess the cybersecurity of their architecture.

The last steps, (4) Predication, (5) Parthood, and (6) Ontology, will not be further addressed in this iteration.

4 Cybersecurity Assessment of MISSION

4.1 Use Case Description

To demonstrate the cybersecurity assessment within the MISSION project, we will use the following fictitious use case description that is based on the project partners' inputs: A Shipping Line (SL) is optimizing port-to-port communication for a shared maritime service involving three major ports, referred to as Port A, Port B, and Port C. The goal is to overcome siloed data and communication structures by enabling consistent and automated exchange of port call information.

Currently, communication of timestamped registries between these ports is inconsistent, and essential documents are exchanged using non-automated and poorly digitalized means. This leads to a lack of process visibility and operational inefficiencies due to limited predictability for vessel traffic and uncertainty about cargo readiness for intermodal transport.

The use case begins with a vessel from SL operating between Port C, Port B, and Port A. As the

vessel departs from Port C, it sends a preliminary Estimated Time of Departure (ETD) to Ports B and A using integrated digital platforms.

Upon departure from Port C, SL's FMS communicates with Port C's PCS to confirm the completion of loading and other port services. This data is shared with Port B through automated updates, ensuring all parties can access the latest information.

When the vessel arrives at Port B, the FMS interacts with Port B's port systems, providing updated ETD and Estimated Time of Arrival (ETA) information to Port A. Delays or changes in operations are immediately communicated back to Port C and forwarded to Port A, allowing these ports to adjust their schedules accordingly.

When arriving at Port A, the PCS receives real-time updates from Port B's port systems. This ensures that Port A can efficiently plan the vessel's arrival, allocate resources, and prepare the berth and cargo handling facilities within the related TOS. Any delays encountered at Port B are analyzed, and the updated ETD is communicated to all relevant stakeholders in Port A to replan incoming port calls.

The underlying architecture used for the simulation in harborLang is presented in Figure 3b.

4.2 Potential Cybersecurity Attack Scenario

Based on the previously described use case, we illustrate one potential attack scenario and what documentation and analysis look like in YACRAF. A more detailed attack simulation is performed using harborLang that serves as input for our calculations.

In this scenario, a sophisticated cyber attacker targets the integrated port communication system, which includes the FMS, TOS, GAS, and PCS of Ports A, B, and C. The attack's objective is to disrupt port operations, causing delays and financial losses and compromising the integrity of communication between these ports.

The attacker employs a multi-stage strategy, beginning with an initial breach through a phishing email targeting employees with access to the FMS and PCS. Once inside, the attacker moves laterally within the network to gain access to the integrated systems, eventually focusing on the PCS platform to manipulate port call information.

Initial Breach: The attacker sends a phishing email containing a malicious link or attachment. This email targets employees, exploiting the lack of training on phishing attacks and inadequate email security measures. *Defense:* Implementing comprehensive employee training, robust email filtering, and anti-phishing tools are crucial to mitigate this.

Lateral Movement: After breaching the initial defenses, the attacker exploits weak internal network segmentation and inadequate monitoring to move laterally within the network. *Defense:* Network segmentation, intrusion detection systems, and continuous monitoring can significantly reduce this risk.

Targeting PCS: Using stolen credentials or exploiting software vulnerabilities, the attacker gains access to the PCS. *Defense:* Multi-factor authentication, regular software updates and patches, and vulnerability scanning are essential to protect against such exploits.

Manipulation of Port Call Information: The attacker alters ETA and ETD data within the PCS, creating discrepancies in port operations. *Defense:* Implementing data validation protocols, integrity monitoring, and blockchain-based data verification can help maintain data integrity.

Disruption of Operations: The manipulation of port call information leads to delays in vessel docking and cargo handling, financial losses, and reputational damage to port authorities and SL. *Defense:* A comprehensive incident response plan, backup communication channels, and coordination with cybersecurity experts are necessary to mitigate these impacts.

