TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Muhammed Erbas IVCM223533

Application of PASTA Threat Modeling to ECDIS in Autonomous Ships for Enhanced COLREG Compliance

Master's Thesis

Supervisor: Olaf Manuel Maennel
Professor

Co-supervisor: Gábor Visky

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Muhammed Erbas IVCM223533

PASTA OHU MODELLEERIMISE RAKENDAMINE ECDISILE AUTONOOMSETEL LAEVADEL, ET PARANDADA COLREGI NÕUETE TÄITMIST

Magistritöö

Juhendaja: Olaf Manuel Maennel
Professor

Kaasjuhendaja: Gábor Visky

Tallinn 2024

Author’s Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Muhammed Erbas

08.05.2024

Abstract

Autonomous vessels equipped with Operational Technology (OT) and Information Technology (IT) systems increasingly face potentially serious cyberthreats. As the frequency and complexity of these cyberthreats continue to increase, vulnerabilities are becoming more widespread, thus becoming an international security concern. This poses a significant risk to the smooth operations of these vessels. The main objective of this research is to provide a comprehensive overview of this topic and introduce a new concept: using threat modeling to assess the impact of cyberthreats on compliance with the International Regulations for Preventing Conflict at Sea (COLREG). This thesis focuses on developing a threat modeling framework to identify and mitigate cyberthreats and vulnerabilities in the autonomous ship systems.

The chosen methodology is based on the principles of Risk-Centric Threat Modeling, specifically the Process of Attack Simulation and Threat Analysis (PASTA) framework. The framework is adapted to autonomous ships' navigation and decision-making systems to realize this approach. This study comprehensively applies the adapted framework to examine the compatibility of navigation system decision mechanisms with COLREG, thus addressing in advance potential conflicts arising from potential cyberattacks. The results of this research contribute to creating a practical threat modeling framework specifically designed for autonomous vessels, thereby promoting the safe operation of such ships in the maritime industry. In this way, this study aims to reduce the probability of cyberattacks and strengthen the overall security of autonomous vessels. In conclusion, the findings from this study have the potential to provide the safety of autonomous ships and proactively prevent potential cyberthreats that could affect navigation and the failure of COLREG rules.

Keywords: Autonomous Ships, Maritime Cybersecurity, Threat Modeling, ECDIS, COLREG

(The thesis is written in English and is 102 pages long, including 6 chapters, 12 figures, and 1 table.)

List of Abbreviations and Terms

AI	Artificial Intelligence
AIS	Automatic Identification System
APS	Autonomous Passenger Ships
BIMCO	Baltic and International Maritime Council
COLREG	International Regulations for Preventing Collisions at Sea
CYRA-MS	Cyber-Risk Assessment for Marine Systems
DiD	Defense-in-Depth
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
ENC	Electronic Navigational Chart
FMECA	Failure Mode, Effects, and Criticality Analysis
FGSM	Fast Gradient Sign Method
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICS	Industrial Control System
ICT	Information and Communication Technology
IMO	International Maritime Organization
IoT	Internet of Things
IT	Information Technology
LiDAR	Light Detection and Ranging
MaCRA	Maritime Cyber Risk Assessment
MASS	Maritime Autonomous Surface Ships
MCDM	Multi-Criteria Decision-Making
ML	Machine Learning
MPC	Model Predictive Control
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
OT	Operational Technology
PASTA	Process of Attack Simulation and Threat Analysis
RADAR	Radio Detection and Ranging

RBAC	Role-Based Access Control
RCC	Remote Control Center
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
TID	Threat-Informed Defense
VDR	Voyage Data Recorder
VTS	Vessel Traffic Service
YOLO	You Only Look Once

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Motivation

Autonomous ships are equipped with OT and IT systems to increase operational efficiency and reduce human error, which is often a problem in maritime [1]. However, when the literature is examined, it is seen that cyberthreats to these systems have increased, and security vulnerabilities have become widespread. These vulnerabilities can cause significant damage to the ship and the company's ability to carry out effective operations. More importantly, it may become a matter of international security issues [2]. These potential cyber risks include the vulnerability of complex control systems, unauthorized access to the navigation system in the ship's bridge, access to the data of sensors that enable various operations on autonomous ships [3].

The industry needs to address the risks associated with their operation. Ensuring the safety and security of these complex systems is important. These vessels rely on OT and IT systems, including sensors, control systems, and communication networks [4]. Each system is vulnerable to cyberattacks, and a successful attack on one system could risk the entire ship's operation and the environment. While we still face such risks today, autonomous ship security should be emphasized more than it currently receives. With the development of autonomous ships, artificial intelligence (AI) and machine learning (ML), which will manage the movement and capability of the autonomous ship and provide management through sensors that recognize its environment, will be a part of these threats. Therefore, recent research by [5] has shown that the increase in cyber attacks on OT systems is disrupting operations and causing various maritime logistics problems.

Autonomous ships aims to revolutionize the maritime industry by enhancing the efficiency of sea navigation and reducing the risk of human error, which has historically been a factor in maritime accidents. These ships rely heavily on OT and IT systems, such as the Electronic Chart Display and Information System (ECDIS), to autonomously navigate the seas while adhering to the COLREG. However, as the attack surface expands with increased connectivity and autonomy, the literature reveals a growing trend of cyberthreats targeting these systems, which could undermine COLREG's compliance [6]. For instance, a cyberattack that exploits vulnerabilities in the ECDIS could manipulate navigational data, leading to incorrect decision-making by autonomous navigation systems. This could result in the violation of COLREG, such as failing to maintain a safe distance from other vessels or incorrectly navigating crossing situations, thereby increasing the risk of collisions at sea. Moreover, the autonomy of these vessels places a significant reliance on the integrity and availability of sensor data, which is used to make real-time navigational decisions. Cyberattacks that alter or corrupt this data could undermine the ship's ability to interpret and comply with COLREG, thereby compromising the safety of the ship and all surrounding maritime traffic.

1.2 Problem Statement

As the maritime industry continues to develop in the autonomy, ships are being equipped with increasingly sophisticated interconnected navigation systems, most notably ECDIS [7]. This integration also heightens the exposure of these vessels to cyberthreats. OT systems control and operate the ship's physical equipment and systems. These systems are critical components that ensure the ship's mobility and effectively manage all functions of the ship. Another essential function of OT systems is to provide management of the sensors used to collect and analyze data from the ship's environment. These sensors monitor the ship's maneuverability and environmental conditions, enabling the ship to move safely. For example, radar sensors detect other ships and objects near the ship, while Global Navigation Satellite System (GNSS) sensors determine the ship's position [8].

OT systems can be vulnerable to cyberattacks and, if exposed to attacks, can cause severe disruption of the ship's operations or take complete control of the ship, leading to dangerous situations. Therefore, it is important to conduct effective threat modeling and take appropriate cybersecurity measures for the OT systems of autonomous ships. Researching and developing effective threat modeling methods that consider the maritime environment's unique aspects and the potential risks associated with autonomous ships' OT systems is important. The outcomes of this research involve the creation of a threat modeling structure designed for autonomous ships, which will enhance the safe navigation of these vessels within the compliance regulations. By identifying and mitigating potential threats, the safe operation of autonomous ships can be ensured, and the possible economic, environmental, and security risks can be minimized.

Such vulnerabilities can lead to aberrations in navigational decisions by autonomous ships, potentially resulting in deviations from the established COLREG [9]. There is a noticeable gap in the existing literature, particularly in the absence of comprehensive threat modeling that intersects cybersecurity, autonomous ships, and COLREG. This focus on research and analysis undermines the ability to foresee, identify, and mitigate cyberthreats that could prevent an autonomous ship from adapting to these important regulations during critical navigation phases. This research seeks to bridge this gap using the PASTA threat modeling framework. By applying the PASTA framework, the study aims to examine and understand the impact of cyberthreats targeting ECDIS on the compliance of COLREG rules, specifically in the decision-making processes of autonomous ships. The aim is to create a comprehensive framework that enhances cybersecurity measures, enabling autonomous ships to navigate accurately and safely and comply with navigational rules designed to prevent collisions at sea.

1.3 Research Questions

The following main research question is proposed:

How can the threat modeling methodology be adapted to comprehensively model and assess the risks and impacts of cyberthreats on the ECDIS for autonomous ships and ensure compliance with COLREG?

An approach to threat modeling should be adopted to perform threat modeling for ships' OT systems. This approach involves identifying system components, threats, vulnerabilities, and risks and developing appropriate mitigations. With this approach, we have used PASTA quality to identify and analyze potential theories tailored to autonomous ships' specific needs and characteristics. The modeling should consider the unique characteristics of ships, such as navigation, communication, and control systems, and the potential impact of threats on safety, security, and operations. The model should also consider the different attack surfaces and possible attack vectors that can be exploited. The threat modeling we will develop for ECDIS will be used to analyze threats, vulnerabilities, and attacks and will address the important COLREG rules to comply with regulations. To address the main research question, we take two approaches. The first is to identify the cyberthreats faced by autonomous ships; the second is to determine the most suitable threat modeling strategy and highlight the importance of literature contribution. So, the following questions should be answered:

RQ1: Which cybersecurity threats are common in the ECDIS for autonomous ships, and how can these vulnerabilities affect the decision-making process and lead to non-compliance with COLREG rules?

According to the literature, autonomous ships face six main attack surfaces from which unauthorized access can be gained or operations interrupted. These are positioning systems, communication systems, navigation systems, control systems, power systems, and cargo systems [3]. These identified threats can cause critical damage to the autonomous ship system and disrupt operations. We will examine how the different attack vectors can be exploited for the navigation system. Therefore, these attacks will be minimized by the applied methods in this research.

RQ2: How can the PASTA threat modeling methodology be used to identify, assess, and prioritize vulnerabilities in the ECDIS and ensure that navigational decisions are COLREG compliant?

According to the literature, there are several different threat modeling methods. Our research showed that the STRIDE and PASTA methods best fit our problem. PASTA threat modeling is a more comprehensive and structured methodology for threat modeling than STRIDE. PASTA threat modeling includes more structured and formalized processes for threat modeling, such as risk ranking and attack modeling. It is more designed to handle complex systems, a big problem for autonomous ships. STRIDE is a more general methodology that covers a wide range. Our research will seek a better cybersecurity method for autonomous ships with PASTA threat modeling.

1.4 Scope and Goal

This study aims to explore the potential security threats associated with autonomous ships' ECDIS and apply the PASTA threat modeling framework to identify vulnerabilities and risks. The study's scope will involve reviewing the existing literature on autonomous ships, OT and IT systems, COLREG compatibility with autonomous vessels, threat modeling, and risk assessment methodologies. The review will highlight gaps and challenges in the current research and identify areas for further investigation. The collected data will then be used to conduct a PASTA threat modeling analysis of the ECDIS and sub-components, which involves identifying the potential attack paths and the associated threats, vulnerabilities, and risks. By applying the PASTA threat modeling framework, the research aims to uncover specific weaknesses that could be exploited to disrupt the safe navigation of these vessels, leading to potential collisions. This includes comprehensively analyzing the security issues associated with autonomous ships' ECDIS and sub-components and contributing to developing effective mitigation strategies. The analysis will identify the strengths and weaknesses of the PASTA methodology for autonomous ships' ECDIS and suggest improvements to the method where necessary.

1.5 Contribution and Novelty

This research presents a threat modeling approach emphasizing compliance with COLREG by focusing on ECDIS on autonomous ships. By integrating this focus, the method goes beyond traditional cyber security measures to cover navigational safety, a critical aspect of maritime operations. The approach will help to ensure the safe operation of autonomous ships in a maritime industry where security measures and risks are taken to prevent cyber threats and eliminate the consequences of damages caused by these cyber attacks. The proposed threat modeling method will identify potential threats in the OT systems of autonomous ships. This thesis will investigate recent cyber-attacks targeting autonomous ships and examine how these attacks can affect compliance with COLREG rules and lead to collisions.

One of the most important contributions of the method is the decomposing of the autonomous ship systems. This allows us to take the most critical vulnerabilities by categorizing and focusing on them. Providing a framework for mitigating these threats enables the maritime industry to be alert to emerging technologies and take security measures accordingly. The key benefit of using this methodology is that it has proven effective in identifying and mitigating threats in complex systems and provides a security approach for threat modeling on autonomous ships. This prevents significant damage, loss of control, and cyberattacks that could endanger human lives. Furthermore, the research provides valuable insights and practical solutions to improve security measures in the maritime industry, thus contributing to the existing literature.

1.6 Thesis Structure

The rest of the thesis is organized as follows. In Section 2, explained the background information, focusing on autonomous ships, their OT, IT, and the regulatory frameworks governing their navigation, emphasizing the COLREG. Section 3 provides a comprehensive literature review by examining existing research on cybersecurity threats in the maritime domain, various threat modeling and risk assessment methodologies, and the characteristics of COLREG compliance. The methods adopted for this study are detailed in Section 4, highlighting the research design, approach, and data analysis techniques employed. Section 5 presents an in-depth application of the PASTA threat modeling framework to examine COLREG compliance, focusing on cyberthreat identification, analysis, and mitigation in ECDIS and its subsystems. Section 6 discusses these results and concludes findings.

2. Background

This section provides a comprehensive background to support the research into applying the PASTA threat modeling framework to the ECDIS in autonomous ships. It lays the foundation for understanding the critical elements that the research addresses, focusing on autonomous ships, the regulatory frameworks guiding their operation, and the PASTA framework's relevance and application. The emergence of autonomous ships marks a significant shift in maritime technology that aims to revolutionize safety, efficiency, and operational capabilities. These vessels, characterized by their ability to operate with minimal human intervention, stand at the forefront of a new era in maritime transportation.

The introduction of computerized navigation systems, satellite communication, and advanced electronic charting has transformed the way ships navigate and operate. These technologies have improved safety, efficiency, and environmental sustainability, preparing the way for the next frontier in maritime evolution [10]. The latest phase in the evolution of maritime technology is the move towards autonomous ships, often referred to as "*Shipping 4.0*." This phase incorporates cyber-physical systems, integrating AI and Internet of Things (IoT) technologies to create vessels that can navigate, make decisions, and operate with minimal human intervention [11]. Among these, the Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) Project [12], DNV GL's ReVolt [13], and the YARA Birkeland [14] stand out as flagship initiatives, each contributing uniquely to developing autonomous maritime technologies.

MUNIN Project: The MUNIN Project was a collaborative European initiative to explore the feasibility of autonomous ships. Focused on addressing unmanned operations' challenges in navigation, sea traffic management, and onboard systems, the project sought to demonstrate how autonomy could enhance safety and efficiency while reducing operational costs. The MUNIN Project envisioned a future where autonomous ships could operate alongside manned vessels, contributing to a sustainable and efficient maritime transport system [15] [1].

DNV GL's ReVolt: DNV GL's ReVolt is a concept design for a fully electric, autonomous cargo ship with the potential to revolutionize short-sea shipping [16]. With a focus on sustainability and safety, the ReVolt eliminates the need for crew accommodations by operating autonomously, reducing operational costs and increasing efficiency. The vessel

[1] Fraunhofer CML, *MUNIN - Maritime Unmanned Navigation through Intelligence in Networks*, 2016, `https://www.unmanned-ship.org/munin/`

is designed to operate short sea voyages. Its electric propulsion system reduces emissions and minimizes maintenance requirements compared to traditional diesel-powered ships, showcasing autonomous technologies' environmental and economic benefits [13] [2].

YARA Birkeland: The YARA Birkeland project represents a significant leap towards realizing zero-emission, autonomous cargo shipping[17]. Touted as the world's first fully electric and autonomous container ship, the YARA Birkeland is a collaboration between YARA International and Kongsberg Maritime. The vessel aims to automate the processes of loading, offloading, and transporting fertilizers between YARA's production facilities, thereby reducing the need for truck haulage and lowering CO2 emissions. The project underlines the industry's move towards greener, more sustainable shipping solutions. It serves as a model for future autonomous shipping initiatives [14] [3].

MEGURI2040 Fully Autonomous Ship Program: Launched in February 2020, MEGURI2040 aims to revolutionize the maritime industry by addressing critical issues such as crew shortages and enhancing navigational safety through the application of cutting-edge AI, Information and Communication Technology (ICT), and image analysis technologies. With successful demonstrations, including the world's first fully autonomous navigation test with a small tourism boat and the comprehensive use of a fully autonomous navigation system on the container ship SUZAKU [4], MEGURI2040 is paving the way for the future of autonomous maritime operations[18]. The project's ambitious goal for full-scale commercialization by 2025 underscores its commitment to transforming the maritime industry and creating a safer, more efficient future[18] [5].

2.1 Autonomous Ships

Autonomous ships represent a significant evolution in maritime technology, promising enhanced operational efficiency and safety. They incorporate advanced IT and OT systems, including navigational equipment like ECDIS, to navigate the seas with minimal human intervention. The introduction of autonomous ships represents a transformational shift in the maritime industry that promises enhanced safety, operational efficiency, and environmental sustainability. Autonomous ships promise significantly safer maritime operations by reducing the potential for human error, which is a significant factor in maritime incidents

[2] Simon Adams, *ReVolt – next generation short sea shipping*, DNV GL, 2014, https://www.dnv.com/news/revolt-next-generation-short-sea-shipping-7279/

[3] Yara International, *Yara Birkeland Press Kit*, 2022, https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/

[4] Loz Blain, *Autonomous container ship completes 790-km trip from crowded Tokyo Bay*, New Atlas, May 17, 2022, https://newatlas.com/marine/suzaku-autonomous-ship-navigation/

[5] The Nippon Foundation, *MEGURI2040 Fully Autonomous Ship Program*, 2022, https://www.nippon-foundation.or.jp/en/what/projects/meguri2040

and optimizing voyage planning [1]. Furthermore, the efficiency gains from optimized routing and reduced fuel consumption contribute to lower operating costs and a smaller carbon footprint, aligning with global efforts toward environmental sustainability [19].

However, the transition to fully autonomous shipping also presents challenges, particularly regarding regulatory compliance, cybersecurity, and integrating autonomous vessels into the existing maritime framework. The development and application of comprehensive threat modeling frameworks like PASTA to systems such as ECDIS are important in addressing these challenges, ensuring that autonomous ships can safely and effectively navigate the complexities of modern maritime operations.

International Maritime Organization (IMO)[6], and Baltic and International Maritime Council (BIMCO)[7] have established guidelines and recommendations to strengthen maritime cybersecurity measures. From January 2021 [8], ship owners and operators must assess the cybersecurity risks associated with their operational and safety management systems and adopt the necessary protective actions as stipulated by these new protocols. Furthermore, to strengthen cybersecurity in the maritime sector, the International Association of Classification Societies has introduced Unified Requirements E26 and E27, which are planned to apply to newly classified marine structures from July 2024 [9]. E26 focuses on protecting the integration and continuous operation of information and operational technologies within maritime networks. In contrast, E27 emphasizes the security of systems supplied by third parties, underlines the critical nature of ensuring the protection of user interfaces, and sets criteria for the design and development of new equipment before deployment on ships.

Innovation efforts in the maritime sector are accelerating the commercialization of remotely piloted or fully autonomous Maritime Autonomous Surface Ships (MASS) vessels. This shift requires comprehensive regulatory measures to protect any collisions, ensure cargo safety, and maintain ship integrity. IMO is actively working to incorporate these technological developments into its regulatory framework, aiming to balance the advantages of these technologies against concerns about safety, security, environmental impacts, and cost to international trade and industry. This initiative also considers the impact on personnel both at sea and ashore. In response to the technological advancement, IMO started a regulatory scoping study in 2021 to assess the applicability of existing IMO tools to ships with different levels of automation. This was an important step towards establishing a

[6] International Maritime Organization, https://www.imo.org/

[7] Baltic and International Maritime Council, https://www.bimco.org/

[8] International Maritime Organization, "Cybersecurity," https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[9] International Association of Classification Societies, "Unified Requirements E," https://iacs.org.uk/resolutions/unified-requirements/ur-e

regulatory framework for MASS and resulted in significant progress during the Maritime Safety Committee (MSC) sessions, particularly at the 107th session in June 2023 [10], when significant progress was made in developing a target-based regulatory instrument for MASS operations. In addition, a MASS Working Group has been established to support further the MASS Code's development and address related issues. The aim is to adopt a non-mandatory, target-based MASS Code by 2025, with a mandatory code set planned to be implemented by 1 January 2028 [11].

Autonomous ships, often called MASS [20], represent a significant technological leap in the maritime industry. Defined by their ability to operate and navigate with little to no human intervention, these vessels embody the integration of cutting-edge technologies to enhance maritime safety, efficiency, and sustainability. Critical features of autonomous ships include, according to [21]:

1. **Autonomy Levels:** These range from ships with automated processes and decision support to fully autonomous vessels operating independently of human oversight.
2. **Sensors and Data Analytics:** Equipped with sensors, autonomous ships continuously gather data from their surroundings, enabling navigation and decision-making.
3. **Communication Systems:** Advanced satellite and radio communication systems ensure data exchange between the ship, other vessels, and shore-based operations centers.
4. **Integrated Control Systems:** An autonomous ship has an integrated control system that synthesizes sensor data, navigates according to maritime regulations, and executes complex operational commands.

As defined by the IMO, this level of autonomy describes the progressive transition from human-operated to fully autonomous ships, with each level presenting different operational and regulatory challenges as shown in the Table 1. As we have yet to reach level 4, this thesis's research will greatly contribute to taking measures for fully autonomous systems [22].

Level 1 Autonomous Vessels: These vessels incorporate autonomous technologies that augment the capabilities of the onboard crew. The autonomous components are designed to enhance navigational safety and operational efficiency, operating under the supervision and decision-making authority of the human crew.

[10] International Maritime Organization, "MSC 107th Session Summary," https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx

[11] International Maritime Organization, "Autonomous Shipping," https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

Level 2 Autonomous Vessels: At this level, while the vessel still hosts a crew on board, the primary operational control shifts to a remote control center. This represents a hybrid model where the synergy between human oversight and autonomous systems is essential for the vessel's navigation and management.

Table 1. Level of Autonomy and Regulatory Challenges [22]

Level of Autonomy	***Description***	***Operational***	***Regulatory Challenges***
Level 1	Vessels with autonomous components to support the crew's capabilities.	Enhanced navigational safety and efficiency under human supervision.	Integrating autonomous technologies within existing maritime frameworks.
Level 2	Crew on board, but primary operation by remote control center.	Hybrid operation with synergy between human oversight and autonomous systems.	Adapting regulatory frameworks to accommodate remote operational control.
Level 3	Remotely controlled without any crew onboard.	Sophisticated remote-control technologies ensure safe navigation.	Ensuring remote navigation complies with international maritime regulations.
Level 4	Unmanned and fully autonomous, capable of independent operational decisions.	Advanced AI and algorithms for real-time, dynamic decision-making.	Refining regulations to support fully autonomous decision-making and compliance.

Level 3 Autonomous Vessels: Vessels under this category are characterized by their operation without an onboard crew, being remotely controlled from land-based centers. This level marks a significant shift towards greater autonomy, relying on sophisticated communication and control technologies to navigate safely across maritime environments.

Level 4 Autonomous Vessels: This ultimate level of autonomy designates vessels that operate independently without human intervention. Fully autonomous ships utilize advanced AI, sensor arrays, and navigational algorithms to make informed operational decisions, ensuring compliance with maritime regulations, including the COLREG, in real-time and dynamic conditions.

2.1.1 AI in Autonomous Ships

The base layer of AI on autonomous ships encompasses a variety of sensors and devices designed for comprehensive environmental data collection. Technologies such as Radio Detection and Ranging (RADAR), Light Detection and Ranging (LiDAR), and Automatic Identification System (AIS) play an important role in obstacle detection and navigation, while ECDIS and other navigation systems such as RADAR, AIS, GNSS, Voyage Data Recorder (VDR), and sensors, as shown in our scheme Figure 5 as Layer 1, provide critical information on underwater environment, ship identification, and geolocation, respectively [2]. Collectively, these sensors provide a detailed understanding of the marine environment, which is important for AI-driven analysis and decision-making.

The autonomous ship's AI system includes a situational awareness module as a first phase in decision-making [23]. This module processes large data streams collected by onboard sensors to create a consistent image recognition of the ship's environment, including identifying nearby vessels, navigational data, and potential hazards. Advanced image processing algorithms and techniques are used to interact with the sensor data so that the AI system has an up-to-date awareness of the marine environment and its dynamic changes.

Then, the collision avoidance system, built on the situational awareness module, uses AI to assess potential risks and execute navigational maneuvers to avoid collisions [23]. By analyzing the trajectories of nearby objects and predicting their future positions, the AI formulates a safe course of action that complies with maritime regulations and minimizes the risk of accidents. This capability is essential to ensure that autonomous ships can navigate safely in congested waters and challenging maritime scenarios. At this point, the output of the processed data is proportional to the accuracy of the input data, and an error can cause the autonomous ship to take the wrong course of action.

As a result, if the correct route coordination is achieved with the processed data, global route optimization is activated. Global route optimization is another critical function facilitated by AI in autonomous maritime systems [23]. This module takes into account multiple factors, such as weather forecasts, sea currents, sea traffic, and navigational constraints, to determine the most efficient and safe passage for the vessel. Using optimization algorithms and predictive models, the AI system can determine routes that optimize fuel consumption, reduce travel time, and mitigate risks associated with maritime navigation.

