



LJMU Research Online

Symes, S, Blanco-Davis, E, Graham, T, Wang, J and Shaw, E

The survivability of autonomous vessels from cyber-attacks

<http://researchonline.ljmu.ac.uk/id/eprint/25324/>

Article

Citation (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

Symes, S, Blanco-Davis, E, Graham, T, Wang, J and Shaw, E (2024) The survivability of autonomous vessels from cyber-attacks. Journal of Marine Engineering and Technology. pp. 1-23. ISSN 2046-4177

LJMU has developed **LJMU Research Online** for users to access the research output of the University more effectively. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LJMU Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain.

The version presented here may differ from the published version or from the version of the record. Please see the repository URL above for details on accessing the published version and note that access may require a subscription.

For more information please contact researchonline@ljmu.ac.uk

<http://researchonline.ljmu.ac.uk/>



The survivability of autonomous vessels from cyber-attacks

Steve Symes, Eddie Blanco-Davis, Tony Graham, Jin Wang & Edward Shaw

To cite this article: Steve Symes, Eddie Blanco-Davis, Tony Graham, Jin Wang & Edward Shaw (06 Dec 2024): The survivability of autonomous vessels from cyber-attacks, Journal of Marine Engineering & Technology, DOI: [10.1080/20464177.2024.2428022](https://doi.org/10.1080/20464177.2024.2428022)

To link to this article: <https://doi.org/10.1080/20464177.2024.2428022>



© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 06 Dec 2024.



Submit your article to this journal [↗](#)



Article views: 231




View related articles [↗](#)



View Crossmark data [↗](#)

The survivability of autonomous vessels from cyber-attacks

Steve Symes , Eddie Blanco-Davis, Tony Graham, Jin Wang and Edward Shaw

School of Engineering, Liverpool John Moores University, Liverpool, UK

ABSTRACT

This literature review is an investigation into the survivability of an automated vessel. More specifically, this study investigates an automated vessel's susceptibility, vulnerability and ability to recover from a cyber-security-related threat. The future of maritime shipping is trending towards transitioning to automated vessels. Automated vessels have the potential to provide significant financial and logistical benefits for shipping companies and stakeholders. The study aims to evaluate the current survivability features of an automated vessel. To achieve this aim objectively, a literature review was conducted into potential threats to automated vessels, the security features they have to combat said threats, and their ability to recover from a cyberattack. It was conducted with the defined scope of 'ship survivability'. Moreover, it was filtered into four areas: susceptibility to a threat, vulnerability to the effects of a threat, the ability to recover from an attack and case studies of previous relevant attacks. The result of the literature evaluation indicates a significant vulnerability of automated vessels. Automated vessels were found to have a high susceptibility to cyber-attacks, the effects of which have potentially significant financial effects, a high chance of significant damage to the vessel, a significant chance of injury or fatality and a low ability to recover from an attack. This study can indicate to the marine transport industry the 'gaps in the market' concerning the survivability, susceptibility, vulnerability and ability to recover from an attack against an automated vessel.

ARTICLE HISTORY

Received 6 March 2024
Accepted 16 October 2024

KEYWORDS

Automated vessels; cyber security; survivability; artificial intelligence (AI); hacking

1. Introduction

This paper is a literature review, investigating the technology available to autonomous vessels to mitigate the risk of cyber attacks. This paper first looks at the literature detailing the technology available to protect autonomous ships from cyber attacks. Then, the shortcomings of the aforementioned technology available and finally, the technology available in the engineering sector that could combat the shortcomings of the technology available. Real-world cyber attacks on the marine sector are utilised to gain more accurate knowledge of the nature of the attacks and their consequences. In Section 6 the findings are discussed with a conclusion in Section 7 detailing the further research and further need for the autonomous shipping sector.

2. Background

The maritime sector is moving towards automated shipping (Alop 2019). Automated shipping, also referred to as autonomous shipping, is an emerging technology revolutionising the transportation industry (Ahvenjarvi et al. 2019). It involves the use of advanced technologies such as artificial intelligence, machine learning and robotics to enable ships to navigate and transport goods without human intervention (Amro et al. 2023). This innovative approach offers numerous benefits, including increased efficiency, enhanced safety and improved supply chain management (Zacone and Martelli 2020; Ahmed and Gkioulos 2022; Damerius et al. 2023).