Next, we present the YACRAF-based risk assessment, including the attack scenario and an excerpt of other potential scenarios. Moreover, we include a set of Tables 1- 3, that present an excerpt of the overall risk assessment and will be developed further throughout the project.

Vulnerability Analysis: The identified vulnerabilities include inadequate employee training on phishing, weak network segmentation and monitoring, insecure access controls, and insufficient data validation and integrity checks. The severity of these vulnerabilities is high due to their potential widespread operational impact.

Threat Modeling: The attacker profile shows a high skill level, strong motivation for financial gain and disruption, and substantial resources. The threat events include a successful phishing attack, lateral network movement, and critical port call data manipulation.

Impact Assessment: The business impact encompasses financial losses from operational delays, reputational damage, and potential legal liabilities. The operational impact includes disrupted coordinated port operations, increased fuel consumption due to unscheduled idling, and extended port stays.

Table 1: Identified Vulnerabilities

Vulnerability	**Severity**	**Defense Mechanisms**
Inadequate employee training on phishing	High	Employee training, email filtering, anti-phishing tools
Weak network segmentation and monitoring	High	Network segmentation, IDS, continuous monitoring
Insecure access controls and unpatched software	High	MFA, regular software updates and patches, vulnerability scanning
Insufficient data validation and integrity checks	High	Data validation protocols, integrity monitoring, blockchain-based data verification

Table 2: Identified Threat Events

Threat Event	**Probability of Occurrence (PoO)**	**Defense Mechanisms**
Successful phishing attack	High	Employee training, email filtering, anti-phishing tools
Lateral network movement	High	Network segmentation, IDS, continuous monitoring
Manipulation of port call data	Moderate to High	MFA, regular software updates and patches, data validation protocols, blockchain-based data verification

Table 3: Identified Impact

Impact	**Magnitude**	**Mitigation Strategies**
Financial losses from operational delays	High	Incident response plan, backup communication channels
Reputational damage	High	Coordination with cybersecurity experts
Legal liabilities	High	Compliance with cybersecurity standards and regulations
Disruption of coordinated port operations	High	Incident response plan, backup communication channels
Increased fuel consumption	Moderate	Efficient scheduling, real-time data sharing
Extended port stays	High	Efficient scheduling, real-time data sharing

Risk Calculation: The overall risk score is high, considering the high probability of threat events, moderate to high probability of success, and significant impact magnitude. This necessitates immediate attention and mitigation efforts.

Mitigation Strategies: Enhancing employee training, strengthening network security, improving access controls, and implementing data integrity measures are essential to reduce the risk of such an attack. By addressing these vulnerabilities and improving defense mechanisms, the ports and SL can ensure the integrity and efficiency of their integrated port communication system.

5 Conclusions

The MISSION project significantly advances optimizing maritime transport by integrating digital real-time port call and voyage optimization tools. MISSION aims to reduce fuel consumption, cut greenhouse gas emissions, and decrease waiting times by facilitating better coordination and information sharing among stakeholders. However, ensuring the cybersecurity of the involved IT systems is paramount to maintaining safe operations.

Integrating harborLang, a domain-specific threat modeling language, with YACRAF offers a robust approach to addressing these cybersecurity challenges. harborLang provides a structured methodology for identifying and analyzing potential threats specific to the maritime domain, while YACRAF enhances risk assessment through model-based security analysis and quantitative risk evaluations. This combination allows for precise threat modeling and simulation of complex attack paths, thereby improving risk assessment accuracy and actionable insights.

This work contributes to the scientific community by developing harborLang, a tailored threat modeling language that encapsulates domain-specific security knowledge within the maritime sector. It bridges the gap between general IT security frameworks and the unique requirements of maritime operations, thereby enhancing the comprehensiveness of cybersecurity risk assessments. Integrating harborLang with YACRAF equips maritime organizations with advanced tools to simulate, assess, and mitigate potential cyber threats, leading to more informed decision-making and improved operational safety.