The multi-layered architecture of these systems is visualized briefly in Figure 1, which describes the composition and interaction between the different subsystems and their role in the overall ship autonomy. Layer 1 encompasses the primary functional categories, showing the navigation, communication, propulsion, and sensor technologies that feed environmental data into the AI core (see Figure 5). The second layer details specific subsystems and control mechanisms, such as navigation, communication, and data analysis subsystems that pre-process raw data for high-level analysis. Moving to Layer 3, we see the central role of decision-making and autonomy systems, where AI algorithms process information to make autonomous navigation decisions. The top level, Layer 4, represents the AI decision of this data processing, where inputs from all lower levels combine into consistent, AI-driven navigation and collision avoidance decisions, leading to optimized route planning and compliance with maritime regulations. Here, the most

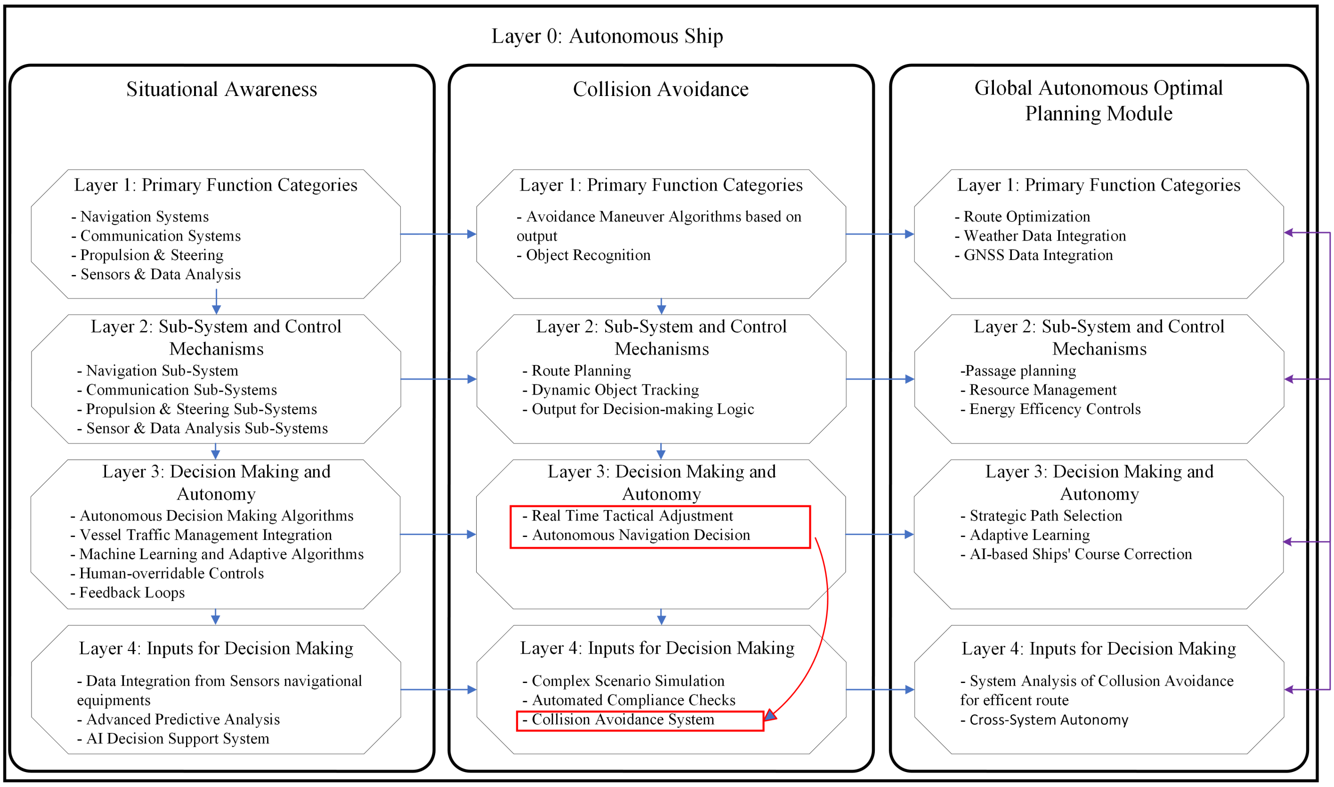
Layer 0: Autonomous Ship
Situational Awareness
Layer 1: Primary Function Categories
- Navigation Systems
- Communication Systems
- Propulsion & Steering
- Sensors & Data Analysis
Layer 2: Sub-System and Control Mechanisms
- Navigation Sub-System
- Communication Sub-Systems
- Propulsion & Steering Sub-Systems
- Sensor & Data Analysis Sub-Systems
Layer 3: Decision Making and Autonomy
- Autonomous Decision Making Algorithms
- Vessel Traffic Management Integration
- Machine Learning and Adaptive Algorithms
- Human-overridable Controls
- Feedback Loops
Layer 4: Inputs for Decision Making
- Data Integration from Sensors navigational equipments
- Advanced Predictive Analysis
- AI Decision Support System
Collision Avoidance
Layer 1: Primary Function Categories
- Avoidance Maneuver Algorithms based on output
- Object Recognition
Layer 2: Sub-System and Control Mechanisms
- Route Planning
- Dynamic Object Tracking
- Output for Decision-making Logic
Layer 3: Decision Making and Autonomy
- Real Time Tactical Adjustment
- Autonomous Navigation Decision
Layer 4: Inputs for Decision Making
- Complex Scenario Simulation
- Automated Compliance Checks
- Collision Avoidance System
Global Autonomous Optimal Planning Module
Layer 1: Primary Function Categories
- Route Optimization
- Weather Data Integration
- GNSS Data Integration
Layer 2: Sub-System and Control Mechanisms
-Passage planning
- Resource Management
- Energy Efficency Controls
Layer 3: Decision Making and Autonomy
- Strategic Path Selection
- Adaptive Learning
- AI-based Ships' Course Correction
Layer 4: Inputs for Decision Making
- System Analysis of Collusion Avoidance for efficent route
- Cross-System Autonomy

Figure 1. Multi-Layered Architecture of Autonomous Ship Systems for Navigation, Collision Avoidance, and Global Route Optimization.

critical point of our study is to emphasize how the Collusion Avoidance System goes through a process while the autonomous ship is making decisions, and the importance of the information provided by the ECDIS to the autonomous ship at this point is emphasized. Most importantly, the critical role of the COLREG rules is also considered to inspect within our PASTA threat modeling.

We have used various sources to create the Figure 1; firstly, from [24], we integrated decision-making responses to adversarial attacks within the collision avoidance module. This informed our design for the decision-making autonomy of Layer 3 and its connection to the decision-making process at Layer 4. This paper has provided valuable insights into the resilience of AI systems on ships, which is essential for building Layer 3: Decision Making and Autonomy for situational awareness. In addition, [2] and [21] categorise various aspects of situational awareness at all layers. These sources provide data on how autonomous ship systems use situational awareness to support reasoning and then direct the output for the collision avoidance module. This helped us to shape the situational awareness module to connect with the control and action phases. We also gained data from [25] on how the autonomous ship integrates situational awareness with the collision avoidance and global planning modules. Their schematic diagrams helped us connect our initial module's layers and create an integrated module. From [23], we gained a general understanding of how situational awareness, collision avoidance, and global autonomous optimal planning modules work together. This provided us with a macro view of the system's operations and enabled our layered architecture to facilitate interactions between modules. Finally, we used the [26] for the development of the collision avoidance module across all layers. This was particularly important for Layer 4 of the collision avoidance system and helped us ensure that our design was efficient and compliant with maritime collision regulations. For layer 1 and layer 2, a detailed explanation has been addressed in Section 5.2.1.

2.1.2 Technological Foundations of Autonomy

As discussed in the [21], the transition to autonomous shipping is underpinned by several core technologies that collectively enable the sophisticated functionalities of these vessels:

1. **AI and ML:** AI algorithms and ML models play a important role in interpreting sensor data, predicting environmental conditions, and making navigational decisions.
2. **GNSS:** Provides location data for accurate navigation and collision avoidance.
3. **IoT:** Enables the interconnectedness of various shipboard systems and components, allowing for real-time monitoring, diagnostics, and control.
4. **Cybersecurity:** Protecting the integrity and confidentiality of data and control systems from cyberthreats is important, given the reliance on digital technologies.
5. **Advanced Propulsion and Energy Systems:** Innovations in propulsion and energy efficiency, including electric and hybrid systems, support the sustainable operation of autonomous vessels.

The development of autonomous ships is not merely an extension of existing maritime technologies but a comprehensive re-imagining of ship design, operation, and management. This paradigm shift towards autonomy promises to address some of the most pressing challenges in the maritime industry, including safety risks associated with human error, the environmental impact of shipping operations, and the growing demand for efficient global trade routes. As this technology continues to evolve, it will undoubtedly shape the future of maritime transportation, ushering in a new era of innovation and progress in the industry.

2.1.3 IT in Autonomous Ships

IT systems in autonomous ships are important for processing data, communication, and other computational needs. These systems support the ship's connectivity, data analysis, and decision-making processes, underpinning the vessel's autonomous functions. The role of IT in autonomous ships cannot be overstated. IT systems serve as the brains of these vessels, processing large amounts of data from various sources like satellite information, oceanographic data, and real-time environmental conditions to make informed navigational decisions. These systems employ AI, ML, and big data analytics technologies to optimize route planning, energy consumption, and cargo management, ensuring operational efficiency surpassing traditional shipping methods.

Navigation and Control Systems, *Sensor Fusion and Data Analysis*, *Communications Systems*, *ML and AI*, *Cybersecurity Measures*, and *Energy Management Systems* are identified as integral components enabling the sophisticated functionalities of autonomous vessels. They collectively enhance the autonomy of ships by facilitating advanced data processing, decision-making, and communication capabilities, thereby ensuring efficient and secure maritime operations.

This exploration underscores the significance of IT systems in the evolution and functionality of autonomous ships, indicating a comprehensive shift towards smarter, more efficient, and safer maritime operations, as discussed in the research [27].

Navigation and Control Systems: These systems use real-time data from GNSS and other navigational sensors to accurately determine the ship's position, speed, and heading. Advanced algorithms process this data to make autonomous navigation decisions, set routes, and avoid obstacles or collisions.

Sensor Fusion and Data Analysis: Autonomous ships have various sensors, including radar, Light Detection and Ranging (LIDAR), sonar, cameras, and weather instruments. Sensor fusion techniques integrate data from these diverse sources, providing comprehensive situational awareness supporting autonomous decision-making.

Communications Systems: Communication technologies ensure that autonomous ships remain in constant contact with satellite systems, other vessels, and shore-based operations centers. These systems facilitate the exchange of navigational data, operational commands, and safety information, enabling remote monitoring and control when necessary.

ML and AI: AI and ML algorithms are integral to processing and interpreting the large amounts of data generated by onboard sensors. These technologies enable the ship to learn from past experiences, predict potential hazards, and make informed decisions autonomously.

Cybersecurity Measures: Given the reliance on digital systems and data exchange, protecting these vessels from cyberthreats is important. Comprehensive cybersecurity frameworks are implemented to safeguard navigation and operational systems from unauthorized access, ensuring the integrity and reliability of autonomous operations.

Energy Management Systems: Optimizing energy consumption and managing power supply are important for the sustainable operation of autonomous ships. IT systems monitor and control fuel usage, battery levels, and the performance of propulsion systems, contributing to energy efficiency and reducing the environmental footprint of maritime operations.

2.1.4 OT in Autonomous Ships

OT systems are responsible for directly controlling and monitoring the physical devices and operations within the ship. This includes the management of propulsion, steering, and other critical systems that ensure the vessel's safe and efficient operation. OT in autonomous ships brings the decisions made by IT systems to life. As highlighted by [28] in their research, the integration and security of OT systems are fundamental to the operational integrity of these vessels. This includes managing and controlling physical shipboard operations such as propulsion, steering, and navigation. OT systems ensure the mechanical aspects of the ship operate with the navigational plans set out by the IT systems. Integrating IT and OT is important; it allows for executing complex maneuvers and adjustments in response to dynamic sea conditions, ensuring safety and compliance with international maritime regulations.

The propulsion and steering mechanisms are at the core of OT systems, which are automated to respond to the navigational commands determined by the ship's control systems. These include engines, rudders, and thrusters, which are optimized for efficiency and sensitivity, enabling the vessel to maneuver through diverse maritime conditions.

Safety systems, another important component of OT, encompass fire suppression, bilge water management, and structural integrity monitoring. These systems are designed to operate autonomously, detecting and responding to onboard emergencies to ensure the ship's and its cargo's safety.

Cargo handling systems in autonomous vessels are automated to manage the loading, stowage, and unloading of goods. These systems utilize robotics and intelligent algorithms to optimize space, secure cargo during transit, and ensure efficient operations in port.

Integration with IT systems is critical for OT systems, as sensor data and navigation systems inform operational decisions. This synergy between IT and OT allows autonomous ships to perform complex maritime tasks independently.

Therefore, this thesis will focus specifically on ECDIS. The decision to focus on ECDIS stems from its critical function in these vessels' navigational and operational safety. ECDIS represents a cornerstone technology that integrates with various OT and IT systems, providing a dynamic platform for electronic navigation charts.

ECDIS

ECDIS is a key component in the navigation of autonomous ships. The architecture and components of ECDIS for autonomous ships are detailed in the [29]. ECDIS provides an integrated platform for Electronic Navigational Chart (ENC) and a range of navigational information, which can be automatically updated in real-time. This system transforms traditional paper chart navigation into a dynamic, interactive process. ECDIS systems enhance navigational accuracy and safety by offering comprehensive situational awareness. They display information about the ship's location, movement, and marine environment, incorporating data from GNSS, radar, and other navigational sensors. Features such as automatic route planning, collision detection algorithms, and alert systems for navigational hazards are integral to ECDIS, facilitating safer and more efficient voyage planning. From our findings of the Chapter 3, we found that the ECDIS is often at the center of cyberthreats for autonomous ships, as shown in our network (Figure 2) and density (Figure 3) diagram. In our network diagram, the nodes vary in size to demonstrate the frequency of each keyword's occurrence in the literature related to autonomous ships and cybersecurity, highlighting the prominence of each concept within this specialized field. The larger nodes, such as *"ECDIS"* and *"autonomous ships"*, signal their higher prevalence in the discussions and studies we've analyzed. The thickness of the connecting lines illustrates the co-occurrence of these keywords within the literature, offering visual insights into the strength of the relationship between these concepts. For instance, the substantial links between *"ECDIS"*, *"navigation"*, and *"collision avoidance"* underscore the close association of these topics in autonomous maritime operations. Because of this, we decided to focus on the ECDIS and its sub-components.

The research highlighted by [30] underscores the urgent need to secure ECDIS systems against cyberthreats, emphasizing their significance in maintaining the safety and efficiency of autonomous maritime operations. For autonomous ships, ECDIS is not just a tool for navigation but a critical component of the vessel's decision-making apparatus. It allows the autonomous control system to make informed decisions about the safest and most efficient

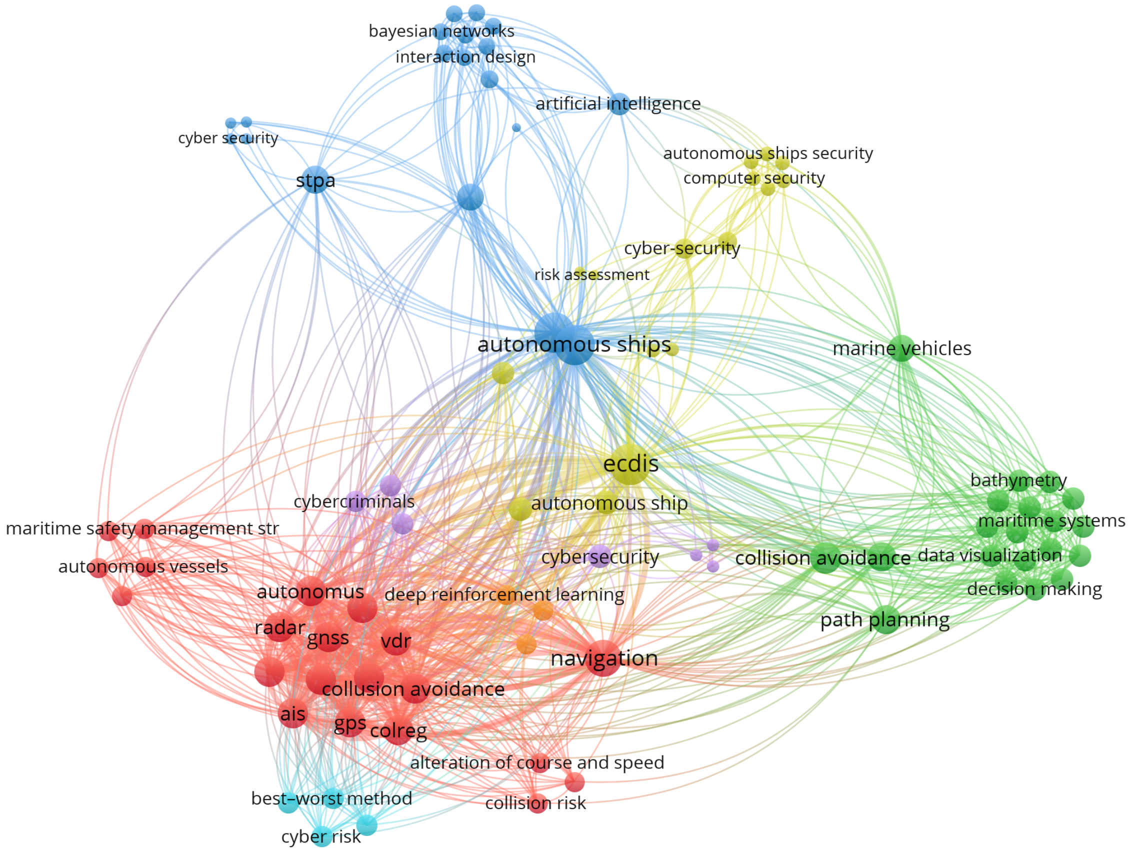

Figure 2. Network diagram for index keywords for literature review focusing autonomous ships using full counting.

routes, considering maritime traffic, weather conditions, and geographical constraints. The integration of ECDIS with other onboard IT and OT systems underscores the collaborative framework essential for autonomous ship operation. This interconnectedness ensures that navigational decisions are informed by real-time data, enhancing autonomous maritime navigation's operational efficiency and safety.

The ECDIS operates at the intersection of IT and OT within the domain of autonomous ships. While traditionally, IT systems are associated with data management, communication, and analysis, and OT systems are directly involved with the operational control of physical devices and processes, ECDIS embodies both aspects.

As an IT component, ECDIS relies on digital data, processing ENC, and integrating real-time information from various sources. [31] highlights the connection of the ECDIS with various subsystems critical to the operation of autonomous ships. This integration includes data from the GNSS, radar, and other navigational sensors to provide a comprehensive overview of the ship's position, navigational status, and the marine environment. The

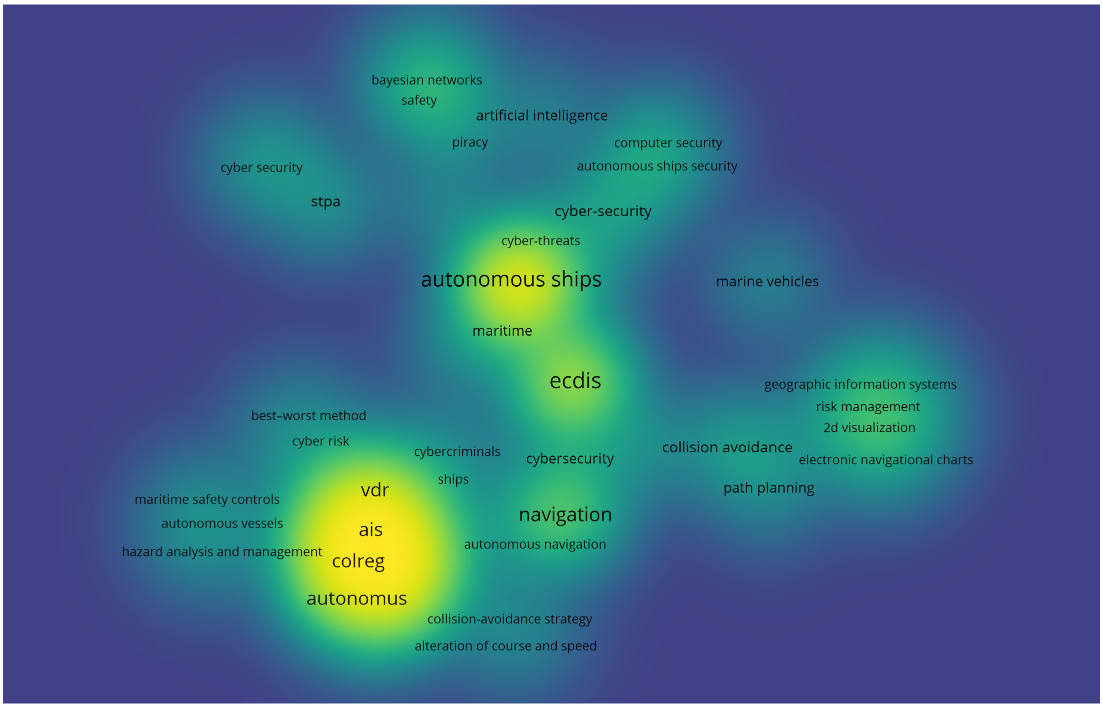

Figure 3. Density diagram for index keywords for literature review focusing autonomous ships using full counting.

system's ability to analyze, update, and display this information dynamically aligns with the core functions of IT systems, focusing on data management and decision support. It plays an important operational role in the navigation and safety of the vessel, directly influencing the ship's course and maneuvering decisions. The system's outputs are integral to the operational processes of the ship, guiding the propulsion and steering mechanisms to respond appropriately. This direct impact on the physical operation of the vessel aligns ECDIS more closely with the characteristics of OT systems.

AIS

AIS is an automatic tracking system used on ships and by vessel traffic services to identify and locate vessels by electronically exchanging data with other nearby ships and AIS Base stations. AIS integrates a standardized VHF transceiver with a positioning system, such as a Global Positioning System (GPS) receiver, along with other electronic navigational sensors, such as a gyro-compass or rate of turn indicator [32]. For autonomous ships, AIS is important in ensuring the vessel can communicate its position, heading, and other relevant information to other ships and maritime authorities, significantly enhancing situational awareness and collision avoidance capabilities.

VDR

VDR is important for autonomous ship operations, called the *"black box"* of maritime vessels. This device records detailed information about the vessel's position, movement, physical status, and command and control for a period leading up to and following an incident [31]. For autonomous ships, the VDR is indispensable for post-incident analysis and is a key tool for continuous improvement in autonomous navigational systems. By capturing a comprehensive dataset, the VDR aids in refining algorithms and decision-making processes, ensuring the autonomous system adheres to navigational standards and regulations.

GNSS

GNSS, like GPS, provides maritime vessels with critical positioning and timing information. GNSS is the backbone of navigation and gives data enabling autonomous systems to accurately determine the vessel's location. Integrating GNSS data ensures that autonomous ships can navigate with precision, maintain course, and avoid navigational hazards, fulfilling essential functions for route planning and execution.

RADAR

RADAR systems are important for detecting and tracking objects such as ships, land, and navigational markers, especially in poor visibility conditions. In autonomous vessels, RADAR systems feed into the decision-making process, allowing the ship to visualize its surroundings and make informed decisions based on real-time data. The information provided by RADAR is key to collision avoidance systems, obstacle detection, and adherence to navigational procedures, ensuring the vessel maintains a safe course.

These components are the initial key elements from which the ECDIS's data comes. It's important when the autonomous ship's decision-making algorithms calculate adjustments in course or speed. We've gone into much detail about each navigational system component as part of the initial phase of the PASTA Threat Modeling process. All of the details of the components of the Navigational system have been described as a part of the PASTA threat modeling first step as explained in Section 5.2.1.

2.1.5 Advantages of Autonomous Shipping

The transition to autonomous shipping marks a big development in maritime operations. These benefits include operational efficiency, safety improvements, and environmental sustainability, all of which contribute to the goal of revolutionizing maritime transportation.

Autonomous ships are set to reshape operational efficiency parameters in the maritime industry. By leveraging advanced technologies such as AI, ML, and sensor data analysis, these vessels can optimize route planning, reduce transit times, and minimize fuel consumption, as discussed by [33]. Automating navigational and operational tasks also reduces manning costs by reducing the need for an extensive crew and allowing more space for cargo. This pattern of facilitated operations increases productivity and contributes to the reliability and predictability of transportation services. One of the most convincing arguments for autonomous maritime adoption is the potential for significant safety improvements. Human error has been identified as one of the leading causes of maritime accidents. Autonomous systems can reduce this risk by ensuring consistent and careful operation. Technologies that are integral parts of autonomous ships, such as collision avoidance systems and real-time environmental monitoring, provide high situational awareness and operational precision, significantly reducing the likelihood of accidents and improving overall maritime safety.

Autonomous ships represent a critical step forward in the maritime industry's journey toward environmental sustainability [34]. These vessels are designed with energy efficiency in mind, incorporating electric propulsion systems, optimized hull designs, and advanced energy management technologies that reduce fuel consumption and lower emissions. By reducing the carbon footprint of maritime operations, autonomous shipping aligns with global efforts to combat climate change and promote a more sustainable future for international trade.

2.1.6 Challenges Facing Autonomous Shipping

One of the most significant barriers to adopting autonomous ships is the current regulatory environment, primarily structured around manned operations. International maritime regulations, including those set forth by the IMO, need to be updated to accommodate the unique aspects of autonomous operations.

Integrating autonomous shipping technologies into the existing maritime infrastructure brings considerable technological and operational challenges. This encompasses the interaction between autonomous and manned vessels, the integration of shore-based control centers, and the compatibility of port operations with autonomous loading and unloading processes. Ensuring that these systems can effectively communicate and operate within the complex maritime environment requires significant advancements in technology and operational practices. Moreover, there is a need for industry-wide standards and protocols to facilitate interoperability and the safe coexistence of autonomous and manned vessels.

2.2 Regulatory Framework

The advancement in autonomous maritime technologies marks a significant shift in maritime activities and requires updates to the regulatory framework and international guidelines to ensure safety, security, and environmental protection. As the leading regulatory body, IMO is critical in establishing these global standards, including addressing how autonomous ships will comply with the COLREG rules. Therefore, to prevent this issue and to contribute to the literature, we have examined the rules that we consider important in this thesis.

2.2.1 COLREG

The COLREG is a comprehensive set of rules authorized by the IMO to ensure maritime safety for ships and other watercraft at sea to prevent collisions [35] [12]. These regulations are essential for manned and autonomous vessel navigation. COLREG consists of 38 rules divided into five sections: Part A - General; Part B - Steering and Sailing; Part C - Lights and Shapes; Part D - Sound and Light Signals; and Part E - Exemptions. Four annexes also detail the technical requirements for lights, shapes, and sound signal appliances. These rules shall apply to all vessels upon the high seas and in all waters connected therewith navigable by seagoing vessels[35].