Efficiency is a significant advantage of automated shipping. By utilising AI algorithms and optimisation techniques, autonomous vessels can optimise their routes, adjust speed and course, and minimise fuel consumption (Amro et al. 2020). According to a study by Yoo *et al.*, autonomous ships can reduce fuel consumption by up to

20% compared to traditional vessels (Yoo and Park 2021). This could lead to cost savings and a reduced environmental impact.

Safety is a crucial aspect of automated shipping. With advanced sensors, cameras and AI-based decision-making tools, autonomous ships can detect and avoid obstacles, navigate through uncertain weather conditions, and mitigate the risk of accidents (Bakdi and Glad 2021). The potential of autonomous shipping to enhance maritime safety and reduce human error is highlighted in (Bakdi and Vanem 2022). Additionally, automated shipping has the potential to bring significant improvements to supply chain management. However, like most new concepts or technologies, autonomous vessels are said to have issues (Amro et al. 2023). Many of the issues reported are concerning aspects of survivability due to threats (Kardakova et al. 2020).

Survivability is defined in the naval context as 'the capability of a vessel to continue to carry out its designated mission/voyage in a combat threat environment' (Anatoliy et al. 2018). It is deemed insufficient for a vessel to merely remain afloat, to survive means to remain effective enough to complete its duties (Amro et al. 2022). Moreover, the survivability of a vessel covers more than simply the construction and design of a vessel. Various tactics, the operating environment and defence weapons or technologies, for naval and merchant vessels, play a vital role in providing a vessel with the ability to survive a threat (Zhou et al. 2018). Surviving a certain situation is not the only aspect to consider. Survivability also considers how the vessel got into the situation in the first instance (Dittman et al. 2021).

This study defines the term survivability as a vessel's susceptibility to a threat, its vulnerability to the effects of a threat and its ability to recover from the aftermath of an attack (Jung et al. 2022a). Therefore, this study will evaluate the susceptibility, vulnerability and ability to recover from a threat, with relevant autonomous vessels.

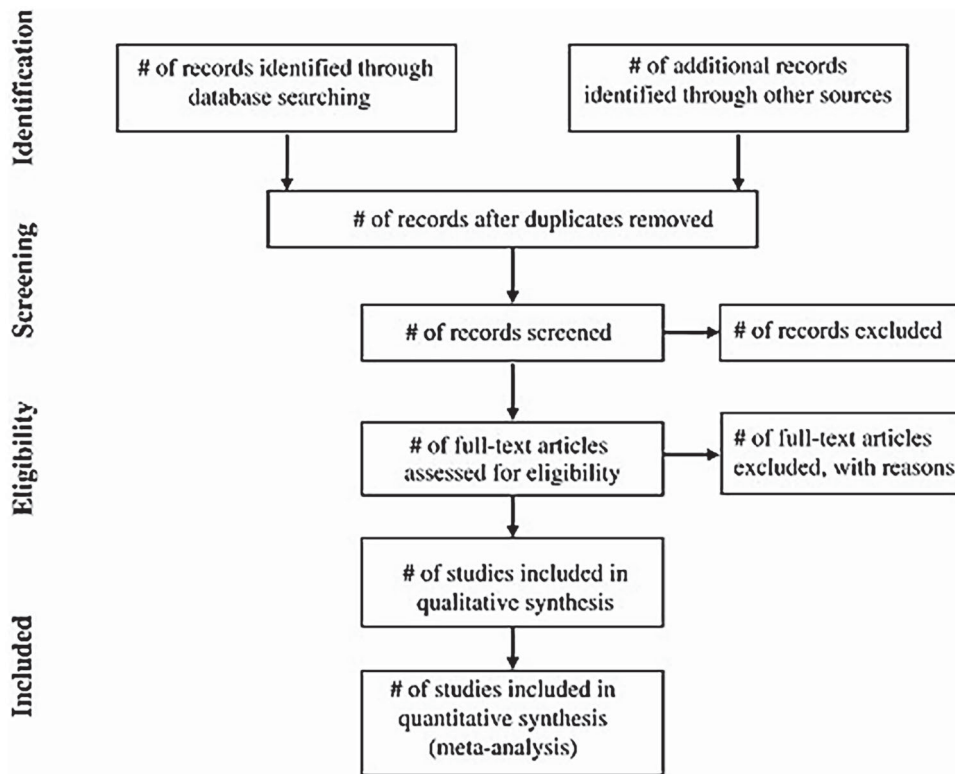


Figure 1. Flow chart of PRISMA methodology (Liberati et al. 2009).