Considering this work, internal validity refers to the degree to which the project accurately measures the impact of its threat modeling and cybersecurity frameworks without being influenced by external factors. This is achieved by focusing on cybersecurity challenges specific to maritime operations. Using DSLs like harborLang, grounded in robust theoretical foundations of MAL [6], enhances the credibility of the internal assessments. Ensuring consistency in the application of harborLang across different scenarios helps isolate the specific effects of the framework on risk assessment outcomes. External validity, on the other hand, pertains to the generalizability of the findings beyond the immediate context of the project. We consider maritime environments by incorporating diverse use cases and stakeholder inputs, strengthening the work's external validity. The frameworks are tested in varied maritime settings, including port configurations and communication protocols, to evaluate their adaptability and robustness in real-world scenarios. Furthermore, collaboration with industry partners and alignment with international cybersecurity standards facilitate the external applicability of the project's results, making them relevant to a broader range of maritime operations. The iterative feedback and refinement processes also enhance internal and external validity by ensuring the tools remain relevant and effective in addressing evolving cybersecurity threats.

Future steps include refining and expanding harborLang to cover a broader range of cybersecurity scenarios. Continuous collaboration with industry partners will ensure the language remains relevant and effective in addressing emerging threats. Additionally, the project aims to standardize harborLang's threat modeling protocols to align with international regulations and best practices, potentially involving global entities such as the International Maritime Organization (IMO). This standardization will facilitate wider adoption and implementation of harborLang across the maritime industry.

In conclusion, the MISSION project, through the integration of harborLang and YACRAF, paves the way for a more secure and efficient maritime transport system. The project's outcomes will contribute to reducing environmental impacts and operational inefficiencies and set a new standard for cybersecurity in the maritime industry.

Acknowledgement

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

We want to thank our colleague Diana Malakhova, Department of Computer and System Sciences, Stockholm University, for her contribution to the latest sketch of harborLang.

References

[1] United Nations. Review of Maritime Transport 2023; 2023.

[2] Hák T, Janoušková S, Moldan B. Sustainable Development Goals: A need for relevant indicators. Ecological indicators. 2016;60:565-73.

[3] Sung I, Zografakis H, Nielsen P. Multi-lateral ocean voyage optimization for cargo vessels as a decarbonization method. Transportation Research Part D: Transport and Environment. 2022;110:103407.

[4] Ekstedt M, Afzal Z, Mukherjee P, Hacks S, Lagerström R. Yet another cybersecurity risk assessment framework. International Journal of Information Security. 2023;22(6):1713-29.

[5] Johnson P, Lagerström R, Ekstedt M. A Meta Language for Threat Modeling and Attack Simulations. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM; 2018. p. 38.

[6] Wideł W, Hacks S, Ekstedt M, Johnson P, Lagerström R. The meta attack language-a formal description. Computers & Security. 2023;130:103284.

[7] Hacks S. Towards a Threat Modeling Language for Vessel Navigation and Port Call Optimization-harborLang. In: EMISA 2024. Gesellschaft für Informatik, Bonn; 2024. p. 10-18420.

[8] Hacks S, Katsikeas S, Rencelj Ling E, Xiong W, Pfeiffer J, Wortmann A. Towards a systematic method for developing meta attack language instances. In: International Conference on Business Process Modeling, Development and Support. Springer; 2022. p. 139-54.

[9] De Nicola A, Missikoff M. A Lightweight Methodology for Rapid Ontology Engineering. Commun ACM. 2016 feb;59(3):79–86.

[10] Gokce A, Erturk E. A Bayesian Network-based Approach for Maritime Cybersecurity Risk Assessment. Ocean Engineering. 2021;219:110164.

[11] Schermer M, van der Vlist M. Cybersecurity Challenges and Solutions in Maritime Logistics. Journal of Operations Management. 2020;68:101123.

[12] Xu X, Zhu K. Blockchain Technology for Enhancing Maritime Cybersecurity. Marine Policy. 2019;103:103670.