Part A - General: This section lays the groundwork for the regulations, defining their applicability and the responsibilities of the vessel's master and crew to comply with the rules to avoid collisions. It emphasizes the importance of good seamanship and the discretion to deviate from the rules when necessary to prevent immediate danger. *Part B - Steering and Sailing*: Part B is important for day-to-day navigation, providing detailed rules on vessel movements in various situations. It includes rules on sailing in opposite directions, overtaking other vessels, and navigating in narrow channels and at sea junctions. The section is designed to ensure that vessels' actions are predictable to others, thereby reducing the risk of collisions. *Part C - Lights and Shapes*: This section specifies the lights and shapes vessels must display to signal their presence and activities to other ships. It covers various situations, including sailing, anchoring, and vessel status, ensuring that vessels can communicate their intentions and operations visually, especially during reduced visibility. *Part D - Sound and Light Signals*: Part D outlines the sound and light signals vessels must use to communicate with other ships, especially in conditions of poor visibility or when close encounters are imminent. The rules specify the types of signals used in different scenarios, such as altering course, overtaking, or warning other

[12] International Maritime Organization, "International Regulations for Preventing Collisions at Sea," https://www.imo.org/en/About/Conventions/Pages/COLREG.aspx

vessels of their presence, to prevent misunderstandings and collisions. *Part E - Exemptions*: This final part provides provisions for exemptions from the other rules under specific circumstances, recognizing that not all situations can be addressed through rigid adherence to the regulations. It allows for flexibility in operations, provided that the overall safety of navigation is not compromised.

The development of autonomous shipping brings a unique challenge to the existing COLREG framework, which was primarily designed with manned vessels in mind. Autonomous ships must be able to understand and follow these rules to ensure safe navigation and avoid collisions. This requires advanced sensor systems, algorithms, and AI to interpret the complex scenarios and regulations specified in COLREG and make real-time navigational decisions. One of the key challenges in integrating autonomous ships into the COLREG framework is ensuring that they can comply with the rules, communicate with manned ships, and predict their actions. There is also a need for revisions or new guidelines in COLREG to address situations specific to autonomous navigation, such as the ability to control ships without human intervention or the ability to make decisions remotely. As IMO continues to explore the implications of autonomous shipping, there may be changes or additional protocols in the COLREG specifically tailored to address these new operational paradigms. The aim will be to ensure that autonomous ships can safely coexist with manned ships while maintaining the highest maritime safety standards.

2.2.2 Importance of COLREG in Autonomous Ship Navigation

For autonomous vessels, strict compliance with COLREG is not just a legal requirement but a necessity for operational safety. Ensuring that autonomous navigation systems, particularly ECDIS, can accurately interpret and apply COLREG in real-time scenarios is important for the safe coexistence of autonomous and manned vessels in international waters. Autonomous vessels operate using complex systems that include sensors, AI algorithms, and automated navigation systems. Despite these system's capabilities, they are not immune to failures that can arise from various factors, such as cyberattacks. Such failures could lead to difficulties adhering to the COLREG, especially in dynamic environments or complex maneuvering navigation scenarios.

For instance, a failure in the sensor system could impair an autonomous vessel's ability to maintain an effective lookout as required by *Rule 5 - Look-out*, compromising its ability to appraise the situation and risk of collision fully. Similarly, if the vessel's decision-making algorithms fail to interpret the navigational data accurately, it could struggle to comply with *Rule 8 - Action to Avoid Collision*, which mandates decisive and timely maneuvers to prevent collisions.

Moreover, autonomous ships must be designed to recognize and navigate according to *Rule 10 - Traffic Separation Schemes* and *Rule 19 - Conduct of Vessels in Restricted Visibility*. Errors in these areas can lead to navigational errors, increasing the risk of collision in busy or visibility-limited sea areas.

To address these challenges, autonomous ship development focuses on redundancy in critical systems, and advanced cybersecurity measures. Therefore, this thesis uses a risk-centric approach to address the cybersecurity risk of targeting ECDIS on autonomous ships to indicate COLREG failures. Using PASTA Threat Modeling, it shows the failure of potential COLREG rules that could occur to increase the security of these systems.

2.3 PASTA Threat Modeling Framework

The PASTA framework is a risk-centric approach to threat modeling, offering a structured methodology to identify, evaluate, and mitigate cyberthreats [36] [13]. Its application to autonomous ship navigation, especially ECDIS, is critical for ensuring the systems' security and integrity.

PASTA is an innovative approach to threat modeling designed to align with the risk management and software development life cycle. Its application to autonomous ship navigation systems, particularly ECDIS, is critical for enhancing compliance with the COLREG.

2.3.1 Introduction to PASTA

PASTA is a structured threat modeling methodology specifically designed to identify and address potential security threats in an IT system. This methodology is particularly pertinent to autonomous shipping, where IT and OT systems are important in vessel operation and navigation. Applying PASTA involves a comprehensive seven-step process, each focusing on a critical aspect of threat modeling.

PASTA is a seven-step, risk-centric methodology as shown in the Figure 4 with adopted to our methodology. It aims to provide a threat analysis that is both structured and flexible, integrating well with traditional risk assessment and management processes. The steps in the PASTA methodology are:

1. **System Decomposition:** The first step involves breaking down the autonomous

[13] VerSprite, "What is PASTA Threat Modeling?" `https://versprite.com/blog/what-is-pasta-threat-modeling/`

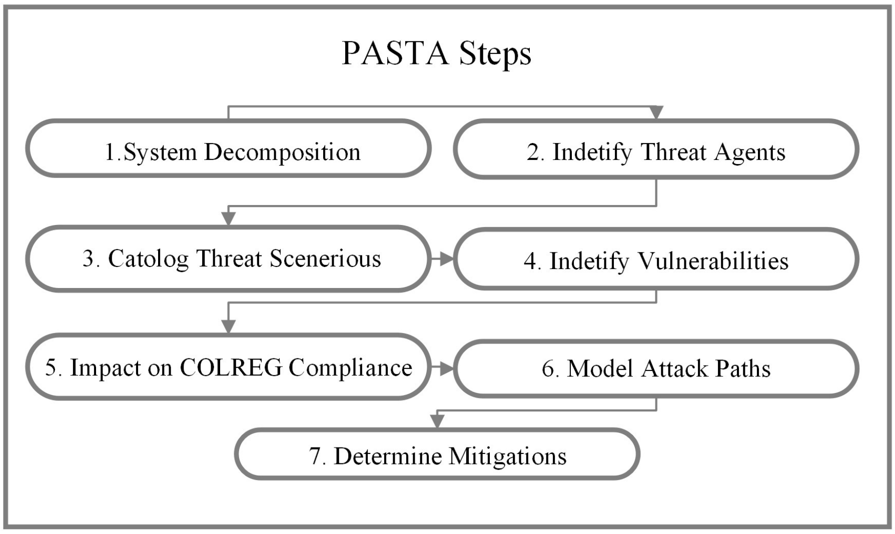
PASTA Steps
1.System Decomposition
2. Indetify Threat Agents
3. Catolog Threat Scenerious
4. Indetify Vulnerabilities
5. Impact on COLREG Compliance
6. Model Attack Paths
7. Determine Mitigations

Figure 4. PASTA Threat Modeling Steps for Autonomous Ships COLREG Compliance.

ship's system into its core components of navigation, propulsion, communication, and sensor systems. This decomposition allows for a detailed examination of each element and its interactions within the more extensive vessel system as shown in the Figure 5. For this thesis, we will focus only on the navigation components.

2. **Identify Threat Agents:**Threat agents are individuals or entities that could potentially exploit vulnerabilities in the system. Identifying these agents is important for understanding the source of threats, ranging from hackers and terrorists to internal personnel or competing corporations.
3. **Catalog Threat Scenarios:** This step involves enumerating the scenarios in which the autonomous ship's systems could be threatened. Scenarios might include cyber-attacks to disrupt navigation, tampering with communication data, or turning off safety features.
4. **Identify Vulnerabilities:** In this phase, the specific vulnerabilities within the autonomous ship's systems that the identified threat agents could exploit are pinpointed. These vulnerabilities could be due to design flaws, software bugs, inadequate security practices, or any other weakness that could be a vector for attack.
5. **Impact on COLREG Compliance:** Evaluating how these vulnerabilities could affect the vessel's ability to comply with COLREG is essential. For instance, a threat compromising navigation systems could violate these regulations and increase the risk of a collision.
6. **Model Attack Paths:** Modeling attack paths involves creating a detailed blueprint of how a threat agent could exploit vulnerabilities to carry out a threat scenario. This helps understand the flow of a potential attack and the points at which the system is most at risk.

7. **Determine Mitigation:** The final step is establishing strategies to mitigate the identified risks. These strategies could include technical solutions like encryption and firewalls, procedural changes like enhanced security protocols, and continuous monitoring for anomalous behavior that may indicate a security breach.

2.3.2 Importance of PASTA in Autonomous Ship Navigation

PASTA plays a critical role in addressing COLREG failures. This analytical framework simplifies a proactive approach to maritime cybersecurity and aligns with navigational safety requirements and regulatory compliance. PASTA's strategic approach deconstructs the complex systems aboard autonomous vessels, identifying potential threats and vulnerabilities. It enables the preparation of special defenses, reducing the risks that could compromise the functionality of important navigation and communication systems.

The advantages of using PASTA's structured approach to threat modeling are that it allows for a detailed and comprehensive analysis of potential security threats, making it an invaluable tool for identifying and addressing vulnerabilities in advance. This is especially true for autonomous maritime, where cybersecurity is important for the vessel's safe operation. By identifying and modeling threats, ship operators can implement security measures that protect against potential cyberattacks that could disrupt navigation or other critical ship systems.

Furthermore, PASTA greatly assists in addressing non-compliance with international safety regulations. By ensuring that all potential threats to ECDIS are considered and mitigated, autonomous vessels can better comply with safety standards, including those required by COLREG. In essence, PASTA enhances the reliability and credibility of autonomous maritime operations by facilitating a risk management strategy that is compliant with safety and regulatory requirements.

3. Literature Review

3.1 Introduction

Upon reviewing the existing literature, it became apparent that there needs to be a significant gap in the analysis of common failures in the navigational systems of autonomous ships, particularly those leading to non-compliance with the COLREG. To address this, we have formulated a main research question as *"How can the threat modeling methodology be adapted to comprehensively model and assess the risks and impacts of cyberthreats on the ECDIS for autonomous ships and ensure compliance with COLREG?"*. We have examined existing research about autonomous vessels and COLREG compliance. To follow that, we have addressed the *RQ1* and *RQ2* by examining the existing literature to enhance our research.

3.2 Autonomous Vessel

This section synthesizes key research findings examining the complexities of protecting autonomous ships against cyberthreats and innovating navigation technologies. By examining the interplay between technological developments, this review aims to illuminate how autonomous ships will be integrated into the global maritime fleet. To start with, [37] highlights growing concerns about cyberattacks on autonomous ships and their potential risks to the maritime industry and international security. [28] addresses the challenges autonomous ships face in cybersecurity. The research particularly emphasizes the development of effective risk management strategies in OT system security. [9] examines the important role of self-guided navigation in evolving sea transportation. It examines the development of system intelligence comparable to a digital navigator derived from human operators to manage approaching vessels and a fuzzy logic-driven framework for collision avoidance to assist the decision-making systems. [38] highlights the complex navigation scenarios anticipated for future ships operating in diverse conditions alongside manned, remotely operated, and fully autonomous vessels, underlining the need for a decision support system that complies with maritime rules and regulations to ensure correct responses from both human operators and automated systems. The consistency of decision-making and action between humans and automated systems during key collision avoidance scenarios has been studied to identify possible gaps in regulatory frameworks in simulated environments. Furthermore, [39] addresses the difficulties in calculating collision risks in actual maritime encounters, given the variable nature of ship positioning and movement, and promotes intelligent systems informed by a thorough grasp of the COLREG. The significance of crafting a decision support tool that mirrors human reasoning and adheres to regulatory standards is emphasized to bolster the safety of next-generation autonomous maritime vessels. Besides that, [40] has studied autonomous ships' general principles and security. By presenting a comprehensive review of autonomous ships' development and potential benefits, five research clusters are technological development, collision avoidance autonomous ship applications, human elements, and regulatory and management issues. [41] explores the role of AI in enhancing maritime cybersecurity, discussing current applications and potential future developments. [42] survey various security models applicable to autonomous maritime systems, important for ensuring the security of these advanced vessels.

These studies comprehensively guide us to understand the operational, technological, and regulatory dimensions critical to advancing and integrating autonomous ships within the maritime industry. The synthesis of these insights has been instrumental in informing the thesis' exploration of autonomous vessel navigation.

3.3 COLREG Compliance with Maritime Regulations

The development of autonomous maritime systems has led to many studies aiming to address the compliance of these systems with COLREG. This chapter helps us to understand the existing literature gap regarding COLREG compliance for autonomous ships.

When looking at the [43] emphasizes the need for an in-depth re-evaluation and possible modification of COLREG to facilitate incorporation of MASS into the existing maritime order while stressing that new regulations must be clear and understandable for both human mariners and automated systems to protect maritime safety. It offers a critical analysis of the COLREG in autonomous maritime operations, pointing out the unclear aspects and the incomplete adherence of existing collision avoidance methods to these rules, which points out the aim of this thesis.

While some research focuses on deep learning and COLREG compliance, for example [44], [38] also highlights the complexity of ensuring that autonomous ships are COLREG compliant through deep learning technologies. The research underscores the potential of deep learning in mimicking human navigational behaviors, ensuring autonomous ships can navigate in compliance with maritime rules. The paper discusses the need for an additional decision support layer to enhance the capabilities of deep learning technologies in identifying and avoiding collision risks, aligning with COLREG's requirements. [45] developed a COLREG-compliant decision support tool to prevent collisions at sea. This tool uses existing ICT and sensor technologies to reduce misunderstandings and non-compliance with COLREG, often attributed to human error. By providing early suggestions in line with COLREG regulations, the tool assists watch-keeping officers in making informed decisions, potentially reducing collisions. Another significant contribution is the exploration of scenario-based Model Predictive Control (MPC) for assessing collision risks in autonomous ships from [46]. This approach emphasizes the predictive aspect of navigating autonomous vessels, ensuring they can plan maneuvers well in advance to comply with COLREG. The study presents a mathematical framework that enables autonomous ships to evaluate potential future scenarios and adjust their course to minimize collision risks. However, an unaddressed gap remains to demonstrate how the COLREG rules might fail in specific scenarios and lead to collisions.

The study on [47] provides insights into the broader aspects of autonomous navigation, touching upon the importance of systems that can autonomously comply with maritime regulations. It illustrates how autonomous navigation systems must integrate with existing maritime safety standards, including COLREG, to ensure that autonomous vessels can safely coexist with manned ships in open seas. Research on [45] introduces a system architecture that integrates various modules with sensor input data. This architecture supports the decision-making process by suggesting appropriate actions when there's a risk of potential collisions, ensuring compliance with COLREG through utilizing AIS data, which is mandatory for all ships. [48] investigates integrating autonomous navigation systems with the COLREG to ensure safe and compliant maritime operations. This research underscores the necessity for autonomous ships to interpret and adhere to COLREG effectively, highlighting the challenge of translating qualitative navigational rules into quantitative actions that autonomous systems can execute. [49] discusses the dynamic interactions between autonomous and manned vessels within the framework of COLREG. It suggests innovative solutions like route exchange and "automation transparency" can enhance mutual understanding and compliance, ensuring the safe coexistence of diverse maritime traffic. In [50], the authors develop an automatic collision avoidance system for unmanned marine craft that adheres to COLREG. They introduce a reactive path planning algorithm that, through simulations, proves capable of generating viable trajectories in the presence of stationary and dynamic obstacles, showcasing a practical approach to compliance with maritime regulations. [51] examines how the subjective nature of "good seamanship" as mandated by COLREG presents challenges for autonomous ship operations. This research identifies the need for clearer guidelines and possibly revising COLREG better to accommodate the capabilities and limitations of autonomous navigation systems. [39] explores innovative methods for ensuring autonomous vessels comply with COLREG by applying deep reinforcement learning. This approach enables ships to make decisions considering the dynamic maritime environment and the inherent navigation risks, aiming to balance operational efficiency and strict adherence to collision avoidance regulations. [52] examines the ambiguities of COLREG when applied to autonomous shipping. This discussion highlights the challenges in translating COLREG's principles into algorithmic decisions, emphasizing the need for more precise definitions and rules that human navigators and autonomous navigation systems can uniformly understand. These studies collectively highlight the advancement in collision avoidance systems, the development of decision support tools, and scenario-based risk assessments as pivotal in aligning autonomous ship operations with COLREG. Furthermore, they address the nuanced challenges of translating the qualitative aspects of COLREG into quantifiable actions for autonomous systems, suggesting a potential gap in current research.

This literature review shows that COLREG compliance within autonomous maritime navigation has been extensively explored across various studies. However, a notable gap exists in explicitly showing how implementing COLREG rules might fail when applied to autonomous ships. While considerable progress has been made in developing technologies and methodologies to ensure compliance, less attention has been paid to systematically identifying and analyzing scenarios where these rules could fail, leading to collisions. This gap underscores the need for further research that continues to explore compliance strategies and examines into the limitations and potential failures of current approaches in real-world autonomous shipping scenarios.

3.4 Cybersecurity Threats in Maritime Domain

Another notable gap is the under-representation of potential cybersecurity risks and vulnerabilities in the ECDIS of autonomous ship navigation to address COLREG failures. Our literature review identified these potential cybersecurity issues to answer *RQ1*.

The maritime industry faces a growing threat of cyberattacks, according to [53]. This issue requires consistent security practices across the sector. Technologies such as AIS, port community systems, and satellite systems enhance safety and security, but cyberthreats like phishing and spoofing create significant challenges. Therefore, studies like [54] examine past cybersecurity incidents in the maritime sector, providing insights into patterns, vulnerabilities, and response strategies. [55] delving deeper into specific cybersecurity issues faced in the maritime industry and how they have been addressed historically. [56] explores instances and allegations of cyberattacks sponsored by nation-states targeting the maritime sector, highlighting the geopolitical dimensions of maritime cybersecurity. [57] discuss creating and applying cyber environments and testbeds designed for the maritime sector. These environments could be important for testing cybersecurity measures and training personnel. [58] provides a comprehensive overview of the various threats faced by the maritime sector, including potential impacts and mitigation strategies. [59] brings attention to the aspects of cybersecurity in the maritime sector, highlighting unique challenges that may need to be more widely recognized and understood. [60] emphasizes the importance of securing critical maritime infrastructures against cyberthreats, recognizing the sector's important role in global trade and security. [61] and [62] focus on specific aspects of maritime cybersecurity, such as the vulnerabilities of radar systems and the evolving nature of cyberthreats in commercial shipping. [63] evaluates the concept of cyber-seaworthiness, which involves ensuring that maritime vessels are physically and digitally secure against cyberthreats. [64] and [65] examines the specific cybersecurity challenges in maritime navigation, including the applicability of existing risk models to the emerging class of autonomous marine surface ships.

Most importantly for our research, it is helpful to use such cyberattacks addressed by [3], which covers potential security risks associated with unmanned maritime vessels, mainly remotely controlled boats, and autonomous ships. This research examines six primary attack surfaces: positioning systems, sensors, firmware upgrades, voyage data recorders, intra-vessel networks, and vessel-to-shore communication. It explores the different types of attacks that could exploit these vulnerabilities. The paper identifies various attacks, such as GPS spoofing, code injection, modification, AIS spoofing, and jamming connection disruption. [5] also examines cybersecurity vulnerabilities in maritime cybersecurity and future research. By reviewing the existing literature on maritime cybersecurity, they identify what research is available and what needs to be added to the maritime industry. [66] presents a systematic method for detecting potential cyberattacks and anomalies in marine navigation systems by analyzing NMEA messages. The main part of the research outlines various attack techniques and anomaly types and suggests detection methods, including frequency-based and specification-based approaches. [67] probes the intricate issues and obstacles linked to the collision avoidance mechanisms of MASS. The maritime industry-specific cybersecurity issues and solutions for the past are given in [55]. In more, [58] reviewed the maritime threats, their possible effects, and ways of mitigation, and also [68] brings simulated attacks on autonomous ships and OT systems and minimizes risk by analyzing threats. [54] gives an overview of the cybersecurity issues in the industry brought to light through past incidents, showing prevalent attack vectors, weaknesses, and defenses. Finally, the work done by [69] has classified cyber attacks against ships and examined threats in detail.

3.5 Threat Modeling and Risk Assessment Methods

The literature review has highlighted the importance of decision support systems and the assessment of ship behavior in collision avoidance scenarios. To address this, we review existing threat modeling approaches and explain why we apply PASTA threat modeling to solve this specific problem. This objective is covered in *RQ2* and guides our approach to solving this critical problem. Firstly, [69] systematic literature review aimed to evaluate and compare existing threat modeling and risk assessment methods in ship cybersecurity, with focusing on ships. The research analyzed 25 papers to identify existing challenges and gaps in the literature. The findings underlined the lack of consistency in existing methodologies and highlighted the need for standardized frameworks that meet the unique needs of autonomous ships. Validation of expert knowledge and support of advanced tools for threat modeling applications was considered important.

Many researchers have conducted various studies on autonomous ships within the scope of threat modeling and risk assessment. For example, potential attacks on manned ships have also been analyzed using the Maritime Cyber Risk Assessment (MaCRA) threat model [70]. Developing another threat modeling with MaCRA, [31] proposes a Multi-Criteria Decision-Making (MCDM) framework for assessing cybersecurity risk in autonomous shipping. The research aims to provide a flexible framework for ensuring cybersecurity in the shipping industry, which is becoming increasingly complex due to the higher cyber-physical interaction required in autonomous shipping operations. While PASTA identifies and mitigates specific vulnerabilities, MCDM ranks different systems and equipment's overall cybersecurity risk. For use in this paper, more emphasis is placed on the PASTA methodology.

A model-based risk assessment called MaCRA is designed to identify and significantly assess cyber risks in the maritime domain. MaCRA serves as an extensive framework designed to tackle cybersecurity risks within the maritime sector, which is particularly important for the operation of unmanned ships. It systematically pinpoints cyberthreats, assesses their potential repercussions, and shapes strategies for risk mitigation and persistent surveillance. This framework aligns with global maritime cybersecurity protocols, which are critical in preserving autonomous maritime infrastructure's security and operational soundness. Informed by the studies highlighted in the works of [71], [31], [72], and [73], the MaCRA framework provides a holistic approach to cybersecurity risk management in the maritime domain. It encapsulates a mixed-methods assessment to craft a comprehensive understanding of the cyber risks specific to unmanned vessels. Through this adaptive and systematic framework, MaCRA enhances the ability to pinpoint and mitigate cyberthreats effectively. It stands out for integrating qualitative and quantitative analyses, confirming its flexibility and depth in addressing cybersecurity within the maritime operations.

When examining through the comparison of PASTA threat modeling, it is clear to see that while the MaCRA framework offers a hybrid approach that melds qualitative and quantitative assessments for maritime cybersecurity, PASTA threat modeling delineates a more sequential process that simulates attack scenarios to inform risk management strategies. Where MaCRA excels in flexibility and a comprehensive perspective, which is important for the dynamic environment of unmanned vessels, PASTA emphasizes a stepwise methodology conducive to detailed threat analysis and system-specific insights. Both frameworks provide strong mechanisms for addressing cybersecurity but differ in their approach: MaCRA, with its broad adaptability to various maritime operations, and PASTA, with its structured, in-depth focus tailored to the intricacies of autonomous navigation systems. The choice between the two could be influenced by the specific requirements of the vessel's operational profile and the nature of the cyberthreats faced.

[74] developed a STRIDE threat modeling that provides a wide range of cyberthreats for autonomous ships. This threat modeling was used to identify potential cyberthreats to autonomous ships and to derive a corresponding analysis. The work on C-ES then proceeds and discusses these risks and proposes appropriate cybersecurity baseline controls to mitigate them[75]. The difference between our methodology and this study is that although both aim to identify and mitigate potential cyberthreats, their approach and focus differ. While PASTA focuses more on identifying potential attack scenarios and defining countermeasures, the modified STRIDE method proposed in this paper focuses more on assessing the cyber risks of cyber-physical systems and proposing appropriate cybersecurity baseline controls to mitigate these risks. Therefore, our work will be improved by considering the work done here, and a more general threat modeling will be used. The STRIDE model, formulated by Microsoft, is a systematic approach for pinpointing security weaknesses in software systems, detailed through an official guide. It classifies threats into six categories: Spoofing identity, Tampering with data, Reputation threats, Information disclosure, Denial of service, and Elevated privileges. The model is crafted to preemptively tackle these security issues during the system design stage, aligning with the proactive stance in software development security outlined by [76]. Initially developed for software, STRIDE has since been adapted for broader applications, including cyber-physical systems and Industrial Control Systems (ICS), due to its comprehensive and well-established threat modeling capabilities, as noted in the literature [77].

As proposed by [25], the Cyber-Risk Assessment for Marine Systems (CYRA-MS) approach introduces a quantitative risk assessment method specifically tailored for cybersecurity in maritime systems, including autonomous vessels. This approach enables ship operators to systematically identify cyber risks and implement effective countermeasures, thereby enhancing the ships' resilience against cyberattacks. Notably, [78] applied this methodology to autonomous inland waterway vessels by prioritizing hazards through a modified formal safety assessment, quantifying risks, and pinpointing uncertainties. Complementing this, bow-tie diagrams ([79]), computational vulnerability scanning ([80]), and probabilistic methods ([71], [31]) offer precise, quantifiable evaluations of risk elements. These techniques underscore the value of quantifying cyberthreats, focusing on measurable and objective risk analysis within the maritime. These methodologies diverge in their application and focus. For instance, [25] utilizes quantitative risk assessments to examine cyberattack scenarios in maritime systems. Conversely, the MV-HARM model by [81] introduces a quantitative, graphical method for assessing risks within vessel networks, presenting a hierarchical visualization of potential cyberthreats and security metrics applicable at various network levels. While these visual tools offer clarity, concerns about their ability to fully capture the complexities of network interactions and cyberthreats may exist. [78] has argued for an integrated approach that considers both safety and security, advocating for developing dynamic and adaptive quantitative methods that can evolve with the maritime industry.

The differences become apparent when presented with PASTA threat modeling, which systematically examines targets, technical scopes, and threats to identify vulnerabilities. PASTA provides a structured framework for identifying targets, such as the operational technology systems of an autonomous ship, ensuring compliance with safety standards, and crafting security mechanisms to protect these assets. In contrast to the quantitative emphasis of CYRA-MS and similar frameworks, PASTA offers a comprehensive process that spans from goal definition through threat analysis, leading to the development of defense strategies. This allows for a holistic understanding of the threat environment, where quantitative methods can inform the various stages of PASTA modeling, ensuring a strong security posture for autonomous maritime operations.