3. Research questions

The scope and purpose of this literature review is to answer the following research questions:

- (1) What technology is available to mitigate the risk of cyber attacks on autonomous ships?
- (2) What are the shortcomings of the latest technology concerning autonomous shipping?
- (3) What technology is available to combat the shortcomings of the latest technology?
- (4) Recommendations for future research and the demand of the autonomous shipping sector?

3.1. Research hypothesis

It is hypothesised that there are many shortcomings concerning autonomous shipping's protection against cyber attacks. The increase in technology required to successfully utilise autonomous vessels could mean that there are significantly more opportunities for cyber criminals. The cost to the maritime autonomous sector could be in the millions if not billions of pounds annually.

4. Methodology

The methodology used in this literature review is preferred reporting items for systematic reviews and meta-analyses (PRISMA). PRISMA offers a standardised checklist, ensuring that the reporting of systematic reviews is transparent and complete. This framework is also applicable to various intervention-based reviews (intervention is the cornerstone behind the reason for conducting this research, as this review will pave the way for the development of a concept, assessment, demonstration, manufacture, in-service and disposal/termination cycle to tackle the issues faced by cyber criminals

targeting the maritime sector). A PRISMA methodology also ensures a clear, critical evaluation of methods, assesses potential biases and ultimately, trusts the presented review outcomes (Liberati et al. 2009).

Figure 1 is a flow chart of the methodology used for this review.

5. Literature review

The scope of the literature review covers the current technologies available or applied to a fully autonomous vessel to enhance survivability, and case studies of various threats to an automated vessel's survivability. As previously mentioned, the relevant literature is identified based on a PRISMA methodology. The four sections of PRISMA are: Identification, Screening, Eligibility and Included. These four sections are detailed below with critical questions answered.

PRISMA Identification: The literature is sourced from Web of Science, SciFinder, Scopus, Google Scholar and various newspaper articles (Rules of engagement issued to hacktivists after chaos – BBC news, (Tidy 2023), Royal Navy contractor forced to pay off cyber criminals – The Telegraph (Corfield 2023), SeeByte to Develop Secure Drone Swarm Operation Methods for Royal Navy (Manuel 2023), A Comprehensive Guide to Maritime Cybersecurity (Mission Secure 2023), Maritime cyber risk (The International Maritime Organisation (IMO), 2019). Additional sources included expert knowledge from domain experts including some of the authors of this work).

PRISMA Screening: The keywords or phrases used in the literature search are: Maritime autonomous surface ships (MASS), automated vessel, survivability, cyber attack, threats to safety, hacking and automated vessel security. A preliminary literature search indicated that the literature detailing cyber-attacks on autonomous ships is currently scarce due to the early stages of this type of vessel's implementation. Therefore, this literature review's scope was extended to

cyber-attacks on the maritime sector as a whole (for which relevant literature is more widely available). It seems that cyber-attacks on shipping companies and non-autonomous vessels will be conducted similarly against autonomous ships (Gkioulos and Ahmed 2021). The main difference is the potential consequences, as an autonomous vessel will likely be unmanned (Alop 2019).

PRISMA Eligibility: The literature search, firstly, using the Web of Science and the keywords of maritime, cyber attack, MASS and autonomous vessels showed 29 results. Secondly, a search on Scopus, using the same keywords was done and this showed 27 research papers. Thirdly, Google Scholar was used. This search resulted in 19,814 academic documents. Therefore, the additional keywords of ship survivability, a threat to safety and hacking techniques were added. This produced 547 documents. To further filter the found documents, all documents older than 2018 were omitted with specific onus on the most recent publications. This was due to the rapid technological advancement that happened circa 2018. For example, improved sensor fusion, advanced image recognition, decision-making algorithms, autonomous navigation, higher speed data transfer, communication networks (satellite and cellular) and many more. Research conducted after 2018 is more likely to incorporate the latest technological advancements mentioned prior. This final filter resulted in 204 documents (older publications were still read to gauge the concept of the evolution of maritime cyber technology).