[13] Lee H, Kim J. Leveraging Machine Learning for Cyber Threat Detection in Maritime Networks. Computers & Security. 2022;113:102214.

[14] Brown T, Jones L. Cybersecurity Policy and Regulation in the Maritime Industry: Challenges and Opportunities. Marine Policy. 2019;106:103570.

[15] Hacks S, Katsikeas S. Towards an ecosystem of domain specific languages for threat modeling. In: International Conference on Advanced Information Systems Engineering. Springer; 2021. p. 3-18.

[16] Katsikeas S, Hacks S, Johnson P, Ekstedt M, Lagerström R, Jacobsson J, et al. An Attack Simulation Language for the IT Domain. In: Eades III H, Gadyatskaya O, editors. Graphical Models for Security. Cham: Springer International Publishing; 2020. p. 67-86.

[17] Hacks S, Katsikeas S, Ling E, Lagerström R, Ekstedt M. powerLang: a probabilistic attack simulation language for the power domain. Energy Informatics. 2020;3(1).

[18] Xiong W, Lagerström R. Threat Modeling: A Systematic Literature Review. Computers & Security. 2019;84:53-69.

[19] Shostack A. Threat Modeling: Designing for Security. In: Microsoft Press; 2014. .

[20] Morana M. Process for Attack Simulation and Threat Analysis. ISACA Journal. 2010;4:20-30.

[21] Schneier B. Attack Trees. Dr Dobb's Journal of Software Tools. 1999;24(12):21-9.

[22] Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. Privacy Threat Modeling for Trustworthy Software Systems. Science of Computer Programming. 2011;74(9):702-18.

[23] Dorfleitner G, Rößle F. The impact of high-frequency data on credit risk management. Journal of Banking & Finance. 2018;93:225-38.

[24] Caldarelli G, Elefante F, Pappalardo G, Scorza S. Social media data as a source for market volatility forecasting: A review. Computers in Human Behavior. 2021;114:106547.

[25] Haque A, Dinakarrao SM, Kandasamy V. Real-time network threat detection using machine learning. Journal of Network and Computer Applications. 2020;149:102458.

[26] Chui KT, Glover R. The use of IoT in predictive maintenance: A review of the state-of-the-art. Procedia CIRP. 2019;86:276-81.

[27] Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R. Action design research. MIS quarterly. 2011:37-56.

[28] Caldeirinha V, Nabais JL, Pinto C. Port community systems: accelerating the transition of seaports toward the physical internet—the Portuguese case. Journal of Marine Science and Engineering. 2022;10(2):152.

[29] Moros-Daza A, Amaya-Mier R, Paternina-Arboleda C. Port Community Systems: A structured literature review. Transportation Research Part A: Policy and Practice. 2020;133:27-46.

[30] Grafelmann M, Zlotos C, Lange AK, Jahn C. Modelling the IT and business process landscapes at inland intermodal terminals. In: Data Science in Maritime and City Logistics: Data-driven Solutions for Logistics and Sustainability. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 30. Berlin: epubli GmbH; 2020. p. 159-79.

[31] Pagano P, Antonelli S, Tardo A. C-Ports: A proposal for a comprehensive standardization and implementation plan of digital services offered by the "Port of the Future". Computers in Industry. 2022;134:103556.

[32] Šafár J, Hargreaves C, Ward N. The VHF data exchange system. In: Antennas, Propagation & RF Technology for Transport and Autonomous Platforms 2017. IET; 2017. p. 1-8.

[33] Mihailović A, Kapidani N, Lukšić Ž, Tournier R, Vella G, Moutzouris M, et al. Planning a Case for Shared Data Retrieval across the European Maritime Common Information Sharing Environment. In: 2022 26th International Conference on Information Technology (IT). IEEE; 2022. p. 1-6.

[34] Pinto CJ, Anunciacao PF. European seaports information systems. The impacts of directive 2010/65/EU. Economics and Culture. 2020;17(2):38-49.