The MITRE ATT&CK framework has been tailored to the maritime sector for adversarial behavior modeling within navigation systems, as explored by [82]. This approach encompasses a comprehensive classification of system components, assessing potential failure modes, and examining the ramifications of these failures. Alongside this, the framework also delves into the computation of risk scores and categorization of risk tiers, focusing predominantly on the detectability aspect of cyberthreats. The methodological application extends to specific maritime components, enabling an exhaustive analysis of cyberthreats and the evaluation of numerous mitigation tactics. Similarly, [83] devised a cyberthreat management strategy for Autonomous Passenger Ships (APS), merging the principles from the MITRE ATT&CK framework with the methodologies of Threat-Informed Defense (TID) and Defense-in-Depth (DiD) strategies. This inclusive approach considers potential failure modes, evaluates their probability and consequences, and computes risk priority numbers as part of a comprehensive risk assessment.

Further integrating MITRE ATT&CK with Failure Mode, Effects, and Criticality Analysis (FMECA) for APS was the initiative of [84]. This integration, MITRE ATT&CK analysed failure modes using enemy tactics and assessed not only their impact on operations, but also their financial and security implications. [85] expanded upon this approach, aligning it with existing standards and using MITRE ATT&CK tactics to pinpoint failure modes. The efficiency of current detection methods was evaluated, the impact of potential failures assessed, and mitigations identified, culminating in a risk prioritization algorithm that guides the selection of countermeasures. A distinct analysis by [86] concentrated on the literature about maritime cyberthreats and the exploration of prominent cyberattack instances within the industry. By mapping out MITRE ATT&CK techniques and tactics to ship systems, a thorough understanding of potential security weaknesses and attack pathways was achieved.

While PASTA's structured, step-by-step analysis is fundamental for uncovering and analyzing vulnerabilities sequentially, using the MITRE ATT&CK framework, particularly in a maritime, emphasizes an adversary-centric perspective. It provides a granular focus on potential attackers' tactics, techniques, and procedures, enabling a detailed mapping of threat actor behaviors to specific system components. This contrast offers insights into the varied maritime cyber risk assessment strategies. PASTA lays out a more traditional threat modeling sequence, and MITRE ATT&CK offers a tactic-based lens to view potential cyberattacks.

As discussed in the literature review, choosing between PASTA and other methodologies such as MaCRA, STRIDE, CYRA-MS, and the MITRE ATT&CK framework involves evaluating cyberthreat identification risk assessment approaches for autonomous maritime operations. PASTA's structured, step-by-step methodology and detailed threat analysis suit the research of this thesis, making it the preferred choice for our research objectives. This fit is evident in the comparative analysis, demonstrating PASTA's ability to provide a comprehensive process from target definition to threat analysis. In the next section, the applicability of PASTA to our research will be further clarified, and the application methodology will be discussed.

After comparing PASTA with other methodologies, we have found PASTA threat modeling fits our scope and research. After that, we conducted extensive research about applying PASTA threat modeling. The methodology has been widely recognized and used in various research fields, highlighting its adaptability and effectiveness in addressing security challenges. In [87], researchers showcase the application of PASTA in the IoT domain, highlighting its ability to mitigate security risks by integrating it into the software development process through a Development, Security, and Operations tool-chain. This approach demonstrates the practical applicability and significant benefits of using PASTA to mitigate vulnerabilities. [88] provides a comprehensive review and shows that PASTA is described as a fundamental methodology for protecting critical assets and effectively managing cyber risks, underlining its structured methodology and asset-centric focus. [89] further explores the utility of PASTA in the IoT and details its adaptability in managing the unique security risks and device limitations inherent in IoT systems. Beyond IoT, it extends to enhancing network security, as discussed in [90], which mentions PASTA alongside other methodologies for analyzing and mitigating threats in network environments. Finally, [91] provides an in-depth analysis of PASTA and advocates its application in various environments due to its flexibility and comprehensive approach to aligning security practices with cybersecurity needs. Together with these studies, we have built our PASTA threat modeling, which was implemented to strengthen autonomous ships' cybersecurity, and our methodology as explained in Section 4.

4. Methodology

4.1 Introduction

This thesis takes a comprehensive approach and at the centre of this research is the adaptation and application of the PASTA framework to assess vulnerabilities in navigation systems, in particular ECDIS. This research has used open access peer-reviewed papers to enrich the analysis and validate the findings, compiling findings that have been validated in scientific academia and used to improve the work.

4.2 Research Design and Approach

The quantitative analysis derived from the PASTA framework allows for a nuanced understanding of the cyberthreat, providing a deep insight into the challenges and solutions for securing autonomous ships. Tailored specifically to autonomous ship navigation systems, the seven phases of the framework guide the analysis from initial system decomposition to the development of targeted mitigation strategies. This process starts with a detailed examination of the navigation devices of autonomous ships, focusing on the decision-making mechanism of ECDIS and AI within it. Subsequent phases include identifying potential cyberthreat actors, cataloging possible threat scenarios, identifying system vulnerabilities, modeling attack paths, and assessing the impact on COLREG compliance.

4.3 Data Collection and Analysis Methods

While investigating the cybersecurity aspects of autonomous ship navigation systems with a focus on ECDIS, the PASTA threat modeling framework supported our data collection and analysis methods. This approach ensured a comprehensive and accurate examination of the topic.

The first phase included a comprehensive literature review. This step was critical to identifying vulnerabilities, attack methods, and countermeasures for autonomous ship systems. By analyzing academic articles and conference papers, we established a solid foundation of current cybersecurity practices and highlighted key gaps in autonomous navigation systems research.

Following the literature review, we performed a system decomposition of the navigation systems of autonomous ships guided by the PASTA framework. Based on the resources we obtained, we developed our own models by improving the results used in academic studies.

The threat identification phase allowed us to map potential cyberthreat actors and analyze their capabilities, intentions, and methods. This step was instrumental in predicting possible threat scenarios that could exploit the identified vulnerabilities and laid the groundwork for a strong threat analysis.

Our vulnerability analysis focused on ECDIS and its subsystems to identify specific vulnerabilities that cyberthreats could exploit. This phase was enriched by insights from the literature review, which provided a comprehensive overview of the potential weaknesses within the system.

Utilizing the information from the previous phases, we modeled attack paths following the results of the literature review. This exercise demonstrated how adversaries could compromise system vulnerabilities to impact navigational integrity and COLREG compliance. The attack modeling served as a visual tool to understand the potential consequences of various cyberthreats and the potential COLREG violations that must be addressed.

The impact of these modeled attack paths on COLREG compliance was assessed, considering the potential for navigational errors, collisions, and other safety risks. This assessment helped prioritize vulnerabilities, guiding the development of targeted mitigation strategies.

4.3.1 Ethical Framework for Utilizing Open-source Materials

Addressing the use of open-source materials to model attack path on autonomous ships, this thesis underlines the necessity of ethical considerations. The research commits to an ethical framework to ensure that such material is used responsibly and aims to improve maritime cybersecurity without allowing malicious exploitation. Balancing the accessibility of information with the potential risks involved, this thesis is committed to ethically advancing the security of autonomous maritime operations.

5. Results

5.1 Introduction

The primary technical contribution of this research is implementing and improving the PASTA threat modeling framework to address cyberthreats targeting ECDIS and subsystems in autonomous ships. The research that developed this specific threat modeling for autonomous ships marks an important technical step in maritime operations and cybersecurity. As the maritime industry advances, this proactive analysis of cyberthreats will be instrumental in ensuring that the deployment of autonomous vessels is technologically advanced and safely compliant with navigational laws and standards. Based on PASTA threat modeling, the structured methodology provided by this study offers a systematic approach to cyberthreat detection and prevention in navigational systems and its decision-making process.

As autonomous maritime technologies evolve and new systems are implemented, the findings and methodologies from this research will provide a foundation for future studies and future-proof the industry against cyberthreats. Wider adoption of autonomous ships will be supported by this framework, contributing to their safe and secure operation in an increasingly automated and interconnected maritime domain. Another important outcome is highlighting the incompatibility of the navigation rules under consideration, namely COLREG, with autonomous ships and contributing to the literature to start its adaptation. This includes a step-by-step presentation of the threats that the selected COLREG navigation rules may create in the future and the results of the mitigations to be adapted to them.

5.2 PASTA Threat Modeling Application

5.2.1 System Decomposition

The decomposition of the ECDIS for autonomous vessels incorporates a multi-layered architectural approach as depicted in our diagram shown in the Figure 5. This structured approach delineates the complex interdependencies and hierarchy of systems that enable autonomous navigation. The overarching architecture integrates both hardware and software elements, aligning navigational functionality with autonomous decision-making capabilities. By collating and synthesizing insights from the literature, we have mapped out the intricate network of sensors, data pathways, and control mechanisms that form the backbone of ECDIS. The resultant schema underscores the transition from traditional seafaring paradigms to a digitally interconnected and self-sufficient navigation system tailored for the emerging era of autonomous ships.

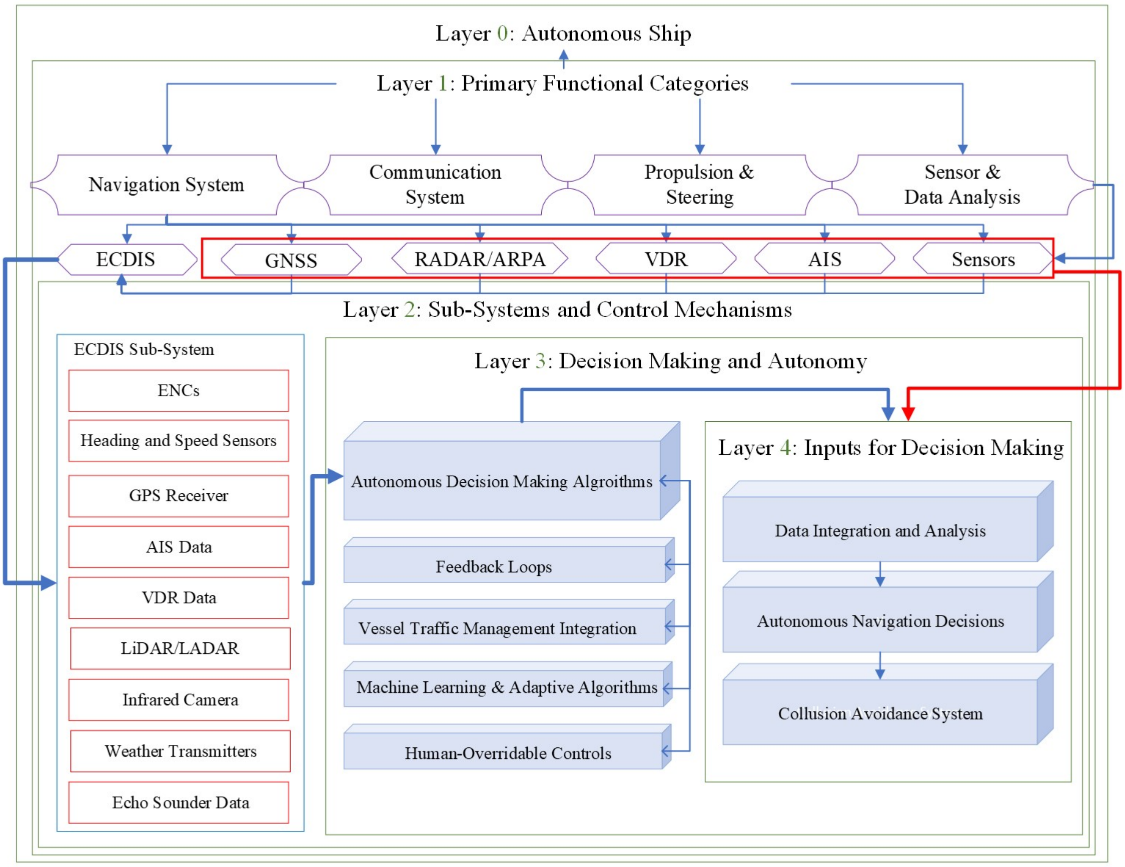
Layer 0: Autonomous Ship
Layer 1: Primary Functional Categories
Navigation System
Communication System
Propulsion & Steering
Sensor & Data Analysis
ECDIS
GNSS
RADAR/ARPA
VDR
AIS
Sensors
Layer 2: Sub-Systems and Control Mechanisms
ECDIS Sub-System
ENCs
Heading and Speed Sensors
GPS Receiver
AIS Data
VDR Data
LiDAR/LADAR
Infrared Camera
Weather Transmitters
Echo Sounder Data
Layer 3: Decision Making and Autonomy
Autonomous Decision Making Algroithms
Feedback Loops
Vessel Traffic Management Integration
Machine Learning & Adaptive Algorithms
Human-Overridable Controls
Layer 4: Inputs for Decision Making
Data Integration and Analysis
Autonomous Navigation Decisions
Collusion Avoidance System

Figure 5. Decomposition of ECDIS and Decision-Making Algorithms.

In constructing the multi-tiered decomposition of ECDIS and the decision-making architecture for an autonomous ship, our methodology integrates insights from a spectrum of seminal works. The schematic of network interactions is adapted from the foundational research on [92], providing a road map for understanding the potential cyber-physical interplays within an autonomous ship's framework. Contributions from [58] underpin the inclusion of sophisticated automation systems for autonomous ships, emphasizing the criticality of cybersecurity in an industry advancing towards autonomy. The [74] study informs our system architecture design.

Further enrichment of the ECDIS subsystems' depiction draws from [30], which elucidates the technical prerequisites and security imperatives of maritime navigation systems in contemporary cyber-physical ecosystems. To capture the nuances of ECDIS integration within autonomous ships, we reference [93], giving the key schemes of IT and the OT components for autonomous ships.

The dynamic between different layers of the decision-making process for MASS is articulated through the lens of [94]. In contrast, [95] provides us with a structured technology framework for autonomous ship navigation, the communication between Layer 3 and the ECDIS subsystems, and outputs that come to the collision avoidance system.

From [96], we extracted the essence of the decision-making layer, detailing the complex network of OT and IT devices and the important role of AIS in maritime communication schemes. This work and [28] shape our understanding of autonomous ships' overarching OT and system architecture overview.

To delve into the communication dynamics within the decision-making hierarchy, [2] highlights the critical interactions between situational awareness instruments and autonomous decision-making algorithms. More detailed, it gives us a reference to a detailed communication scheme between the Layer 3 decision-making phases consisting of communication between situational awareness detection equipment like Radar, LiDAR, AIS, and the autonomous decision-making algorithms.

Addressing the human element, [97] provides insight into the mechanisms that enable human override controls, ensuring that human expertise remains a fail-safe with autonomous decision-making algorithms as our main concept.

The link between ECDIS sub-components and Layer 3 - decision-making is further clarified by [98], which maps out the safety control structure within an autonomous vessel. The [99] showed us the Three-layered approach for driving a vessel for autonomous ships which describes our Vessel traffic management integration.

The concept design for the Layer 4 data and their connection to each data from the decision-making and autonomy are referenced from [100]. This is complemented by the focused analysis within [101], which informs the MASS decision-making and autonomy layer, and [102], which showed us the creation of Layer 4 - inputs for decision-making making which is described as Decision-making process of ship autonomous collision avoidance the process of decision-making for collision avoidance into a discrete layer within our decomposition model.

Layer 0 - Autonomous Vessel

The Autonomous Vessel forms the base level of our structural decomposition, representing the entire vessel as a holistic and autonomous entity. This layer acts as an overarching boundary for the whole system, symbolizing the vessel as a singular unit operating with full autonomy. All subsequent layers and their respective components fit and function within this scope. The autonomous ship, as conceptualized in this model, is a synthesis of advanced technologies that enable maritime operations to be conducted autonomously without direct human oversight. The identification of this layer underlines the transformational shift from traditional crewed operations towards a future in which the ship itself emerges as the central actor, autonomously navigating the complexities of the maritime domain.

Layer 1 - Primary Functional Categories

It categorizes the autonomous ship into operational columns that are critical to its independent functioning. This categorization clearly describes the ship's systemic capabilities and responsibilities.

Navigation System: At the center of autonomous operations is the navigation system, the ship's cerebral tool for geographical orientation and course-plotting. This subsystem is supported by ECDIS, which integrates ENCs with real-time data to provide a comprehensive navigational picture. Complementing ECDIS, GNSS provides the point position accuracy required for precision navigation. Together with RADAR/ARPA systems for obstacle detection and AIS for maritime traffic awareness, the navigation system enables the vessel to plot and follow an optimized course through the seascape. The VDR acts as the ship's black box, recording vital navigational data for safety audits and incident analysis.

Communication System: Serving as the ship's communication link, this system bridges the gap between the ship and external entities such as other ships, harbor authorities, and satellite communications. The system, which includes devices such as RADAR/ARPA and VDR, is important for disseminating and receiving essential operational data. It is integrated with the Global Maritime Distress and Safety System (GMDSS) to ensure that the ship remains in constant communication readiness for safety and coordination, giving us a clear link with ECDIS.

Steering: This mechanical domain manages the ship's propulsion and direction of travel by translating the autonomous system's decisions into physical movement. It includes the engine control mechanisms, the rudder for steering, and the thrusters for maneuverability, all of which are important for the navigation and positioning of the ship in sea areas. In this thesis, the important components of ECDIS are the engine control, rudder, and thrusters of the autonomous ship.

Sensor and Data Analysis: A network of environmental and internal sensors act as the ship's sensory system, collecting data ranging from meteorological conditions to engine performance measurements. These sensors feed advanced data processing units, including AI algorithms and neural networks, which analyze and synthesize information to aid decision-making. This analysis underpins the ship's ability to interpret its environment autonomously, adapt to changing conditions, and make informed navigational choices.

Layer 2 - Sub-Systems and Control Mechanisms:

It describes the complex network of specialized subsystems within the autonomous ship, each designed to perform different but interdependent tasks. These subsystems are operations that translate the broader commands of Layer 1 into specific actions.

ECDIS Sub-System: The ECDIS Subsystem receives a wide variety of inputs to create a dynamic and detailed representation of the marine environment. According to our findings, all ECDIS sub-systems are analyzed as shown in the Figure 5. ENCs provide geographical data, while GPS receivers enhance this with accurate position data. Course and speed sensors provide information on the vessel's heading and speed, which is critical for course adjustments and optimization. AIS data provides real-time traffic information, enabling proactive navigational decisions in restricted sea lanes. Contributing to the all-round view of ECDIS are sensory inputs from LiDAR/LADAR, which maps the immediate environment with high accuracy, and infrared cameras that extend the ship's perception into the thermal spectrum, which is invaluable during night navigation or in foggy conditions. Weather transmitters keep the system informed of meteorological changes, allowing adjustments to be made for atmospheric conditions, while echo sounder data reveals underwater topography and potential hazards, ensuring safe passage.

Engine Monitoring and Control System: This system is important behind the autonomous ship's movement and is carefully regulated by sensor feedback and navigation decisions. It harmonizes the output from the navigation system to modulate propulsion power, ensuring that the ship sticks to the plotted course with optimum fuel efficiency and engine performance. The system continuously interfaces with navigation data to adjust the ship's power and steering mechanisms, facilitating responsive and calculated movements in the water.

Auxiliary Systems: Auxiliary systems provide critical support functions that ensure the continuous operation of the ship. Power generation subsystems fulfill the ship's electrical requirements and ensure that all systems have an uninterrupted power supply. Emergency systems, consisting of auxiliary power units and automatic distress signaling devices, increase the ship's resilience to unforeseen events and scenarios, ensuring safety and compliance with international maritime safety standards.

Human-Machine Interfaces: Despite the autonomous nature of the ship, human-machine interfaces are integral and serve as important links between the ship and human controllers. Shore-based control centers are remote hubs for operation, monitoring, and response and provide a layer of human oversight and expertise. Manual control stations on board provide the means for direct human control when required and ensure that critical decision-making capabilities are maintained in exceptional circumstances.

Environmental Monitoring: Consisting of a network of meteorological and oceanographic sensors, this subsystem collects environmental data that can affect navigational safety and operational efficiency. Meteorological sensors monitor atmospheric conditions such as wind, temperature, and humidity, while oceanographic instruments provide information on marine phenomena such as currents, wave height, and water saltiness. Together, these inputs enrich the ship's data ecosystem, enabling adaptive responses to the dynamic marine environment.

Layer 3 - Decision Making and Autonomy

It represents the intellectual center of the autonomous ship, where complex algorithms and computational logic come together to exploit the decision-making capacity of trained data and inputs. This layer is where autonomy moves from concept to implementation, enabling the ship to navigate with human-like understanding and accuracy.

Autonomous Decision-Making Algorithms: At the center of this layer are sophisticated algorithms that extract large data feeds to generate navigation decisions autonomously. This involves integrating and comprehensively analyzing real-time information from GNSS, ECDIS, RADAR, and various other sensors and transforming it into a rich texture of situational awareness. Key functions include route planning and optimization, where algorithms calculate the most efficient routes while respecting environmental constraints and designated restricted areas. Furthermore, these systems use sensor inputs and AIS data to adjust collision avoidance maneuvers and ensure safe passage dynamically.

Feedback Loops: Integral to the system's adaptability are feedback loops that allow the vessel to modify its behavior in response to sensory and operational feedback. Continuous monitoring of the vessel's condition and the marine environment triggers calibrated adjustments to course, speed, and other navigational parameters.

Vessel Traffic Service (VTS) Integration: The ship's communicative and cooperative interaction with VTS systems is essential for safe operations. This function ensures regular, automatic exchange of navigational data with shore-based traffic observers, compliance with maritime traffic regulations, and cooperative navigation within established maritime traffic frameworks. Automated responses to VTS directives and synchronized interactions with port operations facilitate efficient passage through controlled waterways and exacting enforcement of berthing and departure times.

ML and Adaptive Algorithms: Underlying this decision-making layer is the application of ML algorithms that serve as the evolving computational layer of autonomous navigation. These algorithms specialize in pattern recognition, identifying deviations from established operational baselines and flagging anomalies. Their continuous learning capacity allows for iterative optimization and fine-tuning of performance parameters based on cumulative experiences and emerging data patterns, thus improving the ship's navigational intelligence over time.

Human Modifiable Controls: Despite the high degree of autonomy, the system retains provisions for human oversight through interfaces and protocols that allow manual intervention. Remote control interfaces provide an additional layer of safety and decision-making by allowing human operators to assume control when necessary. Manual override protocols have been meticulously crafted to allow human commanders to intervene effectively during complex navigational scenarios or in the event of autonomous system failures. These controls ensure that while the vessel is capable of self-management, the invaluable insights and judgments of human expertise remain an integral component of maritime operations, thus combining the technological advances of autonomous navigation with the nuanced judgments of human experience.

Layer 4 - Inputs for Decision Making

It is transformed into an intelligence that utilizes the autonomous ship's cognitive abilities, contains the data necessary for informed decision-making, and at the same time, puts it into action.

Data Integration and Analysis: Acting as the cerebral brain of the ship, this component combines different data flows into a unified and coherent whole by carefully merging them.

This integration process synthesizes information from GNSS, ECDIS, RADAR, and a range of sensory inputs into a navigable form. By making sense of this combined data, the system provides the comprehensive situational awareness required for navigational efficiency and safety at sea.

Autonomous Navigation Decisions: The data becomes the driving force for autonomous navigation decisions regarding the ship's trajectory and speed. These decisions are made autonomously and are calculated through sophisticated algorithms that take into account both instantaneous and expected sea conditions. The system continuously plots and redraws routes, optimizing them for efficiency and compliance with maritime regulations and environmental management.

Collision Avoidance System: The collision avoidance system is the key to the ship's safety measures. This framework enables the ship to perform autonomous avoidance maneuvers using integrated data to detect potential collision risks in advance. The system is calibrated to take into account dynamic variables such as the position, speed, and heading of nearby vessels. This part of the system is a key element in our case studies that helps us discover critical COLREG failures.

After decomposing ECDIS and developing a comprehensive understanding of the layered decision-making architecture on an autonomous vessel, we have detailed the various components and their interconnections. This detailed understanding plays an important role in identifying potential vulnerabilities and the points within the system where cyberattacks can be most effective. Our informed perspective allows us to anticipate how threat actors can exploit these complex systems. Consequently, the logical progression of strengthening our cybersecurity posture is the identification of potential threat elements. This includes understanding who might target these systems and their capabilities.

5.2.2 Identify Threat Agents:

Identifying threat actors is an important step in the PASTA threat modeling process. Threat actors can range from individual hackers to organized crime syndicates, state-sponsored groups, and even insiders with access to the system. Each agent brings unique threats depending on their resources, technical skills, and motivations. Understanding the profiles of these agents and their potential attack vectors will be important in assessing the risks to the autonomous ship's ECDIS and related subsystems. In this phase, we will classify these agents, estimate their potential to exploit specific vulnerabilities for ECDIS and its components and assess the likely impact of such breaches on the operational integrity and safety of the ship.

In our case studies, we identified a number of potential threat elements that could target ECDIS and other critical systems of autonomous ships. This identification process is essential in applying the PASTA threat modeling methodology and allows us to adapt cybersecurity measures to various factors effectively. These threat elements, each with different motives and capabilities, are selected for different case studies.

Cyber Sea Pirates: This category of threat actor focuses on exploiting autonomous vessels for financial gain or to disrupt maritime operations. By targeting the vessel's navigational and operational systems, maritime pirates can create security risks and potentially lead to hijacking, cargo theft, and even environmental damage in search of ransom or booty.

Internal Personnel: Employees with system access present a unique security challenge, whether they act maliciously or accidentally. This can come from employees manipulated by external organizations or who need greater cybersecurity awareness.

Generic Hackers: These individuals or groups spread malware to extort ransom, characterized by a lower technological level. Their attacks could potentially disrupt the ECDIS by locking out essential functionalities or manipulating data.

Amateur and Ethical Hackers: With varied goals from self-improvement to system enhancement, these actors have moderate to high levels of skill. Ethical hackers, in particular, can help to improve ECDIS systems by finding and reporting vulnerabilities.

External Service Providers: These actors may seek to extract valuable data or compromise the ECDIS through the supply chain. The systems could be compromised through updates or maintenance activities performed by these providers.

Hacktivists and Criminal Hackers: Individuals or groups with an agenda to disrupt operations or steal for monetary gain. These actors might seek to disrupt the ECDIS as a form of protest or to commandeer the vessel for criminal purposes, such as theft or smuggling.

Competitors, Terrorists, and State Actors: These groups are typically highly skilled and have resources at their disposal that can enable sophisticated attacks against ECDIS systems. Their motives can range from industrial espionage to political, economic, or military advantage.

5.2.3 Catalog Threat Scenarios

In an effort to catalog potential threat scenarios for ECDIS and sub-components that affect ECDIS data within the framework of an autonomous ship, we have identified several key assets that are integral to its operation. These assets, essential to the navigation and safety of the ship, must be protected against cyberthreats. Focusing on ECDIS-related assets enables an intensive examination of vulnerabilities and the formulation of strong countermeasures.