PRISMA Included: From the literature search, 67 documents were used due to duplicate publications (46), duplicated cyber security techniques (97) and journals that were outside the age bracket (< 2019) (17) [These 17 documents were still referenced and used to gain background knowledge of the evolution of cyber prevention technologies]. The 67 documents resulted in the identification of four different technologies used to mitigate the risk of cyber attacks. These technologies are detailed in Section 5.1.

5.1. Technology available to ensure autonomous ships' survivability

To ensure the survivability of autonomous ships, several advanced technologies are available (Ahmed and Gkioulos 2022). These technologies work together to enhance the safety and reliability of autonomous vessels in various scenarios.

5.1.1. Sensor systems

Sensor Systems were a consistent feature that showed up in literature searches on various platforms. The work by Ahmed *et al.* states that autonomous ships rely on a range of sensors, including radar, light detection and ranging (LiDAR), cameras and sonar systems, to perceive their surroundings and collect real-time data (Ahmed and Gkioulos 2022). Amro *et al.* state that these sensors provide crucial information about the ship's environment, such as the presence of other vessels, obstacles and weather conditions (Amro *et al.* 2020). However, when it comes to cyber security, sensor systems on autonomous ships can present several challenges and negatives, which are as follows:

Bolbot *et al.* suggest that sensor systems can be Vulnerable to Cyber Attacks (Bolbot *et al.* 2020). Fang *et al.* state that autonomous ships rely on interconnected sensor systems that communicate with each other and external networks. This interconnectedness increases the risk of cyber-attacks, such as unauthorised access, data breaches, or manipulation of sensor data (Fang *et al.* 2022). Chang *et al.* express that malicious actors could exploit vulnerabilities in the system, potentially compromising the ship's operations, safety and sensitive information (Chang *et al.* 2021).

- Dittman *et al.* profess that Sensor Spoofing is a significant cyber threat to autonomous vessels' sensor systems (Dittman *et al.* 2021). Jung *et al.* state that sensor spoofing involves manipulating sensor data to provide false or misleading information to the ship's autonomous systems (Jung *et al.* 2022a). Chiu *et al.* express that by spoofing sensors, attackers can deceive the ship's navigation, collision avoidance, or environmental monitoring systems, leading to incorrect decisions that may endanger the vessel, its cargo and the environment (Chiu *et al.* 2011).
- Issa *et al.* detail that an autonomous ship sensor can be vulnerable to denial of service (DoS) Attacks (Issa *et al.* 2022). Ehlers *et al.* state that a DoS attack aims to disrupt the ship's sensor systems by overwhelming them with excessive requests or malicious traffic (Ehlers *et al.* 2022). Grieman *et al.* express that by targeting the sensors, such attacks can incapacitate or degrade their functionality, affecting the ship's ability to collect accurate data and make informed decisions (Grieman 2019).
- The diversity of sensor types and manufacturers, combined with varying degrees of security implementation, can result in inconsistencies and potential weak points within the overall system (Schinas and Metzger 2023). This can make sensor systems more susceptible to exploitation, increasing the risk of unauthorised access, data breaches, or malicious activities (Epikhin and Modina 2021).
- Sensor systems on autonomous ships may face challenges in terms of updating and patching security vulnerabilities (Liou 2011). Solnor *et al.* state that these systems are often deployed over long periods without regular maintenance or updates. As new security threats emerge, it can be challenging to implement timely patches or security updates to address vulnerabilities in sensor systems, leaving them exposed to potential cyber-attacks (Solnor *et al.* 2022).

The vast majority of autonomous vessels use AIS or radar systems (Ahmed and Gkioulos 2022). AIS has been shown to be vulnerable (Goudossis and Katsikas 2019; Marco *et al.* 2014). Radar, instead was detailed in terms of its vulnerability (Longo *et al.* 2023b; Longo *et al.* 2023a). More specifically, the way that these techniques could result in an autonomous vessel being dead in the water. Figure 2 shows on board sensor systems and the areas in which they are installed.

5.1.2. Artificial intelligence and machine learning

Artificial Intelligence (AI) and Machine Learning (ML) tools were another feature that consistently showed in literature searches, concerning technologies available for autonomous ship survivability. Vagale *et al.* state that AI algorithms and ML techniques play a vital role in autonomous ship survivability. They enable the vessel to process data from sensors, make intelligent decisions and adapt to dynamic situations (Vagale *et al.* 2021a). Park *et al.* state that AI algorithms help identify potential hazards, interpret sensor data, and make real-time adjustments to ensure safe navigation (Park and Kontovas 2023).

While AI and ML systems have the potential to enhance various aspects of autonomous ships, they also introduce certain negatives (Hopcraft *et al.* 2023). The following are some considerations that arose from the literature search:

- Adversarial Attacks: Kardakova *et al.* state AI and ML models are vulnerable to adversarial attacks, where malicious entities intentionally manipulate input data to deceive or exploit the system (Kardakova *et al.* 2020). Kavallieratos *et al.* advise that adversarial attacks on AI and ML systems in autonomous ships could lead to incorrect decision-making, compromised sensor data, or unauthorised access (Kavallieratos *et al.* 2020a).

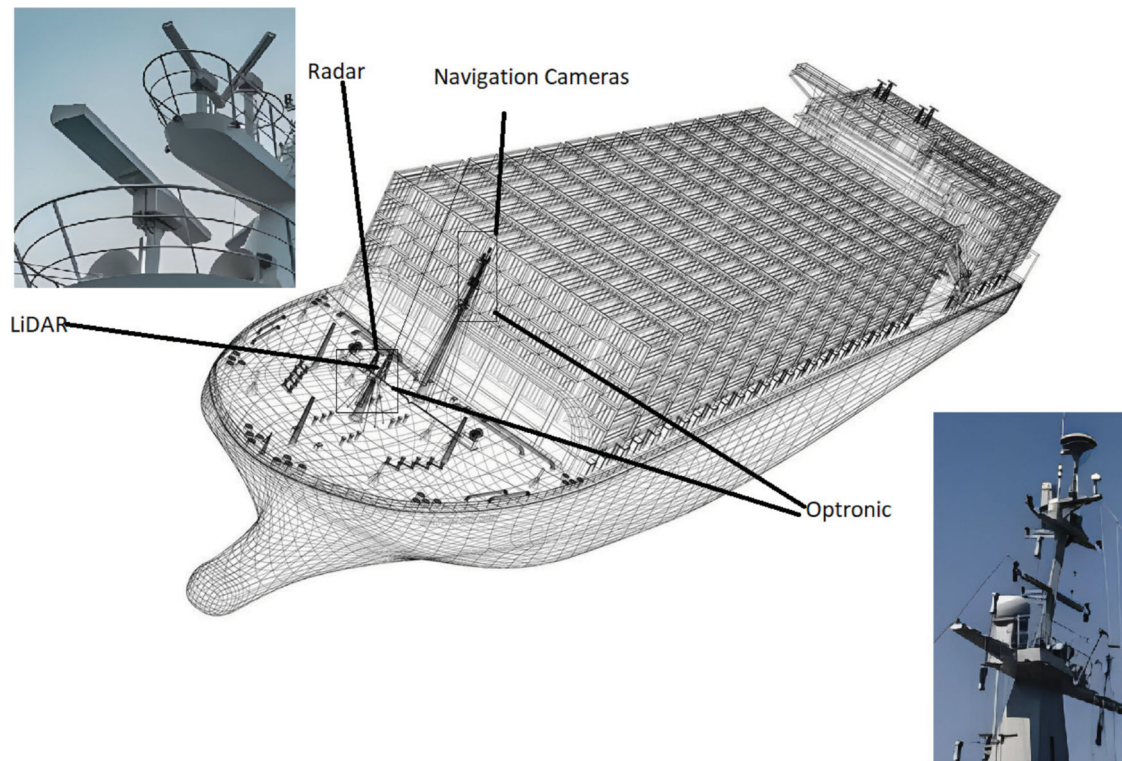


Figure 2. Autonomous ship sensor systems.