ECDIS as a Key Component: ECDIS is the primary electronic charting tool that provides critical decision support for safe and efficient maritime navigation. It integrates various data streams to provide a real-time, comprehensive navigational picture that is important for the autonomous ship's continuous adaptation to the dynamic maritime environment. ECDIS is a high-value target for cyberthreats due to its central importance in ship navigation. Threat scenarios could include corruption of chart data or false input from its sub-components defined in Section 5.2.1, leading to incorrect navigational outputs or disruption of decision support capabilities that could seriously jeopardize navigational safety.

ECDIS Subsystem Assets: ENC data is the digital foundation on which ECDIS operates and is as valuable as the system itself. In addition, sensory inputs from LiDAR/LADAR, infrared cameras, and echo sounders collectively enrich the situational awareness of ECDIS. Threat scenarios may involve manipulating this sensory data, potentially creating false navigational environments, or increasing the risk of marine accidents by concealing real hazards.

Decision-Making and Autonomy Assets: At the center of autonomous navigation are the algorithms that drive navigational strategies and the feedback loops that facilitate the ship's responsive adaptability. cyberthreats targeting these algorithms can disrupt autonomous decision-making, potentially leading to unsafe navigation choices or an inability to react to emerging situations.

Inputs for Decision Making: Data integration and analysis provide a convergence point for multiple data streams and serve as the information infrastructure for autonomous decisions. Threats to this process can undermine the entire navigational decision-making framework, leading to incorrect course adjustments or inadequate speed changes. A collision avoidance system that relies on accurate data synthesis is particularly vulnerable; a compromised system may fail to detect collision risks, endangering the ship and its environment.

5.2.4 Identify Vulnerabilities

Following the cataloging of potential threat scenarios, the next stage in developing our cybersecurity threat modeling involves the identification of specific vulnerabilities and corresponding cyberthreats within focusing ECDIS and sub-systems. We have examined the vulnerabilities that represent weaknesses that could be exploited by the mentioned cyberthreats, potentially resulting in navigational errors or even collisions.

ECDIS Vulnerabilities

Hardware and Configuration Vulnerabilities

The foundational layers of ECDIS security are compromised by basic hardware and configuration oversights, such as open USB ports and poorly configured firewalls. These vulnerabilities create entry points for unauthorized access, allowing cyberattacks to bypass security measures through malware installation or exploit default settings, including default passwords [25]. This is a potential vulnerability for autonomous ships when systems are controlled and updated via the Remote Control Center (RCC) and could be a possible attack vector to manipulate the ships' systems and decision-making processes.

Software and System Integrity Challenges

Outdated software significantly compounds the risk, rendering ECDIS systems vulnerable to known exploits and reducing their resilience against cyberthreats. The tendency of ECDIS to run on obsolete systems exacerbates these vulnerabilities, leaving essential navigation and safety systems exposed to cyberattacks due to unsecured sensors and outdated protocols [93]. Knowing that an un-updated system runs through ECDIS, this could be a potential backdoor to manipulate the data or decision-making phase Layer 3, which is affecting Autonomous decision-making algorithms for potential collision.

Lack of Segmentation

Integration of ECDIS with various other shipboard systems without adequate network segmentation creates a significant vulnerability in the maritime navigation infrastructure. While it is important for operational effectiveness that ECDIS relies on data from other navigation systems such as GPS, RADAR, and AIS, it creates a converged network environment where the accidental compromise of one system can potentially compromise the entire network's security. This lack of segmentation means that peripheral or less secure systems vulnerabilities can serve as entry points for cyberthreats, allowing malicious entities to propagate attacks or gain unauthorized access to critical navigation systems.

Attack Types Targeting ECDIS Vulnerabilities

ECDIS vulnerabilities open pathways for various cyberattacks, from social engineering and phishing to malware installation and Denial of Service (DoS) attacks, aiming to disrupt ship operations and compromise safety. The spectrum of attack types extends to eavesdropping, spoofing, and unauthorized access, each capable of altering navigational data or outright disabling the ECDIS [25].

Social Engineering Attacks: Social engineering attacks manipulate human factors to trick individuals into disclosing confidential information or performing actions that compromise the ECDIS system [7]. Through deceptive emails, messages, or websites, attackers can gain unauthorized access to ECDIS systems, enabling them to manipulate navigational data or install malicious software. Such tactics often exploit crew members' trust and lack of cybersecurity awareness, underscoring the need for stringent cybersecurity training and protocols, especially in ports or RCC.

Malware Installation: The installation of malware on ECDIS systems presents a significant threat, allowing attackers to disrupt ship operations from a distance [7]. Malware can be designed to corrupt navigational data, disable the ECDIS, or gain remote control over the ship's navigational systems [103]. The entry points for malware include compromised software updates, which could lead to a potential compromise of whole network and supply chain attacks.

DoS Attacks: DoS attacks aim to overload the ECDIS system with excessive requests or traffic, rendering it unable to perform its navigational functions. This can lead to a temporary or permanent system disruption, potentially placing the ship and its crew in challenging situations. DoS attacks can originate from external networks or be triggered by malware within the ship's systems, emphasizing the need for effective network security and traffic monitoring solutions.

Eavesdropping: Eavesdropping involves the unauthorized interception of data being transmitted to or from the ECDIS system [103]. This can enable attackers to gain insight into sensitive navigational information, ship movements, and operational plans. By exploiting vulnerabilities in the communication infrastructure, eavesdroppers can collect data that may be used for further attacks or sold to interested parties, necessitating the use of encrypted communication channels and secure data protocols.

Unauthorized Access: Unauthorized access to ECDIS systems can occur through various means, including exploiting weak passwords, unpatched software vulnerabilities, or insecure network connections. Once inside the system, attackers can alter navigational data, delete critical information, or introduce false information, jeopardizing the safety of the vessel. Implementing strong authentication methods, regular software updates, and network segmentation are important in preventing unauthorized access [25].

ECDIS Sub-system Vulnerabilities

Each sub-component of ECDIS, including the sensors and network connections that feed navigational data into the system, may be vulnerable to specific cyberthreats. For example, communication channels between GNSS and ECDIS can be compromised or disrupted, sensor spoofing can feed false data into the system, and any weak link in data encryption can be exploited to gain unauthorized data access.

AIS Vulnerabilities

Communication Protocol Vulnerabilities: AIS's reliance on specific communication protocols without adequate security measures leaves it susceptible to various cyberattacks, emphasizing the need for protocol enhancement and security hardening [25].

Absence of Encryption and Authentication: As shown in the research by [25] and [93], the lack of encryption and integrity checks within AIS systems exposes them to data manipulation risks, where critical navigational and identification information can be altered undetected.

Integration with Navigation: The ability of AIS to integrate with systems such as GNSS and ECDIS increases its vulnerability to attacks such as spoofing and jamming, directly affecting the reliability of navigational outputs and potentially leading to navigational errors[7].

Default Passwords and Unauthorized Access: The use of default passwords can lead to unauthorized access, allowing attackers to perform adverse actions such as altering navigational information, which endangers both the vessel and its operations([7][25]).

DoS Attacks and Data Manipulation: A significant proportion of AIS systems are vulnerable to DoS attacks, which can disrupt their functionality, and logical vulnerabilities that allow the injection of invalid data, undermining the system's reliability [104].

Attack Types Targeting AIS Vulnerabilities

Eavesdropping and Jamming: These attacks exploit the open nature of AIS communications, allowing attackers to intercept or block the transmission of critical data, thus compromising navigational safety and data integrity [25].

Spoofing and AIS Data Manipulation: Spoofing attacks involve broadcasting false AIS signals to misrepresent a vessel's position or identity, potentially leading to navigational confusion or collisions [3].

DoS: By targeting the AIS protocol or leveraging logical vulnerabilities, attackers can render AIS systems inoperative, directly affecting the ship's ability to navigate safely and communicate effectively [104].

Ghost Ships and False Information: Creating fictitious vessel signals ('ghost ships') or broadcasting false navigational warnings exploits AIS's security gaps, leading to real-world dangers for maritime traffic [105].

GMDSS Vulnerabilities

Data Integrity Concerns: The manipulation of GMDSS data, particularly weather conditions and ship positioning, brings significant risks. Such alterations can lead to hazardous situations, misleading vessels into navigating dangerous paths or underestimating weather-related risks [7].

Confidentiality Breaches: Unauthorized access to GMDSS systems can lead to a breach of confidentiality, undermining the safety and operational protocols of the vessel. The dissemination of sensitive information can severely harm ship operations and compromise safety measures [7].

Attack Types Targeting GMDSS Vulnerabilities

The vulnerabilities built into the GMDSS framework open up several ways for cyberattacks, each with the potential to significantly disrupt maritime security and communications.

False Data Transmission and Identity Spoofing: Attackers can transmit false data or spoof the vessel's identity, compromising the cargo's security and the safety of individuals onboard. Such attacks undermine the integrity of GMDSS communications and can lead to misinformed decisions [7].

Unauthorized Access and Emergency Protocol Tampering: Gaining unauthorized access with elevated privileges can result in deactivating emergency protocols or their inappropriate activation [7].

Signal Jamming and Spoofing: GPS signal jamming, and spoofing are sophisticated attacks that prevent the receiver from acquiring accurate positioning signals, leading to potential navigation errors. By convincing the positioning systems to accept counterfeit signals, attackers can cause unintentional course corrections, further endangering maritime navigation[3].

RF Signal Disruption: Given GMDSS's reliance on radio frequencies (RF) for distress signals and safety communication, it is particularly vulnerable to RF jamming or spoofing attacks. Such disruptions can incapacitate the system's ability to communicate distress signals or safety messages effectively [28].

Authentication and Encryption Deficiencies: The risk associated with transmitting verified distress signals underscores the importance of signal verification by external entities such as the RCC. Additionally, encrypting signals is important to safeguard against unauthorized access and ensure the confidentiality and integrity of transmitted data [105].

Decision Making and Autonomy Vulnerabilities

Autonomous systems are vulnerable to various adversarial attacks, as noted in Section 5.2.4. Such vulnerabilities can occur in various subsystems, including ECDIS, its sub-components, and the wider situational awareness modules summarised in Section 5.2.1. The main areas of vulnerability can be as follows:

Training Data: The foundation of ML models, where the integrity and security of the data determine the reliability of autonomous decision-making processes.

ECDIS: Central to maritime vessels' navigation and operational functionality, vulnerabilities here can directly impact navigational accuracy and safety given in Section 5.2.4.

ECDIS Sub-systems: Specific attacks targeting navigation and communication subsystems undermine the vessel's operational integrity, which sends its data to ECDIS as shown in Section 5.2.4.

Layer 3 - Decision Making and Autonomy: As defined in Section 5.2.1, it encompasses the core algorithms responsible for making autonomous decisions, where vulnerabilities could lead to compromised operational decisions.

Target Model: Refers to the specific ML models employed by the system, where vulnerabilities might allow for exploitation through adversarial attacks.

Backdoor: Covert vulnerabilities intentionally embedded within the system can be exploited to gain unauthorized access or manipulate system behavior.

Software Dependency for Training Model: The reliance on external or third-party software components may introduce vulnerabilities due to security weaknesses.

Adversarial Attacks on Autonomous Ships Targeting Decision Making

Attackers can launch targeted attacks against this reliance by attempting to exploit vulnerabilities such as insecure wireless communication channels, inadequately protected data storage, or non-encrypted data transmission. These attacks can lead to a series of failures in autonomous decision-making systems.

The reliance on advanced ML and AI systems for decision-making, object detection, and situational awareness, as given in Section 2.1.1 introduces a novel category of cybersecurity threats: adversarial attacks. These attacks are designed to exploit the vulnerabilities of AI/ML algorithms, potentially leading to catastrophic outcomes in terms of navigational safety and operational security. Such manipulations, often imperceptible to humans, can deceive AI systems into making erroneous decisions, misidentifying objects, or failing to recognize obstacles, thereby compromising navigational safety and operational security.

Exploring Adversarial Attack Types

Adversarial attacks on autonomous ships can take various sophisticated forms, each aimed at undermining the reliability and integrity of AI-driven systems. Studies such as those by [24], [23], and [106] have shown how different types of adversarial attack methods, including Fast Gradient Sign Method (FGSM), Iterative FGSM, Momentum Iterative FGSM, and Predictive Gradient Descent, can significantly degrade the performance of these AI models. These methods exploit the model's dependence on the input data to reveal perturbations that lead to misclassification or non-detection of objects, targeting our scope, which is important for mitigating non-compliance with COLREG.

Perturbation Attack: By crafting specific queries, attackers can deceive ML algorithms into making erroneous decisions, disrupting the vessel's situational awareness and decision-making processes.

Model Inversion and Membership Inference: These techniques aim to extract sensitive information about the ML model's features or training data, raising significant privacy and intellectual property concerns.

Model Stealing: Through strategic querying, attackers can deduce a model's parameters and architecture, enabling them to replicate or steal the model, thus compromising intellectual property.

Physical Domain Examples: Modifying physical inputs or spoofing sensor data can cause an ML-based vessel navigation system to misinterpret its environment, leading to potentially hazardous navigational errors.

Supply Chain and ML Lifecycle Attacks: Interfering with the ML lifecycle, including data manipulation or exploiting software vulnerabilities, can lead to compromised model integrity and functionality.

Backdoor Attacks and Software Dependency Exploits: Inserting backdoors in models or targeting software dependencies introduces risks of unauthorized access and manipulation of ML systems, altering their outputs to achieve malicious objectives.

Reprogramming and Poisoning: Altering the operational parameters of an ML system or corrupting its training data undermines the system's accuracy and reliability, posing severe risks to navigational safety and decision-making accuracy.

Evasion through Deep Learning Model Manipulation: Specific focus on adversarial attacks against You Only Look Once (YOLO) version 5 or 3, which are real-time object detection models used in autonomous ships in the research done by [24] and [106], other deep learning models illustrates the potential for manipulated input data to cause misclassification or inaccurate object detection, directly threatening the safety and operational integrity of autonomous ships.

Clean-Label Poisoning Attack: This subtle attack corrupts AI models' training data without altering the labels, leading to incorrect classifications. Such manipulation can prevent the accurate detection of threats, exemplifying a grave security risk to autonomous maritime operations.

Incorrect Inputs to Decision Making

Incorrect or manipulated inputs fed into the autonomous vessel's decision-making algorithms can lead to erroneous navigational decisions. This can be caused by hijacked sensors, AIS spoofing, or manipulated inputs from collision avoidance systems. The integrity of data integration and analysis processes is key to preventing the exploitation of such vulnerabilities, which could otherwise lead to navigation errors or delayed responses to real-time sea conditions.

Vulnerabilities from Compromised Systems

Compromised Navigation Systems: Data manipulation within critical navigation systems such as ECDIS, GNSS, and AIS can directly lead to incorrect navigational decisions [93]. Such manipulated data can result from cyberattacks targeting the signal processing and transmission capabilities of these systems, causing navigational errors[7].

AI-Driven Decision-Making Compromise: AI and ML systems underpin autonomous ship operations and are particularly vulnerable to being fed incorrect inputs. This could lead to miscalculations in navigational paths and decision-making processes, ultimately endangering the ship [28].

Sensor Deception: Attacks aimed at deceiving or degrading sensors, such as radar, LiDAR, or GNSS systems, directly impact navigation by providing incorrect data for decision-making processes. These deceptions can significantly derail an autonomous ship's course and safety protocols[28].

Path Planning and Trajectory Optimization: Manipulated inputs can adversely affect the autonomous ship's path planning and trajectory optimization processes, leading to unsafe routing and potential collisions. Incorrect or tampered ENC data undermines the safety and efficiency of vessel operations, posing significant risks to autonomous ship operations [107].

Weather Routing and Ship Handling: Cyberattacks targeting weather information systems can provide incorrect weather data to autonomous ships, leading to sub-optimal routing decisions and endangering the vessel during adverse weather conditions[108].

Attack Types Leading to Incorrect Inputs

Spoofing and Jamming: Techniques such as spoofing and jamming are used to manipulate the sensory input of autonomous ships, misleading navigation systems about the ship's true position or the presence of other objects in its surrounding environment[25].

Adversarial Data Manipulation: Specially crafted adversarial attacks manipulate the input data to AI and ML systems, causing these systems to make incorrect predictions or judgments. Such manipulations can severely compromise navigational decisions and the overall safety of maritime operations [25].

Coordinated and Overwhelming Alerts: Novel attack concepts, such as coordinated attacks, can cause navigation systems like AIS to display incorrect or conflicting information. Similarly, overwhelming alert attacks can saturate the decision-making systems with false alarms, leading to potential misinterpretations and operational collisions [104].

5.2.5 Impact on COLREG Compliance

Following the systematic categorization of identified cybersecurity threats and vulnerabilities affecting autonomous maritime systems, we mapped the COLREG rules to these categorized cyberthreats. This aims to prevent maritime accidents involving potential autonomous vessels by addressing the complexities and potential uncertainties in the COLREG regulations.

Following the systematic categorization of identified cybersecurity threats and vulnerabilities affecting autonomous maritime systems, we constructed a detailed scheme mapping the COLREG rules to these categorized cyberthreats. This table serves as a foundation for understanding how specific cyberthreats correlate with potential breaches in COLREG compliance, aiming to prevent maritime accidents involving autonomous vessels by addressing the complexities and potential uncertainties in the COLREG regulations. The comprehensive mapping is presented in Figure 6, which provides a structured overview of the intersecting points between cybersecurity and navigational safety.

Rule 2 - Responsibility: Autonomous ships, guided by algorithms and reliant on potentially manipulated data, blur traditional lines of responsibility. Ensuring these vessels adhere to COLREG despite incorrect inputs demands strong algorithmic accountability measures, possibly requiring new legal frameworks to define responsibility when decisions are delegated to AI.

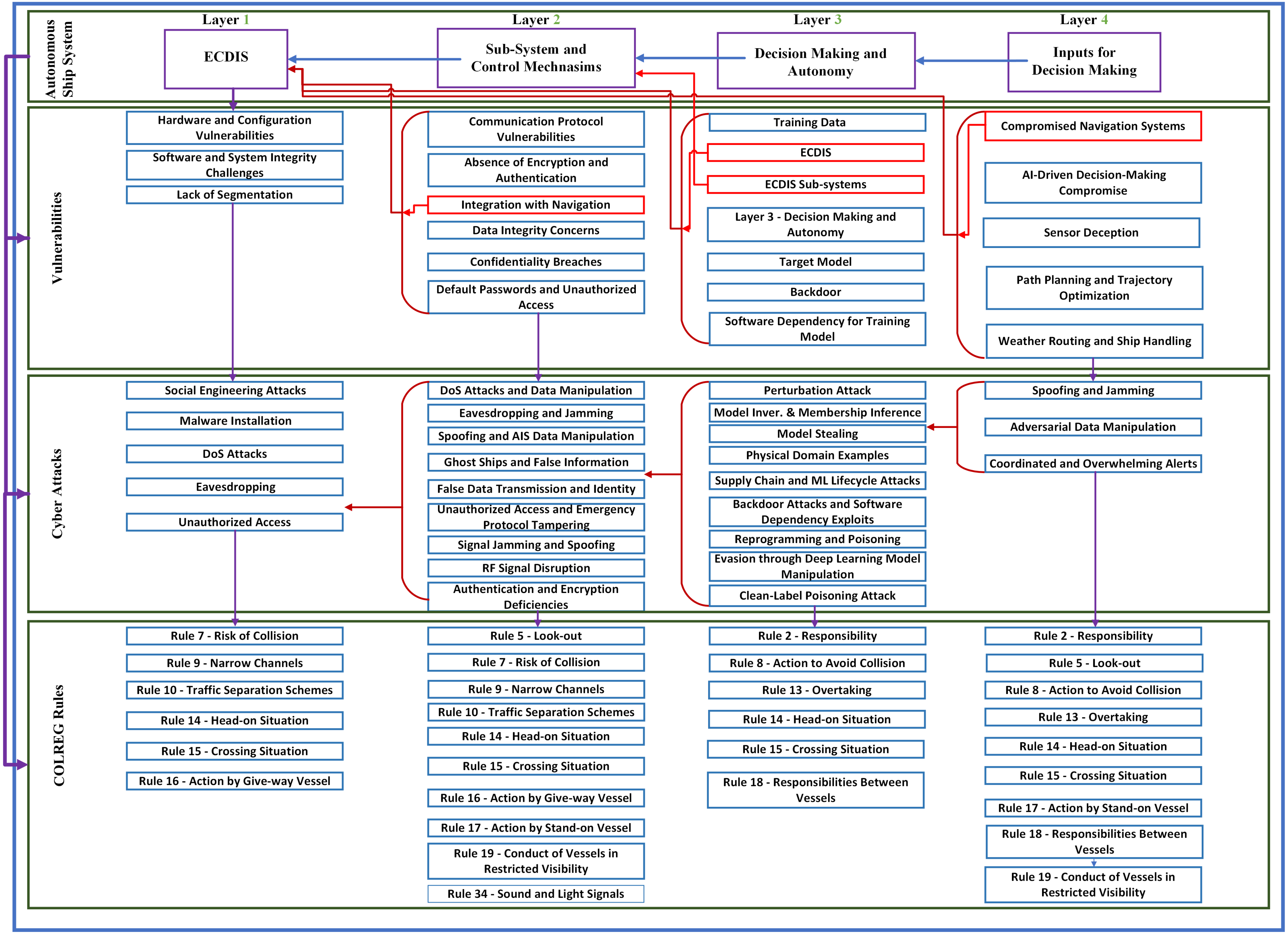
Autonomous Ship System
Layer 1
ECDIS
Layer 2
Sub-System and Control Mechnasims
Layer 3
Decision Making and Autonomy
Layer 4
Inputs for Decision Making
Vulnerabilities
Hardware and Configuration Vulnerabilities
Software and System Integrity Challenges
Lack of Segmentation
Communication Protocol Vulnerabilities
Absence of Encryption and Authentication
Integration with Navigation
Data Integrity Concerns
Confidentiality Breaches
Default Passwords and Unauthorized Access
Training Data
ECDIS
ECDIS Sub-systems
Layer 3 - Decision Making and Autonomy
Target Model
Backdoor
Software Dependency for Training Model
Compromised Navigation Systems
AI-Driven Decision-Making Compromise
Sensor Deception
Path Planning and Trajectory Optimization
Weather Routing and Ship Handling
Cyber Attacks
Social Engineering Attacks
Malware Installation
DoS Attacks
Eavesdropping
Unauthorized Access
DoS Attacks and Data Manipulation
Eavesdropping and Jamming
Spoofing and AIS Data Manipulation
Ghost Ships and False Information
False Data Transmission and Identity
Unauthorized Access and Emergency Protocol Tampering
Signal Jamming and Spoofing
RF Signal Disruption
Authentication and Encryption Deficiencies
Perturbation Attack
Model Inver. & Membership Inference
Model Stealing
Physical Domain Examples
Supply Chain and ML Lifecycle Attacks
Backdoor Attacks and Software Dependency Exploits
Reprogramming and Poisoning
Evasion through Deep Learning Model Manipulation
Clean-Label Poisoning Attack
Spoofing and Jamming
Adversarial Data Manipulation
Coordinated and Overwhelming Alerts
COLREG Rules
Rule 7 - Risk of Collision
Rule 9 - Narrow Channels
Rule 10 - Traffic Separation Schemes
Rule 14 - Head-on Situation
Rule 15 - Crossing Situation
Rule 16 - Action by Give-way Vessel
Rule 5 - Look-out
Rule 7 - Risk of Collision
Rule 9 - Narrow Channels
Rule 10 - Traffic Separation Schemes
Rule 14 - Head-on Situation
Rule 15 - Crossing Situation
Rule 16 - Action by Give-way Vessel
Rule 17 - Action by Stand-on Vessel
Rule 19 - Conduct of Vessels in Restricted Visibility
Rule 34 - Sound and Light Signals
Rule 2 - Responsibility
Rule 8 - Action to Avoid Collision
Rule 13 - Overtaking
Rule 14 - Head-on Situation
Rule 15 - Crossing Situation
Rule 18 - Responsibilities Between Vessels
Rule 2 - Responsibility
Rule 5 - Look-out
Rule 8 - Action to Avoid Collision
Rule 13 - Overtaking
Rule 14 - Head-on Situation
Rule 15 - Crossing Situation
Rule 17 - Action by Stand-on Vessel
Rule 18 - Responsibilities Between Vessels
Rule 19 - Conduct of Vessels in Restricted Visibility

Figure 6. Multi-Layered Threat Analysis Model for ECDIS in the Context of COLREG Compliance.

Cyberthreats such as manipulation of decision-making algorithms or interference with human override controls compromise a vessel's ability to adhere to the responsibility principle. Malicious tampering could render autonomous decisions unsafe or prevent necessary human intervention, directly impacting the vessel's responsibility as stipulated by Rule 2.

Rule 5 - Look-out: Spoofing or disabling of sensory equipment like Radar, LiDAR, or cameras can fail to detect nearby vessels or obstacles. This directly contravenes Rule 5, which mandates a proper look-out by sight and hearing and all available means to assess any risk of collision.

Rule 7 - Risk of Collision: Autonomous systems must assess the risk of collision based on the data received from sensors and ECDIS. Erroneous data can lead to incorrect assessments. Amendments might be necessary to outline the standards for data accuracy, integrity, and the decision-making logic used by autonomous ships to assess collision risks.

AIS spoofing or data manipulation brings significant risks by affecting the tools within the ECDIS used for assessing collision risks. Erroneous AIS data could lead to miscalculated assessments, causing overreaction or underestimation of collision risks, thereby violating Rule 7.

Rule 8 - Action to Avoid Collision: This rule requires actions to avoid collisions to be taken by the rules and to be positive, made in ample time, and with due regard. For autonomous ships, the challenge lies in programming nuanced decision-making that can adapt to incorrect data. The rule may need to include system checks and balances provisions that ensure actions are based on verified data.

Disruption or manipulation of decision-making processes through adversarial inputs or malware impacts an autonomous ship's capability to take appropriate, timely, and sufficient action to avoid collisions, challenging compliance with Rule 8.

Rule 9 - Narrow Channels: Directs that a vessel proceeding along the course of a narrow channel or fairway shall stay near the outer limit of the channel or fairway, which lies on her starboard side, as safe and practicable. The challenge for autonomous ships is accurately interpreting channel boundaries with incorrect ECDIS data.

GPS spoofing affecting the ship's understanding of its position can cause deviation from the correct side of a narrow channel. Misleading positional data could lead to violations of Rule 9, which mandates vessels to keep to the starboard side in narrow channels.

Rule 10 - Traffic Separation Schemes: Autonomous vessels must navigate Traffic Separation Schemes accurately, which depends on the integrity of the navigational data and the vessel's ability to interpret and act on this data correctly. Revisions might focus on the requirements for autonomous ships to verify navigational data's accuracy and respond appropriately to detected discrepancies.

Manipulation of ECDIS systems to display incorrect traffic separation scheme information could result in an autonomous vessel incorrectly navigating through these schemes, failing to comply with Rule 10.

Rule 13 - Overtaking: Defines the responsibilities between vessels when one is overtaking another. Autonomous ships must have algorithms capable of identifying when they are overtaking another vessel and executing the maneuver safely by the COLREG. Sensor spoofing can impair an autonomous vessel's perception system, preventing the accurate identification of vessels from being overtaken. This undermines the safe execution of overtaking maneuvers, contravening Rule 13.

Rule 14 - Head-on Situation: Applies when two power-driven vessels are meeting on reciprocal or nearly reciprocal courses, requiring them to alter course to starboard so that each passes on the port side of the other. For an autonomous ship, interference with communication systems may lead to failure to transmit or receive maneuver intentions in head-on situations. This compromises the ability to take appropriate action as per Rule 14, potentially leading to unsafe encounters.

Rule 15 - Crossing Situation: When two power-driven vessels are crossing to involve collision risk, the ship with the other on her starboard side must keep out of the way. Adversarial attacks on AI algorithms could misinterpret which vessel has the right of way in crossing situations. Incorrect navigational actions taken due to these manipulations challenge the adherence to Rule 15.

Rule 16 - Action by Give-way Vessel: Specifies the requirements for the vessel that has been designated to give way in a situation involving the risk of collision. Cyberattacks affecting a vessel's ability to recognize itself as the give-way vessel or to execute correct maneuvers may lead to non-compliance with Rule 16, heightening the risk of collision. An autonomous ship, relying on incorrect data from ECDIS, may not accurately identify itself as the give-way vessel or may execute inappropriate maneuvers based on flawed situational awareness. This rule might need to be adapted to include mechanisms for verifying the data accuracy used in the decision-making process.

Rule 17 - Action by Stand-on Vessel: Dictates the responsibilities of the vessel that has the right to maintain its course and speed, known as the "stand-on" vessel, in situations that could lead to a collision. An autonomous ship, misled by incorrect ECDIS data, might not recognize when it is the stand-on vessel or might erroneously alter its course or speed when it should maintain it. To address the unique challenges posed by autonomous navigation, this rule could be revised to include guidelines for autonomous ships to confirm their stand-on status using redundant systems or data sources and procedures for maintaining course and speed with high reliability, even when faced with uncertain or conflicting data.

Targeted attacks that force a stand-on vessel to alter course or speed inappropriately, in direct violation of Rule 17, highlight the importance of securing navigational decision systems against cyberthreats.

Rule 18 - Responsibilities Between Vessels: This rule outlines the hierarchy of right-of-way among different types of vessels. There's a need to clarify how these vessels identify and interact with various vessel types, especially under data misinterpretation or decision-making errors. Specific guidelines for autonomous ships could be introduced, such as mandatory identification signals or behaviors that indicate their autonomous nature. Clarifying how autonomous ships identify and interact with various vessel types, underpinned by accurate data, is important. Attacks that alter vessel type or status information can mislead regarding the right-of-way hierarchy, creating unsafe situations and complicating compliance with Rule 18.

For example, a power-driven vessel is responsible for giving way and changing course to avoid collision with a fishing vessel. If the autonomous vessel's decision-making mechanism is compromised by adversarial attacks in the maritime environment in such a way that it cannot recognize the fishing vessel, this could lead to potential conflicts.

Rule 19 - Conduct of Vessels in Restricted Visibility: Autonomous ships must make decisions in restricted visibility based on sensor inputs. Erroneous sensor data can lead to inappropriate actions. Amendments may be required to address the reliability and verification of sensor data in conditions of restricted visibility.

Manipulating visibility data through the spoofing or disabling of meteorological sensors could result in inadequate responses to reduced visibility conditions. Such actions undermine Rule 19, emphasizing the need for accurate environmental sensing and data integrity in autonomous navigation.

Rule 34 - Sound and Light Signals: A cyberattack targeting systems responsible for interpreting and responding to sound and light signals on an autonomous vessel could exploit sensory processing or communication systems vulnerabilities. For example, a malware attack could compromise software that analyses and decodes acoustic signals such as horns or whistles and light signals such as navigation lights and signal lights. This malware could alter the vessel's interpretation algorithms, causing the vessel to misinterpret the intentions of nearby vessels or respond inappropriately. While these sound signals are important to minimize the inconvenience of difficult conditions at sea, such as foggy conditions, a breach of such conditions could result in a major accident.

For example, suppose an autonomous vessel is approached head-on by another vessel in a situation where both vessels are required to alter course to starboard as indicated by specific sound or light signals. In that case, the intercepted system may not be able to detect these signals correctly. Instead of maneuvering to the right, the autonomous vessel may maintain its course or take a dangerous action, leading to a high risk of collision. This scenario underlines the critical importance of securing the signal processing systems of autonomous ships against cyberthreats to ensure compliance with Rule 34 of COLREG.

5.2.6 Model Attack Paths

As shown in the Figure 6, we have identified the corresponding systems with vulnerabilities and their cyberthreats. The 6th step for the PASTA threat modeling is to create the attack paths for the identified COLREG rules to show a more in-depth examination of each cyberthreat that could affect the ship's navigation and lead to a potential collision. Therefore, we have used our categorization to create the attack paths and their relationship.

ECDIS

We have developed an attack path diagram for ECDIS on autonomous ships to represent the possible violations of the COLREG in case cyberthreats manipulate the system data. The model in Figure 7 shows the potential exploitation of ECDIS by threat actors through cyberattacks. These potential cyberattacks compromised the ECDIS. The Ship Control Center then transmits the compromised ECDIS data to the ship's data processing module, namely the Situational Awareness module. This, in turn, passes the correct or corrupted data to the Collision Avoidance module. Based on the integrity of the received data, the module, which must be trained to comply with COLREG, adjusts the ship's course or changes its speed in response to the movements of nearby vessels approaching or passing. Only accurate data from the ECDIS can clarify the decision-making mechanism, potentially resulting in a collision. This scenario brings a significant international regulatory challenge beyond the immediate economic, environmental, and humanitarian losses, as it could also

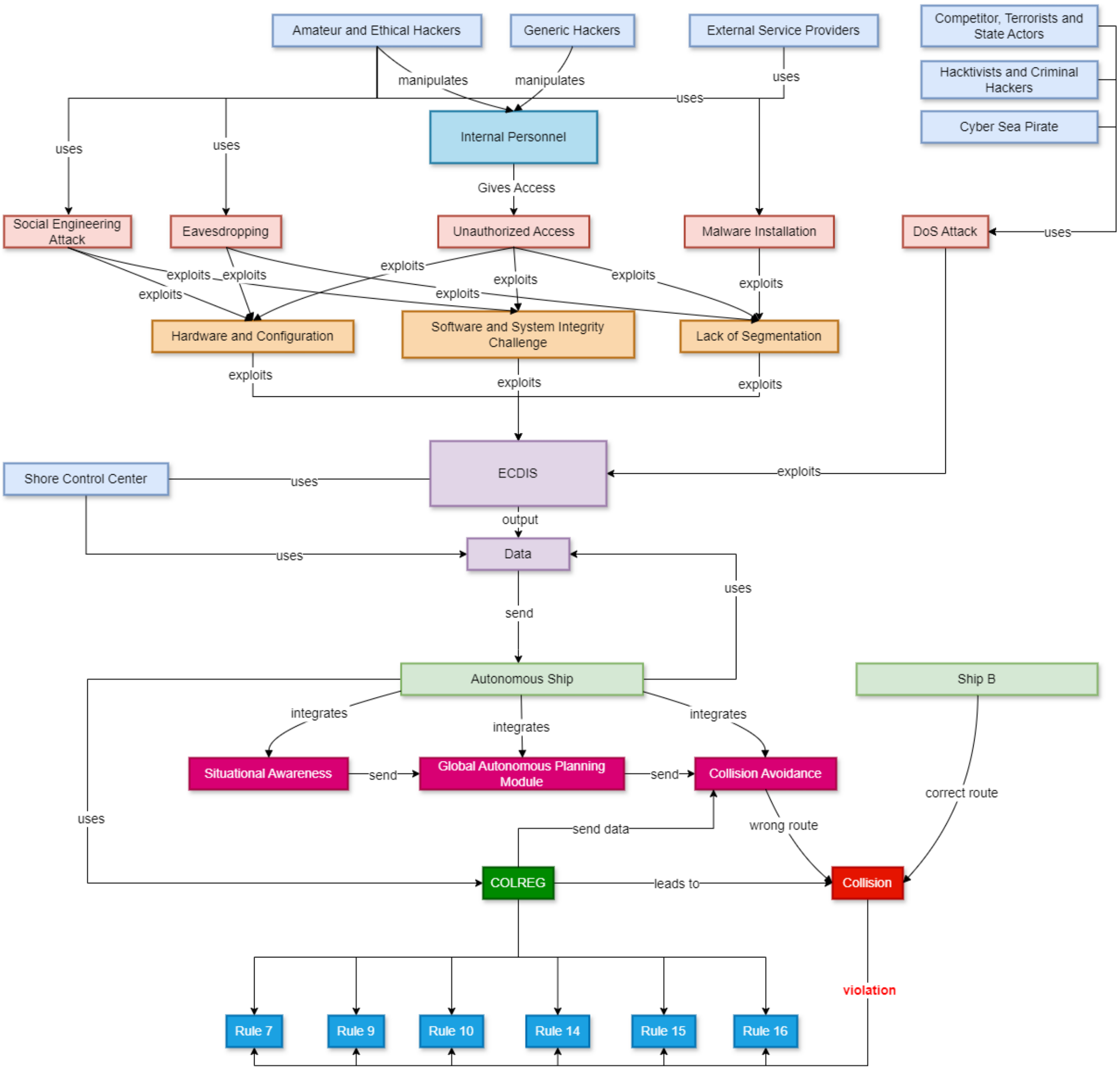

Figure 7. Attack Path Diagram for the ECDIS.

lead to COLREG violations.

Rule 14 requires an autonomous vessel to navigate so that an oncoming vessel stays on the starboard side in a head-on situation. However, suppose ECDIS data has been tampered with. In that case, the vessel's position may be falsely shown as starboard or astern in a Heads-On Zone as shown in Figure 8, misleading the decision-making algorithm.

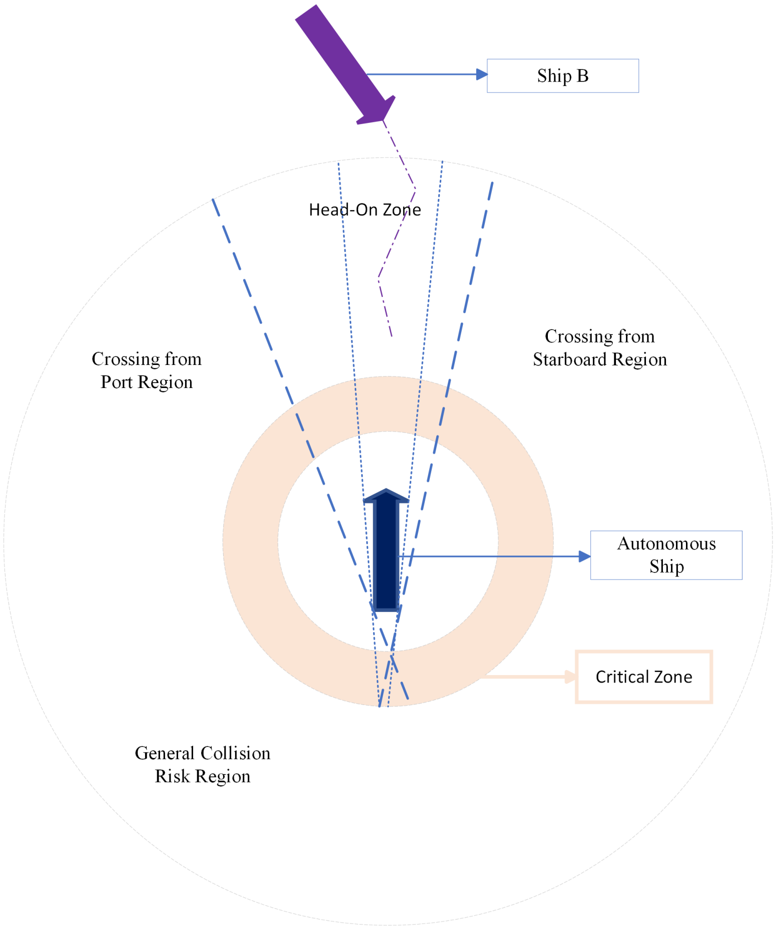
Ship B
Head-On Zone
Crossing from Port Region
Crossing from Starboard Region
Autonomous Ship
Critical Zone
General Collision Risk Region

Figure 8. Visualisation of the Head-on Situation and Corresponding Zone.

Such misinformation is a primary potential collision and represents a clear violation of the COLREG rules under international regulations.

ECDIS Sub-systems

In our research, we have developed a comprehensive flowchart illustrating the multitude of cyberthreats that threaten ECDIS subsystems, focusing on the autonomous ship system and its modules, as shown in Figure 9. This flowchart categorizes potential vulnerabilities, identifies their attack methodologies, and traces the impact of these attacks on sub-systems. At the top are threat actors ranging from individual hackers to state-sponsored organizations, each with different capabilities and motives. The flowchart maps how these actors exploit vulnerabilities such as unauthorized access and protocol weaknesses in maritime systems to compromise critical navigation data from AIS, GPS, and other sensors.

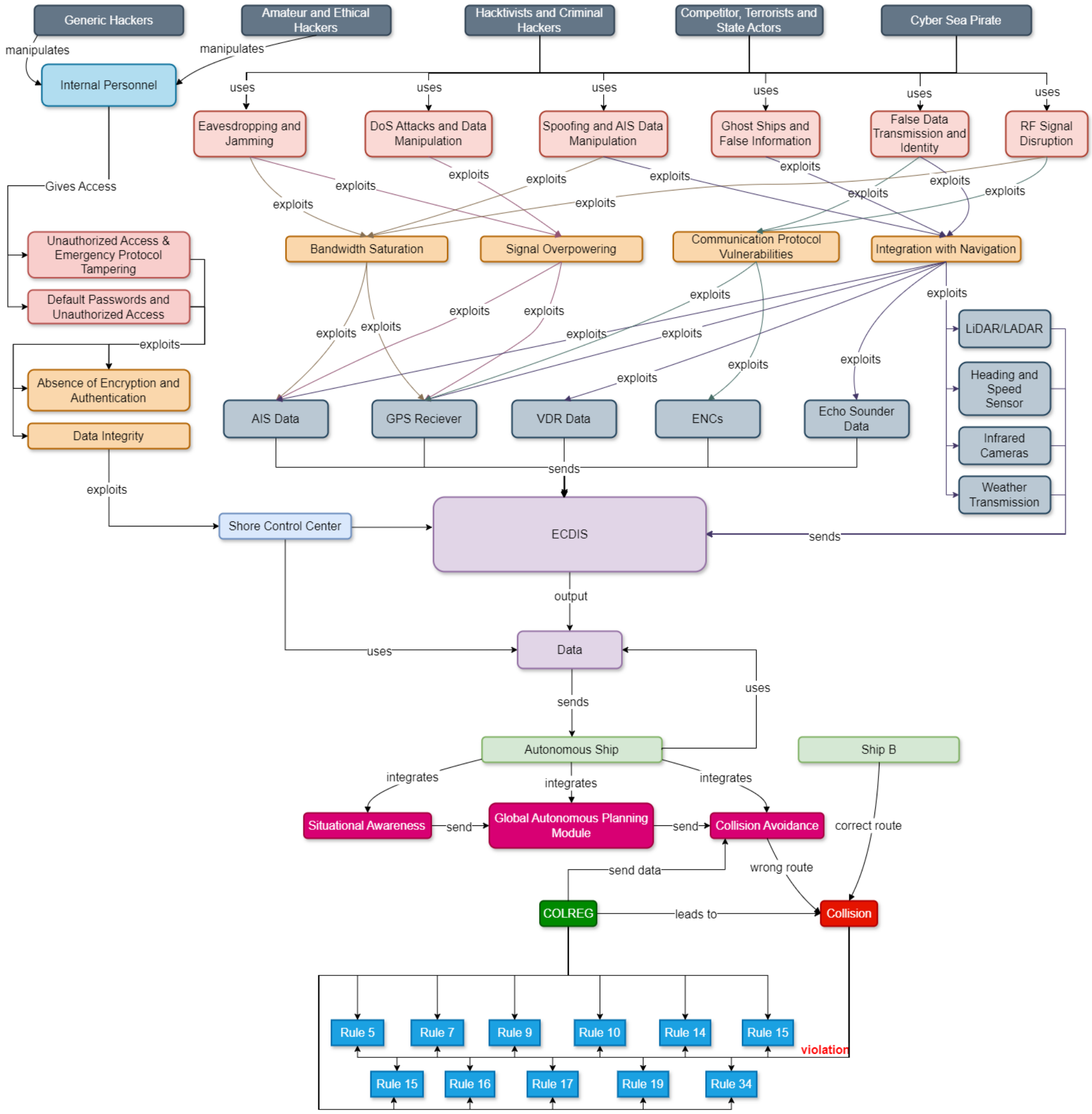

Figure 9. Attack Path Diagram for the ECDIS Sub-Systems.

This corrupted data flows into the ECDIS, an integral part of autonomous ship navigation. The downstream effects of these cyberattacks are highlighted in the flowchart as disruptions to the ship's collision avoidance systems, potentially leading to navigation errors and violations of the COLREG.

Adversarial Attacks

Autonomous ships incorporating modules like situational awareness and global autonomous planning are fundamental in reducing the risk of maritime accidents. However, these technological advancements also open up new avenues for adversarial attacks, which can compromise the safety and integrity of maritime navigation.

Firstly, ECDIS, being central to autonomous navigation, is a prime target for adversarial exploitation. Attackers may employ backdoor attacks or software dependency exploits to manipulate navigational data, resulting in erroneous situational awareness. These attacks could lead to a ship's inability to correctly identify and respond to navigational hazards, potentially causing violations of COLREG rules and resulting in collisions.

The situational awareness module integrates data from various sensors and creates a cohesive picture of the surrounding marine environment. By exploiting this module, adversaries could feed false information, leading to misclassification of objects or incorrect global planning decisions. This can lead to inappropriate collision avoidance maneuvers or, in a worst-case scenario, result in a collision.

The Figure 10 shows that threat actors may utilize different attack vectors to exploit situational awareness and ECDIS systems. For example, model stealing or adversarial examples could be used to deceive the AI models that aid decision-making aboard an autonomous ship. Additionally, exploiting the decision-making and autonomy layer through attacks like Evasion through Deep Learning Model Manipulation can lead to misinformed or hazardous navigational decisions.

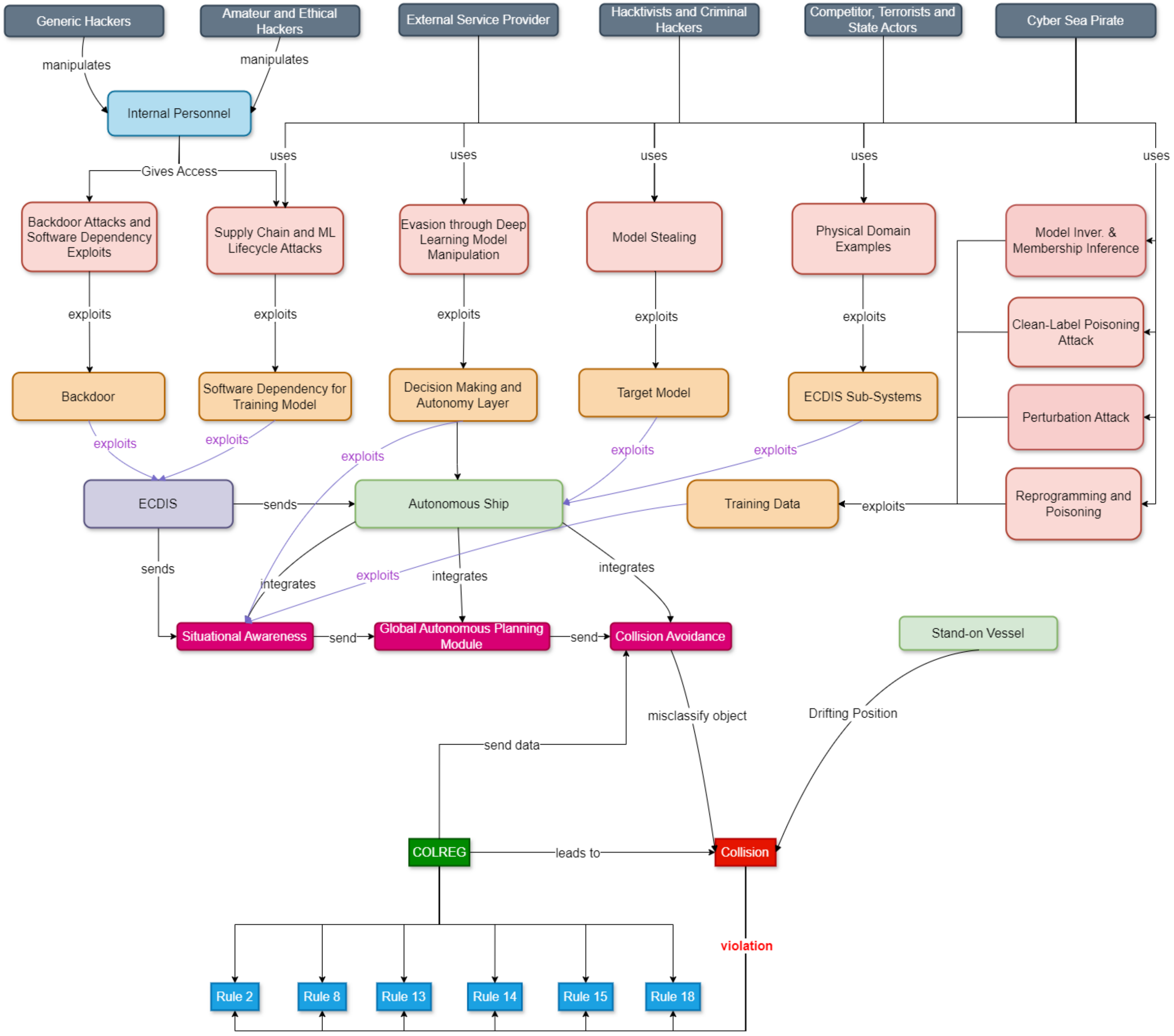

Figure 10. Adversarial Attack Path Diagram.

Compliance with COLREGs is very important in autonomous navigation to prevent maritime accidents. The integrity of ECDIS and situational awareness modules is important for this compliance. Hostile attacks leading to disruption of these systems can lead to violations of certain COLREG rules, such as Rule 18, which is designed to prevent collisions at sea, and inappropriate behavior of ships when bearing each other.

The autonomous onboard object detection system uses a ML model trained like YOLOv3 as defined in Section 5.2.4 to classify marine vessels based on Autonomous System (see Figure 5). An adversarial attack targets this system by subtly altering the input data, causing the model to misclassify any vessel in the environment. In a special case where an autonomous vessel detects a fishing vessel on its course, the navigation system incorrectly assumes it has the right of way due to this misclassification. An autonomous ship maintains its course and speed, expecting the misidentified fishing vessel to maneuver accordingly. However, as the fishing vessel is engaged in fishing, it has limited maneuverability and should be considered a vessel underway according to Rule 18. The failure of the autonomous vessel to give way constitutes a clear breach of Rule 18 and potentially leads to a collision. This incident raises concerns about the reliability of the vessel and autonomous navigation systems involved in complying with the law of the sea. As we have shown in Figure 11, such incidents undermine confidence in autonomous maritime technologies and emphasize the urgent need for amendments to address collision regulations for autonomous ships.

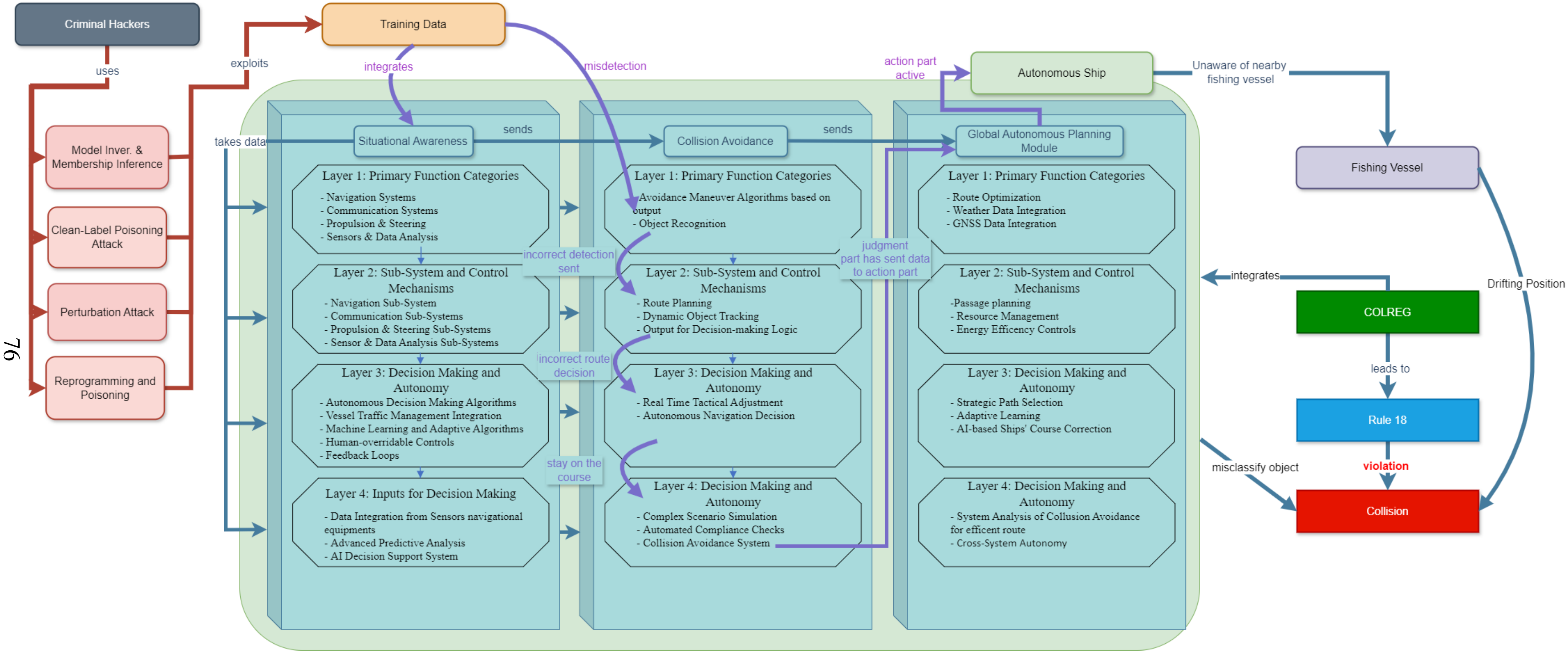
Criminal Hackers
uses
Model Inver. & Membership Inference
Clean-Label Poisoning Attack
Perturbation Attack
Reprogramming and Poisoning
exploits
Training Data
integrates
misdetection
takes data
Situational Awareness
sends
Collision Avoidance
sends
Global Autonomous Planning Module
action part active
Autonomous Ship
Unaware of nearby fishing vessel
Fishing Vessel
Drifting Position
integrates
COLREG
leads to
Rule 18
violation
Collision
misclassify object
incorrect detection sent
incorrect route decision
stay on the course
judgment part has sent data to action part
Layer 1: Primary Function Categories
- Navigation Systems
- Communication Systems
- Propulsion & Steering
- Sensors & Data Analysis
Layer 2: Sub-System and Control Mechanisms
- Navigation Sub-System
- Communication Sub-Systems
- Propulsion & Steering Sub-Systems
- Sensor & Data Analysis Sub-Systems
Layer 3: Decision Making and Autonomy
- Autonomous Decision Making Algorithms
- Vessel Traffic Management Integration
- Machine Learning and Adaptive Algorithms
- Human-overridable Controls
- Feedback Loops
Layer 4: Inputs for Decision Making
- Data Integration from Sensors navigational equipments
- Advanced Predictive Analysis
- AI Decision Support System
Layer 1: Primary Function Categories
- Avoidance Maneuver Algorithms based on output
- Object Recognition
Layer 2: Sub-System and Control Mechanisms
- Route Planning
- Dynamic Object Tracking
- Output for Decision-making Logic
Layer 3: Decision Making and Autonomy
- Real Time Tactical Adjustment
- Autonomous Navigation Decision
Layer 4: Decision Making and Autonomy
- Complex Scenario Simulation
- Automated Compliance Checks
- Collision Avoidance System
Layer 1: Primary Function Categories
- Route Optimization
- Weather Data Integration
- GNSS Data Integration
Layer 2: Sub-System and Control Mechanisms
-Passage planning
- Resource Management
- Energy Efficency Controls
Layer 3: Decision Making and Autonomy
- Strategic Path Selection
- Adaptive Learning
- AI-based Ships' Course Correction
Layer 4: Decision Making and Autonomy
- System Analysis of Collusion Avoidance for efficent route
- Cross-System Autonomy

Figure 11. Violation of the Rule 18 Attack Path Diagram.

Incorrect Inputs for Decision Making

The security of autonomous ships depends heavily on the integrity of their decision-making systems. Figure 12 presents a network of potential vulnerabilities where attackers ranging from hacktivists to state-sponsored pirates can exploit critical navigation and operational systems through spoofing, jamming, and data manipulation that is an input for the decision-making layer. These attacks can compromise navigation systems, AI decision-making errors, and sensor spoofing, ultimately affecting path planning, weather routing, and ship handling. At the center of the system is the Autonomous Vessel, which processes inputs from various subsystems such as ECDIS and collision avoidance systems. Due to cyberattacks, misclassified objects or incorrect positional data can cause collision scenarios that violate COLREG rules. This rule outlines the responsibilities of vessels to avoid collisions and underlines the need for accurate data interpretation and response. The diagram underlines the step-by-step effects of cyberthreats on autonomous ships and the importance of strengthening cybersecurity measures to protect against such vulnerabilities.

5.2.7 Determine Mitigations

In this section, we have included the mitigation strategies of possible cyberattacks, which is the 7th and final stage of PASTA threat modeling, in our threat model to prevent potential conflicts that autonomous ships will face in possible cyberattacks in the future.

Mitigation Strategies for ECDIS

Hardware and Configuration

1. Secure all accessible physical ports to impede unauthorized access, focusing on USB ports, which are common entry points for malicious devices.
2. Properly configure firewalls to effectively manage and monitor incoming and outgoing network traffic, ensuring no unauthorized data penetrating the network.
3. Establish and rigorously enforce policies centered around using strong, complex passwords and mandate regular changes to these credentials to prevent unauthorized system access.

Software and System Integrity

1. Ensure that all software, especially the operating system on which the ECDIS runs, is consistently updated with the latest security patches to mitigate known vulnerabilities.
2. Deploy reputable anti-virus and anti-malware solutions that offer real-time protection

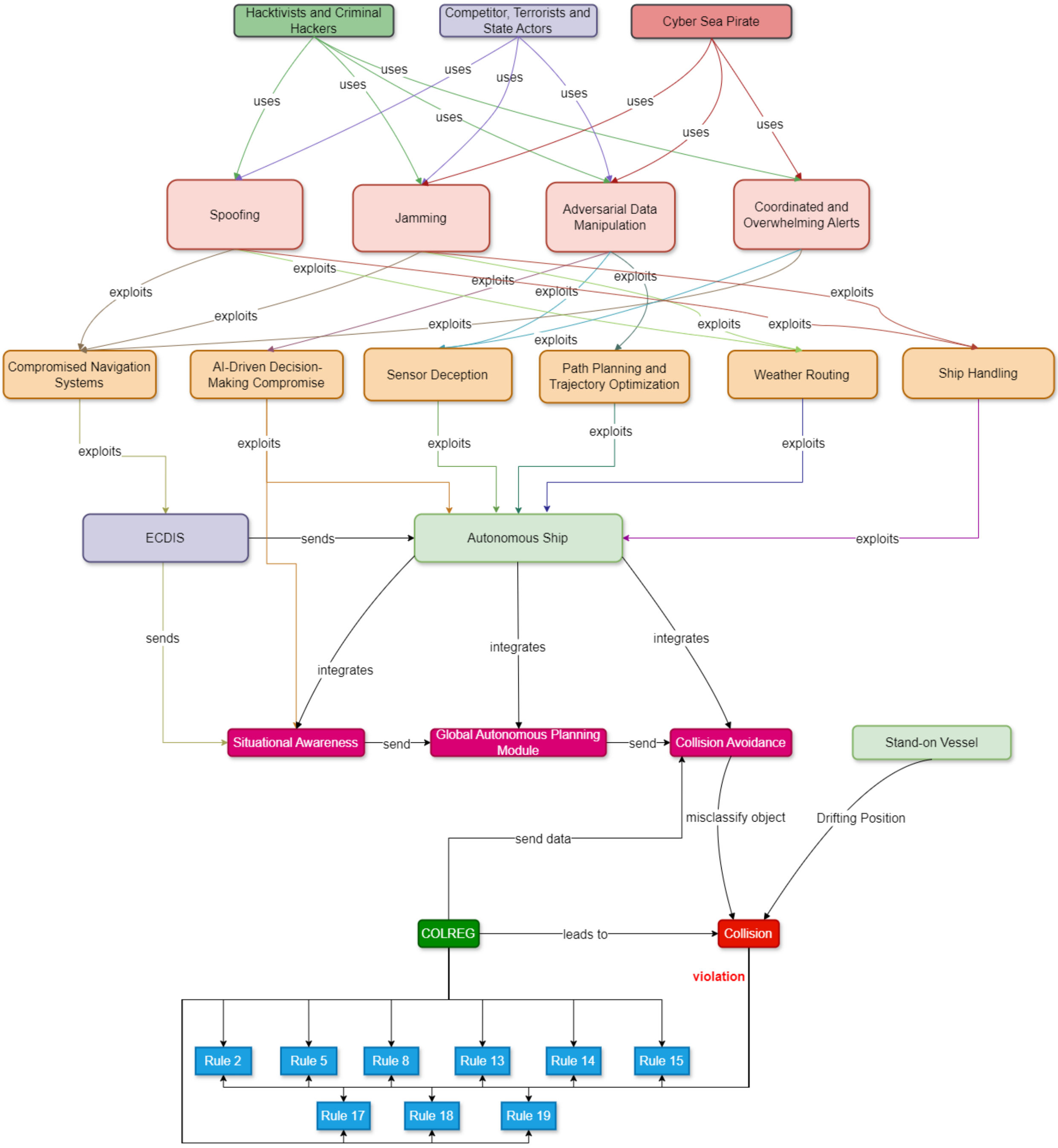

Figure 12. Diagram of Potential Attack Paths for Decision Support Systems Compromised Through Input Manipulation.

against malicious software threats.

3. Adopt application whitelisting to restrict the execution of unauthorized applications, thereby preventing the potential execution of malicious or unauthorized software.
4. Conduct routine security audits and vulnerability assessments to discover and rectify potential security gaps proactively.

Lack of Segmentation

1. Implement network segmentation to isolate the ECDIS from non-essential systems, reducing the potential for widespread network compromise.
2. Utilize Access control lists and network zoning in conjunction with stringent firewall rules to control data flow across the network, ensuring that ECDIS and other segments communicate securely.

Social Engineering and Phishing

1. Conduct extensive cybersecurity awareness training for all personnel, focusing on recognizing and responding appropriately to social engineering and phishing attempts.
2. Employ advanced email and web filtering technologies capable of identifying and intercepting phishing attempts and accessing malicious websites.

Malware Installation

1. Utilize advanced endpoint protection platforms with real-time scanning capabilities to identify and neutralize malware threats promptly.
2. Restrict administrative privileges, limiting the ability of unauthorized personnel to install potentially malicious software.

DoS Attacks

1. Leverage intrusion detection and prevention systems that are capable of identifying and mitigating DoS attack patterns.
2. Design system architecture with redundancy in mind to maintain critical functionalities under excessive load conditions.

Eavesdropping

1. Encrypt all sensitive communications to ensure data confidentiality and integrity.

2. Adopt using secure communication protocols such as Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) for all data transmissions, replacing less secure alternatives.

Unauthorized Access

1. Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to strengthen system access security.
2. Perform periodic reviews of user access levels and privileges, ensuring that they remain appropriate for each user's role and responsibilities, and revoke any unnecessary privileges.
3. Develop and implement a comprehensive Identity and Access Management (IAM) strategy to meticulously control and monitor access to the ECDIS and associated systems.

Mitigation Strategies for ECDIS Sub-Systems

Communication Protocol

1. Regularly update and secure communication protocols to patch known vulnerabilities, ensuring the strongness of AIS data transmission.
2. To enhance confidentiality and integrity, transition to secure, encrypted communication channels for AIS data transmission.

Absence of Encryption and Authentication

1. Implement encryption for AIS data transmissions, thus securing the data against unauthorized interception and tampering.
2. Employ strong authentication measures to reliably verify the identities of AIS data sources and receivers, ensuring that data can be trusted.

Integration with Navigation

1. Ensure that the integration of AIS into the ship's navigation system is conducted via secure interfaces to prevent any vulnerabilities from spreading across systems.
2. Continuously monitor and validate data exchange between AIS and other navigational systems, promptly detecting and responding to any abnormal or unexpected data patterns.

Default Passwords and Unauthorized Access

1. Immediately replace default passwords upon system initialization and enforce regular updates to these passwords.
2. Utilize strong, complex password schemes and consider the adoption of multi-factor authentication mechanisms to reinforce system access control.
3. Consistently conduct audits and monitor access logs to identify and respond to unauthorized access attempts swiftly.

DoS Attacks and Data Manipulation

1. Implement network protection measures, such as rate limiting and traffic pattern analysis, to detect and mitigate DoS attacks.
2. Apply rigorous data validation processes and sanity checks to verify the accuracy and consistency of AIS data.

Eavesdropping and Jamming

1. Employ techniques like frequency hopping or spread spectrum to complicate jamming efforts against AIS communications.
2. Secure communication signals through encryption, thereby significantly reducing the risk of eavesdropping.

Spoofing and AIS Data Manipulation

1. To authenticate information, cross-validate AIS data with alternate data sources, such as radar or visual confirmations.
2. Implement sophisticated anomaly detection systems to monitor for and alert on unusual AIS data patterns indicative of spoofing activities.

DoS Attacks

1. Establish alternative communication channels to maintain AIS functionality during an attack, ensuring continuity of critical operations.
2. Prepare AIS systems to operate under degraded conditions if required, with the capability to transition to backup systems.

Ghost Ships and False Information

1. Integrate and cross-check AIS data against multiple data sources to authenticate vessel presence and positional accuracy.
2. Utilize behavioral analysis algorithms to detect irregular vessel behavior that could suggest the presence of ghost ships or the transmission of false AIS signals.

Data Integrity Concerns

1. Incorporate the use of checksum, cryptography hashes, and digital signatures to ensure and validate the integrity of data being transmitted and received.
2. Adopt secure communication protocols that inherently provide data integrity checks to prevent tampering with the information in transit.

Confidentiality Breaches

1. Encrypt all sensitive data transmissions associated with GMDSS operations, ensuring that such information remains confidential and inaccessible to unauthorized entities.
2. Implement stringent access control measures and continuous monitoring protocols for GMDSS systems, limiting access to sensitive data strictly to authorized personnel.

False Data Transmission and Identity Spoofing

1. Utilize strong authentication protocols that can accurately verify the identity of the sources sending messages through the GMDSS.
2. Systematically cross-check and verify the accuracy of the information received via GMDSS against other independent systems to ensure its reliability.

Unauthorized Access and Emergency Protocol Tampering

1. Establish and enforce comprehensive access controls and detailed audit trails to monitor and prevent any unauthorized access to emergency systems.
2. Apply Role-Based Access Control (RBAC) mechanisms to confirm that only authorized personnel with explicit credentials can access and modify emergency protocols.

Signal Jamming and Spoofing

1. Employ advanced anti-jamming techniques, including frequency hopping, to mitigate the risk and impact of signal jamming attempts.
2. Secure all critical communication channels with authentication and encryption to defend against attempts to spoof communications.

RF Signal Disruption

1. Establish and maintain alternative communication channels as a contingency to ensure continued operation should primary RF signals face disruption.
2. Integrate systems capable of detecting when an RF signal has been compromised, with the capability to automatically switch to alternate methods of communication to maintain operational continuity.

Authentication and Encryption Deficiencies

1. Implement stringent encryption standards across all GMDSS communications to preserve the confidentiality and integrity of the transmitted data.
2. Enforce the use of multi-factor authentication processes to verify that only authorized entities communicate on GMDSS networks.

Mitigation Strategies for Adversarial Attacks

Perturbation Attack

1. Implement adversarial training techniques, wherein ML models are trained with intentionally perturbed inputs. This process aids in enhancing the models' resilience against similar attacks.
2. Utilize model assembling strategies to aggregate predictions from multiple models, thereby diminishing the impact of any single model's perturbations on overall decision-making.

Model Inversion and Membership Inference

1. Limit the granularity of information returned from queries to ML models, preventing attackers from deducing sensitive information about the model's data.
2. Ensure ML models are regularly updated and patched to safeguard against vulnerabilities that could be exploited in these types of attacks.

Model Stealing

1. Restrict access to ML model APIs, limiting the ability of attackers to make repeated queries necessary for reverse-engineering the model.
2. Embed digital watermarks within the ML model to facilitate identifying and tracing unauthorized usage.

Physical Domain Examples

1. Validate sensor data through redundancy checks, verifying data accuracy with multiple sources before it is fed into decision-making systems.
2. Implement physical tamper detection systems to identify compromise or manipulation of sensors or input devices.

Supply Chain and ML Lifecycle Attacks

1. Secure the ML model supply chain, ensuring data provenance, securing data storage, and safeguarding data integrity throughout its transit.
2. Conduct comprehensive security audits at each stage of the ML lifecycle, from initial data collection to final model deployment.

Backdoor Attacks and Software Dependency Exploits

1. Perform detailed code reviews and dependency analyses to identify and rectify potential backdoors within the software.
2. Employ software composition analysis tools to oversee and manage the use of open-source components, mitigating risks associated with known vulnerabilities.

Reprogramming and Poisoning

1. Enforce strict access controls and code integrity checks to prevent unauthorized modifications to ML models.
2. Utilize anomaly detection techniques to identify atypical data patterns that may signify a poisoning attempt.

Evasion through Deep Learning Model Manipulation

1. Apply model hardening methods, such as feature squeezing and input pre-processing, to diminish the model's susceptibility to minor perturbations.
2. Implement continuous monitoring and dynamic model updating to rapidly address and neutralize evasion attempts.

Clean-Label Poisoning Attack

1. Maintain the integrity of training data through regular audits and validations, ensuring the data remains interrupted.

2. Employ advanced outlier detection algorithms during the model training phase to detect and exclude poisoned data effectively.

Mitigation Strategies for Incorrect Inputs to Decision Making

Compromised Navigation Systems

1. Implement system redundancy for all critical navigation components to ensure continuity via a verified backup data source in any situation.
2. Conduct regular updates and apply security patches to navigation systems, safeguarding against exploitation of known vulnerabilities.
3. Perform systematic integrity checks of the navigation data to confirm its accuracy, thereby ensuring the reliability of the information used for decision-making.

AI-Driven Decision-Making Compromise

1. Where possible, validate AI-generated decisions through redundancy checks and human oversight to ensure decisions are logical and safe.
2. Continuously retrain AI models with up-to-date data, allowing them to adapt to new threats and changing conditions effectively.
3. Monitor outputs from AI systems for anomalies or inconsistencies that may suggest manipulation or compromise.

Sensor Deception

1. Utilize sensor fusion techniques to validate and corroborate data across multiple sensor inputs before utilization in decision-making processes.
2. Implement advanced anomaly detection mechanisms to identify and discount deceptive or manipulated sensor inputs.

Path Planning and Trajectory Optimization

1. Use historical data and simulations to apply cross-validation techniques to ensure that path-planning algorithms generate realistic and safe navigation routes.
2. Develop fail-safe mechanisms that can initiate manual control or activate safe-stop procedures if inconsistencies in path planning data are detected.

Weather Routing and Ship Handling

1. Integrate data from multiple weather sources and perform cross-validation to confirm the accuracy of weather information.
2. Employ strong error-checking algorithms designed to detect and dismiss implausible or manipulated weather data inputs.

Adversarial Data Manipulation

1. Integrate adversarial example detection systems to identify and mitigate manipulated inputs before they impact decision-making.
2. Strengthen AI models against adversarial tactics through comprehensive adversarial training methodologies.

Coordinated and Overwhelming Alerts

1. Design and implement sophisticated alert management systems capable of prioritizing and filtering alerts, thereby preventing information overload.
2. Provide specialized training for the RCC to enhance their ability to distinguish between legitimate and false alerts, ensuring that true emergencies are recognized and addressed promptly.

6. Discussion and Conclusion

6.1 Discussion

This work has begun to investigate the application of the PASTA threat modeling framework to the decision-making of AI on autonomous ships, including ECDIS on autonomous ships and navigational comparisons integrated into ECDIS, to enhance COLREG compliance. Through systematic analysis, this research has identified critical cyberthreats and vulnerabilities within ECDIS and demonstrated how these could potentially impact the ability of autonomous ships to comply with COLREG.

The implementation of PASTA provided a comprehensive decomposition of ECDIS, highlighting specific threat elements, scenarios, and vulnerabilities they could exploit. In particular, the study visualized how cyberthreats can compromise navigational accuracy and lead to potential violations of COLREG rules, such as incorrect maneuvering or failure to maintain a safe distance from other vessels. This highlights the importance of cybersecurity in autonomous maritime navigation and the critical need for strong cyber defense mechanisms.

As shown in the application of PASTA threat modeling, non-compliance, such as Rule 18 responsibilities between vessels in COLREG examined in Section 5.2.6, for example, can lead to potential accidents and economic losses or even human loss. These discussions emphasized the need for continued research and development to strengthen the cybersecurity framework for autonomous ships and ensure safe and compliant navigation in accordance with international maritime regulations.

6.2 Conclusion

The findings of this thesis contribute significantly to the understanding of cybersecurity threats in autonomous maritime, particularly with regard to ECDIS systems and their compliance with COLREG. By applying the PASTA threat modeling framework, this research has identified key vulnerabilities and proposed mitigating strategies to improve the security posture of autonomous vessels. This study underlines the imperative to integrate cybersecurity into the design and operation of autonomous ships to ensure their safe, efficient, and regulatory-compliant navigation.

Furthermore, this research highlights the changing cyberthreats with the development of AI/ML and the continuous need for adaptive and forward-thinking cybersecurity strategies in the maritime sector. As autonomous maritime transport moves towards a more widespread future, integrating comprehensive cybersecurity measures will be important to protect these advanced vessels against potential threats and thus enable them to contribute to a safer and more efficient maritime transport system.

6.3 Study Limitations

While this study is comprehensive, it also recognizes some limitations that may affect the scope and applicability of its findings. One of these limitations is the rapid development of cyberthreats, which may lead to the emergence of new vulnerabilities after the study. At this point, cyberspace in this domain requires continuous analysis and adaptation of the threat modeling framework to remain effective and current.

Another limitation is that the study is based on existing vulnerabilities identified in the literature. Given the rapid advances in technology and cyber tactics, these vulnerabilities must be regularly updated to reflect the current threat landscape accurately. This reliance emphasizes the importance of continuous research and documentation of new vulnerabilities in autonomous ship systems, including ECDIS and its subsystems given in Section 2.1.4.

Furthermore, the findings of this study have not been tested in real-world scenarios, which points to an important limitation. While theoretical analysis and expert opinions are valuable, they cannot fully replicate the complexities and unpredictability of real operational environments. Real-world testing can provide critical insights into the practical challenges and effectiveness of the proposed cybersecurity measures and PASTA implementation.

6.4 Recommendations for Future Research

A primary direction for future research is the practical implementation and testing of the cybersecurity measures and PASTA framework developed in this study. Testing these strategies in real-world scenarios on autonomous ships will validate their effectiveness and reveal practical challenges not seen in the theoretical analysis. These applications can be tested in a lab simulation environment in the future, or they can be implemented in real time to develop autonomous ships.

Developing AI/ML used in autonomous ships' cyberthreats requires constant vigilance and adaptation. Future work should continuously identify and assess new vulnerabilities in autonomous ship systems, including but not limited to ECDIS and its components. Establishing a mechanism for regularly updating and assessing potential threats will ensure that cybersecurity measures remain effective against the latest risks and that maritime operations are protected. Beyond ECDIS, applying the PASTA framework to other critical systems on autonomous ships can provide comprehensive insights into the cybersecurity environment.

To solidify the applicability of the research findings, future studies should aim to involve a more diverse group of experts in various fields related to autonomous maritime and cybersecurity. Broadening the range of expert validation can reveal unique insights, identify overlooked challenges, and develop innovative solutions to the cybersecurity challenges faced by autonomous maritime operations. The maritime sector could benefit from research into developing adaptive cybersecurity frameworks. Potentially powered by ML and AI, these frameworks can dynamically evolve in response to new threats and technological developments.

References

[1] Mohamad Issa et al. “Maritime Autonomous Surface Ships: Problems and Challenges Facing the Regulatory Process”. In: *Sustainability* 14.23 (2022). ISSN: 2071-1050. DOI: 10.3390/su142315630. URL: https://www.mdpi.com/2071-1050/14/23/15630.

[2] Jiwoon Yoo and Yonghyun Jo. “Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology”. In: *Sensors* 23.11 (2023). ISSN: 1424-8220. DOI: 10.3390/s23115033. URL: https://www.mdpi.com/1424-8220/23/11/5033.

[3] Bilhanan Silverajan, Mert Ocak, and Benjamin Nagel. “Cybersecurity Attacks and Defences for Unmanned Smart Ships”. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2018, pp. 15–20. DOI: 10.1109/Cybermatics_2018.2018.00037.

[4] Marko Höyhtyä and Jussi Martio. “Integrated Satellite–Terrestrial Connectivity for Autonomous Ships: Survey and Future Research Directions”. In: *Remote Sensing* 12.15 (2020). ISSN: 2072-4292. DOI: 10.3390/rs12152507. URL: https://www.mdpi.com/2072-4292/12/15/2507.

[5] Mawuli Afenyo and Livingstone D. Caesar. “Maritime cybersecurity threats: Gaps and directions for future research”. In: *Ocean & Coastal Management* 236 (2023), p. 106493. ISSN: 0964-5691. DOI: https://doi.org/10.1016/j.ocecoaman.2023.106493. URL: https://www.sciencedirect.com/science/article/pii/S0964569123000182.

[6] Adam James Fenton and Ioannis Chapsos. “Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS)”. In: *Frontiers in Computer Science* 5 (2023). ISSN: 2624-9898. DOI: 10.3389/fcomp.2023.1151188. URL: https://www.frontiersin.org/articles/10.3389/fcomp.2023.1151188.

[7] Hasan Mahbub Tusher et al. “Cyber security risk assessment in autonomous shipping”. In: *Maritime Economics & Logistics* 24 (June 2022). DOI: 10.1057/s41278-022-00214-0.

[8] Paweł Zalewski. “Integrity Concept for Maritime Autonomous Surface Ships’ Position Sensors”. In: *Sensors* 20.7 (2020). ISSN: 1424-8220. DOI: 10.3390/s20072075. URL: https://www.mdpi.com/1424-8220/20/7/2075.

[9] Lokukaluge Perera and Bjørn-Morten Batalden. “Possible COLREGs Failures under Digital Helmsman of Autonomous Ships”. In: June 2019. DOI: 10.1109/OCEANSE.2019.8867475.

[10] Mehrangiz Shahbakhsh, Gholam Reza Emad, and Stephen Cahoon. “Industrial revolutions and transition of the maritime industry: The case of Seafarer’s role in autonomous shipping”. In: *The Asian Journal of Shipping and Logistics* 38.1 (2022), pp. 10–18. ISSN: 2092-5212. DOI: https://doi.org/10.1016/j.ajsl.2021.11.004. URL: https://www.sciencedirect.com/science/article/pii/S2092521221000511.

[11] Giuseppe Aiello, Antonio Giallanza, and Giuseppe Mascarella. “Towards Shipping 4.0. A preliminary gap analysis”. In: *Procedia Manufacturing* 42 (2020). International Conference on Industry 4.0 and Smart Manufacturing (ISM 2019), pp. 24–29. ISSN: 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2020.02.019. URL: https://www.sciencedirect.com/science/article/pii/S2351978920305588.

[12] Hans-Christoph Burmeister et al. “Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective”. In: *International Journal of e-Navigation and Maritime Economy* 1 (2014), pp. 1–13. ISSN: 2405-5352. DOI: https://doi.org/10.1016/j.enavi.2014.12.002. URL: https://www.sciencedirect.com/science/article/pii/S2405535214000035.

[13] Henrik Lemcke Alfheim et al. “Development of a Dynamic Positioning System for the ReVolt Model Ship”. In: *IFAC-PapersOnLine* 51.29 (2018). 11th IFAC Conference on Control Applications in Marine Systems, Robotics, and Vehicles CAMS 2018, pp. 116–121. ISSN: 2405-8963. DOI: https://doi.org/10.1016/j.ifacol.2018.09.479. URL: https://www.sciencedirect.com/science/article/pii/S2405896318321682.

[14] Marte Hvarnes Evensen. “Safety and security of autonomous vessels. Based on the Yara Birkeland project”. MA thesis. The University of Bergen, 2020.

[15] Fraunhofer CML. *MUNIN - Maritime Unmanned Navigation through Intelligence in Networks*. https://www.unmanned-ship.org/munin/. Accessed: 2024-03-31. 2016.

[16] Simon Adams. *ReVolt – next generation short sea shipping*. 2014. URL: https://www.dnv.com/news/revolt-next-generation-short-sea-shipping-7279/ (visited on 03/31/2024).

[17] Yara International. *Yara Birkeland Press Kit*. https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/. Accessed: 2024-03-31. 2022.

[18] The Nippon Foundation. *MEGURI2040 Fully Autonomous Ship Program*. https://www.nippon-foundation.or.jp/en/what/projects/meguri2040. Accessed: 2024-03-31. 2022.

[19] Ivana Jovanović et al. "The feasibility of autonomous low-emission ro-ro passenger shipping in the Adriatic Sea". In: *Ocean Engineering* 247 (2022), p. 110712. ISSN: 0029-8018. DOI: https://doi.org/10.1016/j.oceaneng.2022.110712. URL: https://www.sciencedirect.com/science/article/pii/S0029801822001640.

[20] Ziaul Haque Munim and Hercules Haralambides. "Advances in maritime autonomous surface ships (MASS) in merchant shipping". In: *Maritime Economics & Logistics* 24.2 (2022), pp. 181–188.

[21] Sarang Thombre et al. "Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review". In: *IEEE Transactions on Intelligent Transportation Systems* 23.1 (2022), pp. 64–83. DOI: 10.1109/TITS.2020.3023957.

[22] Amit Sharma, Tae-eun Kim, and Salman Nazir. "Catching up with time? Examining the STCW competence framework for autonomous shipping". In: Oct. 2019.

[23] Mathew J Walter et al. "Adversarial AI Testcases for Maritime Autonomous Systems". In: *AI, Computer Science and Robotics Technology* (Apr. 2023). DOI: 10.5772/acrt.15. URL: https://doi.org/10.5772/acrt.15.

[24] Changui Lee and Seojeong Lee. "Evaluating the Vulnerability of YOLOv5 to Adversarial Attacks for Enhanced Cybersecurity in MASS". In: *Journal of Marine Science and Engineering* 11.5 (2023). ISSN: 2077-1312. DOI: 10.3390/jmse11050947. URL: https://www.mdpi.com/2077-1312/11/5/947.

[25] Victor Bolbot et al. "A novel cyber-risk assessment method for ship systems". In: *Safety Science* 131 (2020), p. 104908. ISSN: 0925-7535. DOI: https://doi.org/10.1016/j.ssci.2020.104908. URL: https://www.sciencedirect.com/science/article/pii/S0925753520303052.

[26] Yang Gu et al. "Unmanned Surface Vehicle Collision Avoidance Path Planning in Restricted Waters Using Multi-Objective Optimisation Complying with COLREGs". In: *Sensors* 22 (Aug. 2022), p. 5796. DOI: 10.3390/s22155796.

[27] Illkyun Im, Dongryeol Shin, and Jongpil Jeong. "Components for Smart Autonomous Ship Architecture Based on Intelligent Information Technology". In: *Procedia Computer Science* 134 (2018). The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops, pp. 91–98. ISSN: 1877-0509. DOI: `https://doi.org/10.1016/j.procs.2018.07.148`. URL: `https://www.sciencedirect.com/science/article/pii/S1877050918311116`.

[28] Sungbaek Cho et al. "Cybersecurity considerations in autonomous ships". In: *NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, Estonia* (2022).

[29] Wilfried Honekamp. "Electronic navigation challenges for autonomous ships". In: *Mobility in a Globalised World 2017* 19 (2018), p. 211.

[30] Georgios Kavallieratos, Vasiliki Diamantopoulou, and Sokratis K. Katsikas. "Shipping 4.0: Security Requirements for the Cyber-Enabled Ship". In: *IEEE Transactions on Industrial Informatics* 16.10 (2020), pp. 6617–6625. DOI: `10.1109/TII.2020.2976840`.

[31] Kimberly Tam and Kevin Jones. "Cyber-Risk Assessment for Autonomous Ships". In: *Cyber Security* (May 2018), p. 9. DOI: `10.1109/CyberSecPODS.2018.8560690`.

[32] Haitong Xu, Hao Rong, and C. Guedes Soares. "Use of AIS data for guidance and control of path-following autonomous vessels". In: *Ocean Engineering* 194 (2019), p. 106635. ISSN: 0029-8018. DOI: `https://doi.org/10.1016/j.oceaneng.2019.106635`. URL: `https://www.sciencedirect.com/science/article/pii/S0029801819307553`.

[33] Ewelina Ziajka-Poznańska and Jakub Montewka. "Costs and Benefits of Autonomous Shipping—A Literature Review". In: *Applied Sciences* 11.10 (2021). ISSN: 2076-3417. DOI: `10.3390/app11104553`. URL: `https://www.mdpi.com/2076-3417/11/10/4553`.

[34] Ismail Kurt and Murat Aymelek. "Operational and economic advantages of autonomous ships and their perceived impacts on port operations". In: *Maritime Economics & Logistics* 24.2 (2022), pp. 302–326.

[35] International Maritime Organization. *COLREG: Convention on the International Regulations for Preventing Collisions at Sea*. `https://www.imo.org/en/About/Conventions/Pages/COLREG.aspx`.

[36] Tony UcedaVelez and Marco M Morana. *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

[37] Jan Vinnem and Ingrid Utne. "Risk from cyberattacks on autonomous ships". In: Ingrid, June 2018, pp. 1485–1492. ISBN: 9781351174664. DOI: 10.1201/9781351174664-188.

[38] Lokukaluge Perera. "Autonomous Ship Navigation Under Deep Learning and the Challenges in COLREGs". In: June 2018. DOI: 10.1115/OMAE2018-77672.

[39] Amalie Heiberg et al. "Risk-based implementation of COLREGs for autonomous surface vehicles using deep reinforcement learning". In: *Neural Networks* 152 (2022), pp. 17–33. ISSN: 0893-6080. DOI: https://doi.org/10.1016/j.neunet.2022.04.008. URL: https://www.sciencedirect.com/science/article/pii/S0893608022001435.

[40] Ziaul Munim. "Autonomous ships: a review, innovative applications and future maritime business models". In: *Supply Chain Forum* 20 (June 2019), pp. 266–279. DOI: 10.1080/16258312.2019.1631714.

[41] Ramanpreet Kaur, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial intelligence for cybersecurity: Literature review and future research directions". In: *Information Fusion* 97 (2023), p. 101804. ISSN: 1566-2535. DOI: https://doi.org/10.1016/j.inffus.2023.101804. URL: https://www.sciencedirect.com/science/article/pii/S1566253523001136.

[42] Farha Jahan et al. "Security Modeling of Autonomous Systems: A Survey". In: *ACM Comput. Surv.* 52.5 (2019). ISSN: 0360-0300. DOI: 10.1145/3337791. URL: https://doi.org/10.1145/3337791.

[43] Elspeth Hannaford, Pieter J. A. Maes, and Edwin van Hassel. "Autonomous ships and the collision avoidance regulations: a licensed deck officer survey". In: *WMU Journal of Maritime Affairs* 21 (2022), pp. 233–266. URL: https://api.semanticscholar.org/CorpusID:248734237.

[44] Lokukaluge P. Perera et al. "Experimental Evaluations on Ship Autonomous Navigation and Collision Avoidance by Intelligent Guidance". In: *IEEE Journal of Oceanic Engineering* 40.2 (2015), pp. 374–387. DOI: 10.1109/JOE.2014.2304793.

[45] Michele Martelli et al. "A COLREGs-Compliant Decision Support Tool to Prevent Collisions at Sea". In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 17.2 (2023), pp. 347–353. ISSN: 2083-6473. DOI: 10.12716/1001.17.02.11. URL: ./Article_A_COLREGs-Compliant_Decision_Support_Martelli,66,1306.html.

[46] Tengesdal Trym, Edmund F. Brekke, and Tor A. Johansen. "On Collision Risk Assessment for Autonomous Ships Using Scenario-Based MPC". In: *IFAC-PapersOnLine* 53.2 (2020). 21st IFAC World Congress, pp. 14509–14516. ISSN: 2405-8963. DOI: https://doi.org/10.1016/j.ifacol.2020.12.1454. URL: https://www.sciencedirect.com/science/article/pii/S2405896320318668.

[47] Zbigniew Pietrzykowski et al. "The autonomous navigation system of a sea-going vessel". In: *Ocean Engineering* 261 (2022), p. 112104. ISSN: 0029-8018. DOI: https://doi.org/10.1016/j.oceaneng.2022.112104. URL: https://www.sciencedirect.com/science/article/pii/S0029801822014275.

[48] Qiang Li. "A Research on Autonomous Collision Avoidance under the Constraint of COLREGs". In: *Sustainability* 15.3 (2023). ISSN: 2071-1050. DOI: 10.3390/su15032446. URL: https://www.mdpi.com/2071-1050/15/3/2446.

[49] Thomas Porathe. "Safety of Autonomous Shipping: COLREGS and Interaction between Manned and Unmanned Ships". In: Jan. 2019, pp. 4146–4153. DOI: 10.3850/978-981-11-2724-3_0655-cd.

[50] Wasif Naeem, George W. Irwin, and Aolei Yang. "COLREGs-based collision avoidance strategies for unmanned surface vehicles". In: *Mechatronics* 22.6 (2012). Special Issue on Intelligent Mechatronics (LSMS2010 AND ICSEE2010), pp. 669–678. ISSN: 0957-4158. DOI: https://doi.org/10.1016/j.mechatronics.2011.09.012. URL: https://www.sciencedirect.com/science/article/pii/S0957415811001553.

[51] Xiang-Yu Zhou et al. "A Study of the Application Barriers to the Use of Autonomous Ships Posed by the Good Seamanship Requirement of COLREGs". In: *Journal of Navigation* 73.3 (2020), pp. 710–725. DOI: 10.1017/S0373463319000924.

[52] Krzysztof Wróbel et al. "The Vagueness of COLREG versus Collision Avoidance Techniques — A Discussion on the Current State and Future Challenges Concerning the Operation of Autonomous Ships". In: *Sustainability* 14 (Dec. 2022). DOI: 10.3390/su142416516.

[53] Mohamed Amine Ben Farah et al. "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends". In: *Information* 13.1 (2022). ISSN: 2078-2489. DOI: 10.3390/info13010022. URL: https://www.mdpi.com/2078-2489/13/1/22.

[54] Meland et al. “A Retrospective Analysis of Maritime Cyber Security Incidents”. In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 15 (Jan. 2021), pp. 519–530. DOI: 10.12716/1001.15.03.04.

[55] Boyan Mednikarov, Yuliyan Tsonev, and A.D. Lazarov. “Analysis of Cybersecurity Issues in the Maritime Industry”. In: *Information & Security: An International Journal* 47 (Jan. 2020), pp. 27–43. DOI: 10.11610/isij.4702.

[56] Aybars Oruc. “Claims of State-Sponsored Cyberattack in the Maritime Industry”. In: Oct. 2020. DOI: 10.24868/issn.2515-818X.2020.021.

[57] Giacomo Longo et al. “MaCySTe: A virtual testbed for maritime cybersecurity”. In: *SoftwareX* 23 (2023), p. 101426. ISSN: 2352-7110. DOI: https://doi.org/10.1016/j.softx.2023.101426. URL: https://www.sciencedirect.com/science/article/pii/S235271102300122X.

[58] Frank Akpan et al. “Cybersecurity Challenges in the Maritime Sector”. In: *Network* 2.1 (2022), pp. 123–138. ISSN: 2673-8732. DOI: 10.3390/network2010009. URL: https://www.mdpi.com/2673-8732/2/1/9.

[59] Joseph DiRenzo, Dana A. Goward, and Fred S. Roberts. “The little-known challenge of maritime cyber security”. In: *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*. 2015, pp. 1–5. DOI: 10.1109/IISA.2015.7388071.

[60] Juan Ignacio Alcaide and Ruth Garcia Llave. “Critical infrastructures cybersecurity and the maritime sector”. In: *Transportation Research Procedia* 45 (2020). Transport Infrastructure and systems in a changing world. Towards a more sustainable, reliable and smarter mobility.TIS Roma 2019 Conference Proceedings, pp. 547–554. ISSN: 2352-1465. DOI: https://doi.org/10.1016/j.trpro.2020.03.058. URL: https://www.sciencedirect.com/science/article/pii/S2352146520302209.

[61] Giacomo Longo et al. “Attacking (and Defending) the Maritime Radar System”. In: *IEEE Transactions on Information Forensics and Security* 18 (2023), pp. 3575–3589. DOI: 10.1109/TIFS.2023.3282132.

[62] Jan Pawelski. “Cyber Threats for Present and Future Commercial Shipping”. In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 17.2 (2023), pp. 261–267. ISSN: 2083-6473. DOI: 10.12716/1001.1790.02.01. URL: ./Article_Cyber_Threats_for_Present_and_Future_Pawelski,66,1296.html.

[63] Orestis Schinas and Daniel Metzger. “Cyber-seaworthiness: A critical review of the literature”. In: *Marine Policy* 151 (2023), p. 105592. ISSN: 0308-597X. DOI: https://doi.org/10.1016/j.marpol.2023.105592. URL: https://www.sciencedirect.com/science/article/pii/S0308597X23001197.

[64] Andrej Androjna et al. “Assessing Cyber Challenges of Maritime Navigation”. In: *Journal of Marine Science and Engineering* 8.10 (2020). ISSN: 2077-1312. DOI: 10.3390/jmse8100776. URL: https://www.mdpi.com/2077-1312/8/10/776.

[65] Christoph Alexander Thieme, Ingrid Bouwer Utne, and Stein Haugen. “Assessing ship risk model applicability to Marine Autonomous Surface Ships”. In: *Ocean Engineering* 165 (2018), pp. 140–154. ISSN: 0029-8018. DOI: https://doi.org/10.1016/j.oceaneng.2018.07.040. URL: https://www.sciencedirect.com/science/article/pii/S0029801818313210.

[66] Ahmed Amro et al. “Navigation Data Anomaly Analysis and Detection”. In: *Information* 13.3 (2022). ISSN: 2078-2489. DOI: 10.3390/info13030104. URL: https://www.mdpi.com/2078-2489/13/3/104.

[67] Krzysztof Wróbel et al. “The Vagueness of COLREG versus Collision Avoidance Techniques&mdash;A Discussion on the Current State and Future Challenges Concerning the Operation of Autonomous Ships”. In: *Sustainability* 14.24 (2022). ISSN: 2071-1050. DOI: 10.3390/su142416516. URL: https://www.mdpi.com/2071-1050/14/24/16516.

[68] John Wiley & Sons and Ltd. “Diving Deeper into Pasta”. In: *Risk Centric Threat Modeling*. John Wiley & Sons and Ltd, 2015. Chap. 7, pp. 343–478. ISBN: 9781118988374. DOI: https://doi.org/10.1002/9781118988374.ch7. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118988374.ch7. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118988374.ch7.

[69] Muhammed Erbas, Shaymaa Mamdouh Khalil, and Leonidas Tsiopoulos. “Systematic literature review of threat modeling and risk assessment in ship cybersecurity”. In: *Ocean Engineering* 306 (2024), p. 118059. ISSN: 0029-8018. DOI: https://doi.org/10.1016/j.oceaneng.2024.118059. URL: https://www.sciencedirect.com/science/article/pii/S0029801824013970.

[70] Kevin Jones and Kimberly Tam. “MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment”. In: *WMU Journal of Maritime Affairs* 18 (Jan. 2019). DOI: 10.1007/s13437-019-00162-2.

[71] Kevin Jones and Kimberly Tam. “MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment”. In: *WMU Journal of Maritime Affairs* 18 (Jan. 2019). DOI: 10.1007/s13437-019-00162-2.

[72] Kimberly Tam and Kevin Jones. “Factors Affecting Cyber Risk in Maritime”. In: *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 2019, pp. 1–8. DOI: 10.1109/CyberSA.2019.8899382.

[73] Ilya S. Shipunov et al. “About the Problems of Ensuring Information Security on Unmanned Ships”. In: *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. 2019, pp. 339–343. DOI: 10.1109/EIConRus.2019.8657219.

[74] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. “Cyber-Attacks Against the Autonomous Ship”. In: *Computer Security*. Ed. by Sokratis K. Katsikas et al. Cham: Springer International Publishing, 2019, pp. 20–36. ISBN: 978-3-030-12786-2.

[75] Georgios Kavallieratos and Sokratis Katsikas. “Managing Cyber Security Risks of the Cyber-Enabled Ship”. In: *Journal of Marine Science and Engineering* 8.10 (2020). ISSN: 2077-1312. DOI: 10.3390/jmse8100768. URL: https://www.mdpi.com/2077-1312/8/10/768.

[76] Michael Howard and Steve Lipner. *THE SECURITY DEVELOPMENT LIFECYCLE*. 2006. ISBN: 9780735622142. DOI: 10.7765/9781526103482.00008.

[77] Shaymaa Mamdouh Khalil, Hayretdin Bahsi, and Tarmo Korõtko. “Threat modeling of industrial control systems: A systematic literature review”. In: *Computers & Security* 136 (2024), p. 103543. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103543. URL: https://www.sciencedirect.com/science/article/pii/S0167404823004534.

[78] Victor Bolbot et al. “A novel risk assessment process: Application to an autonomous inland waterways ship”. In: *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability* 237 (Oct. 2021). DOI: 10.1177/1748006X211051829.

[79] Panayiotis Papageorgiou et al. “Using a Proposed Risk Computation Procedure and Bow-Tie Diagram as a Method for Maritime Security Assessment”. In: *Transportation Research Record: Journal of the Transportation Research Board* (June 2023). DOI: 10.1177/03611981231173641.

[80] Boris Svilicic et al. “Maritime Cyber Risk Management: An Experimental Ship Assessment”. In: *The Journal of Navigation* 72.5 (2019), pp. 1108–1120. DOI: 10.1017/S0373463318001157.

[81] Simon Yusuf Enoch, Jang Se Lee, and Dong Seong Kim. "Novel security models, metrics and security assessment for maritime vessel networks". In: *Computer Networks* 189 (2021), p. 107934. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.107934. URL: https://www.sciencedirect.com/science/article/pii/S1389128621000797.

[82] Aybars Oruc, Ahmed Amro, and Vasileios Gkioulos. "Assessing Cyber Risks of an INS Using the MITRE ATT&amp;CK Framework". In: *Sensors* 22.22 (2022). ISSN: 1424-8220. DOI: 10.3390/s22228745. URL: https://www.mdpi.com/1424-8220/22/22/8745.

[83] Ahmed Amro and Vasileios Gkioulos. "Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth". In: *International Journal of Information Security* 22 (Nov. 2022). DOI: 10.1007/s10207-022-00638-y.

[84] Ahmed Amro, Vasileios Gkioulos, and Sokratis Katsikas. "Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework". In: *ACM Trans. Priv. Secur.* 26.2 (2023). ISSN: 2471-2566. DOI: 10.1145/3571733. URL: https://doi.org/10.1145/3571733.

[85] Ahmed Amro and Vasileios Gkioulos. "Evaluation of a Cyber Risk Assessment Approach for Cyber&ndash;Physical Systems: Maritime- and Energy-Use Cases". In: *Journal of Marine Science and Engineering* 11.4 (2023). ISSN: 2077-1312. DOI: 10.3390/jmse11040744. URL: https://www.mdpi.com/2077-1312/11/4/744.

[86] Yonghyun Jo et al. "Cyberattack Models for Ship Equipment based on the MITRE ATT&CK Framework". In: *Sensors* 22 (Feb. 2022), p. 1860. DOI: 10.3390/s22051860.

[87] Andreas Wolf et al. "The PASTA threat model implementation in the IoT development life cycle". In: *GI-Jahrestagung*. 2020. URL: https://api.semanticscholar.org/CorpusID:222007827.

[88] Livinus Nweke and Stephen Wolthusen. "A Review of Asset-Centric Threat Modelling Approaches". In: *International Journal of Advanced Computer Science and Applications* 11 (Mar. 2020), pp. 1–6. DOI: 10.14569/IJACSA.2020.0110201.

[89] Andreas Wolf et al. *The PASTA threat model implementation in the IoT development life cycle*. 2021. DOI: https://dl.gi.de/handle/20.500.12116/34700. URL: https://dl.gi.de/handle/20.500.12116/34700.

[90] Afnan Siddique. "Threat Modeling Methodologies for Network Security". In: ().

[91] Livinus Obiora Nweke and Stephen Wolthusen. “A review of asset-centric threat modelling approaches”. In: (2020).

[92] Victor Bolbot et al. “Safety related cyber-attacks identification and assessment for autonomous inland ships”. In: Dec. 2020, pp. 95–109. ISBN: 9788395669606. DOI: 10.2478/9788395669606-009.

[93] Dennis Bothur, Guanglou Zheng, and Craig Valli. “A critical analysis of security vulnerabilities and countermeasures in a smart ship system”. In: 2017. URL: https://api.semanticscholar.org/CorpusID:55014465.

[94] Melih Akdağ, Petter Solnør, and Tor Arne Johansen. “Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review”. In: *Ocean Engineering* 250 (2022), p. 110920. ISSN: 0029-8018. DOI: https://doi.org/10.1016/j.oceaneng.2022.110920. URL: https://www.sciencedirect.com/science/article/pii/S0029801822003444.

[95] Lokukaluge Perera. “Deep Learning towards Autonomous Ship Navigation and Possible COLREGs Failures”. In: *Journal of Offshore Mechanics and Arctic Engineering* (May 2019). DOI: 10.1115/1.4045372.

[96] Nimra Tabish and Tsai Chaur-Luh. “Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives”. In: *IEEE Access* 12 (2024), pp. 17114–17136. DOI: 10.1109/ACCESS.2024.3357082.

[97] Erik Veitch and Ole Andreas Alsos. “A systematic review of human-AI interaction in autonomous ship systems”. In: *Safety Science* 152 (2022), p. 105778. ISSN: 0925-7535. DOI: https://doi.org/10.1016/j.ssci.2022.105778. URL: https://www.sciencedirect.com/science/article/pii/S0925753522001175.

[98] Krzysztof Wróbel, Jakub Montewka, and Pentti Kujala. “Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels”. In: *Reliability Engineering & System Safety* 178 (2018), pp. 209–224. ISSN: 0951-8320. DOI: https://doi.org/10.1016/j.ress.2018.05.019. URL: https://www.sciencedirect.com/science/article/pii/S0951832017306233.

[99] Marius Brinkmann and Axel Hahn. “Physical Testbed for Highly Automated and Autonomous Vessels”. In: May 2017.

[100] Osiris A. Valdez Banda et al. “A systemic hazard analysis and management process for the concept design phase of an autonomous vessel”. In: *Reliability Engineering & System Safety* 191 (2019), p. 106584. ISSN: 0951-8320. DOI: https://doi.org/10.1016/j.ress.2019.106584. URL:

https://www.sciencedirect.com/science/article/pii/S0951832017314151.

[101] Xinyu Zhang et al. “Decision-Making for the Autonomous Navigation of Maritime Autonomous Surface Ships Based on Scene Division and Deep Reinforcement Learning”. In: *Sensors* 19.18 (2019). ISSN: 1424-8220. DOI: 10.3390/s19184055. URL: https://www.mdpi.com/1424-8220/19/18/4055.

[102] Hongguang Lyu et al. “Ship Autonomous Collision-Avoidance Strategies—A Comprehensive Review”. In: *Journal of Marine Science and Engineering* 11.4 (2023). ISSN: 2077-1312. DOI: 10.3390/jmse11040830. URL: https://www.mdpi.com/2077-1312/11/4/830.

[103] Osman Metalla et al. “Cyber Security in the Maritime Transport”. In: *Interdisciplinary Journal of Research and Development* 10 (July 2023), p. 74. DOI: 10.56345/ijrdv10n210.

[104] Syed Khandker et al. “Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience”. In: *IEEE Access* 10 (2022), pp. 29493–29505. DOI: 10.1109/ACCESS.2022.3158943.

[105] Osman Metalla et al. “Cyber Security in the Maritime Transport”. In: *Interdisciplinary Journal of Research and Development* 10 (July 2023), p. 74. DOI: 10.56345/ijrdv10n210.

[106] Changui Lee and Seojeong Lee. “Vulnerability of Clean-Label Poisoning Attack for Object Detection in Maritime Autonomous Surface Ships”. In: *Journal of Marine Science and Engineering* 11.6 (2023). ISSN: 2077-1312. DOI: 10.3390/jmse11061179. URL: https://www.mdpi.com/2077-1312/11/6/1179.

[107] Simon Blindheim and Tor Arne Johansen. “Electronic Navigational Charts for Visualization, Simulation, and Autonomous Ship Control”. In: *IEEE Access* 10 (2022), pp. 3716–3737. DOI: 10.1109/ACCESS.2021.3139767.

[108] Lokukaluge Perera. “Deep Learning towards Autonomous Ship Navigation and Possible COLREGs Failures”. In: *Journal of Offshore Mechanics and Arctic Engineering* (May 2019). DOI: 10.1115/1.4045372.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Muhammed Erbas

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Application of PASTA Threat Modeling to ECDIS in Autonomous Ships for Enhanced COLREG Compliance”, supervised by Olaf Manuel Maennel and Gábor Visky
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

08.05.2024

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.