- **Data Poisoning:** Li *et al.* state that ML models depend on large volumes of training data to make accurate predictions. If the training data is compromised or manipulated with malicious intent, it can affect the performance and reliability of the AI system (Li and Yu 2020). This could lead to incorrect navigational decisions or compromised security measures as stated by Liou *et al.* (Liou 2011).
- **Lack of Explainability:** Loukas *et al.* express that deep learning models, which are commonly used in AI systems, often lack transparency and interpretability. This can make it difficult to understand how decisions are made and identify potential vulnerabilities or biases within the system (Loukas 2019). Lack of explainability may hinder the detection of security issues or make it challenging to address them effectively (Kavallieratos *et al.* 2020b).
- **Limited Adaptability to New Threats:** Martelli *et al.* state that AI and ML systems rely on historical data for training and decision-making. If new cyber security threats emerge that were not encountered during the training phase, AI and ML systems may struggle to adapt quickly and effectively. This adaptability limitation can leave autonomous ships vulnerable to emerging threats, as the AI models may not possess the necessary knowledge or patterns to recognise and respond to novel attacks (Martelli *et al.* 2020).
- **Overreliance on Training Data:** Meland *et al.* advise that AI and ML systems heavily rely on the quality and representativeness of the training data. If the training data fails to capture all relevant scenarios, including potential cyber security threats, the system may not be adequately prepared to handle real-world attacks (Meland *et al.* 2021). Limited or biased training data may result in false positives or false negatives, compromising the effectiveness of the system's security measures (McGillivray 2018).
- **Complexity and Opacity:** AI and ML systems can be complex, comprising multiple interconnected components and algorithms

(Martelli *et al.* 2021). This complexity makes it challenging to fully assess and understand the system's overall security posture (Onishchenko *et al.* 2022). Pitropakis *et al.* state that the opacity of some AI models can hinder security audits, vulnerability assessments and the identification of potential weaknesses or attack vectors (Pitropakis *et al.* 2020).

Several principles have been proposed to secure maritime autonomous systems and defend against cyber attacks (Walter *et al.* 2023). These include enforcing strong cybersecurity, conducting risk assessments before development, and making the AI models themselves more robust. The principles also highlight the need for developers to understand how the AI system works while limiting this knowledge for untrusted users, as well as controlling the data feeding the model and coming out of it. Finally, using multiple sensors can make it harder to attack multi-agent systems (MAS AI). Furthermore, possible countermeasures which could be used to implement the principles noted above. These countermeasures include adversarial training, which is a technique to improve the robustness of AI models against adversarial attacks. It involves creating adversarial examples (tricky inputs designed to fool the model) and using them to train the model, making it better at recognising and rejecting such attacks. The document discusses various methods for adversarial training, including generating adversarial samples and using null labels to detect them. It also acknowledges the limitations of these methods, like the difficulty of searching the entire data space for attacks.

5.1.3. Collision avoidance systems

A third survivability feature that consistently appeared in literature searches is Collision Avoidance Systems. Qiao *et al.* state that autonomous ships leverage advanced collision avoidance systems that utilise sensor data and AI algorithms to detect and predict potential collisions (Qiao *et al.* 2020). Schinas *et al.* state that these systems



Figure 3. Collision avoidance system.

enable the vessel to take proactive measures, such as adjusting course or speed, to avoid accidents and ensure survivability (Schinas and Metzger 2023).

Collision avoidance systems play a crucial role in ensuring the safety of autonomous ships. However, there are some negatives to consider:

- **Vulnerability to Sensor Manipulation:** Sepehri *et al.* advise that collision avoidance systems rely heavily on sensor data to detect and respond to potential collision risks. If these sensors are compromised or manipulated by cyber attackers, it can result in false or misleading data being fed into the collision avoidance system. This can lead to incorrect decisions or failure to detect actual collision risks, jeopardising the safety of the ship and its surroundings (Sepehri *et al.* 2022).
- **Sensor Spoofing Attacks:** Serru *et al.* state that cyber attackers may attempt to spoof or deceive the collision avoidance system by manipulating sensor readings. By sending false signals or intentionally distorting sensor data, they can trick the system into perceiving non-existent obstacles or failing to identify actual hazards (Serru *et al.* 2023). This could result in improper course adjustments or failure to take appropriate evasive actions when needed (Kavallieratos *et al.* 2021).
- **Communication Interference:** Shapo *et al.* advise that collision avoidance systems often rely on external communication networks to exchange information with other ships, shore-based stations, or satellite systems. Cyber attackers could target these communication channels, causing interference or disruption. Such interference could lead to delays or loss of critical collision avoidance information, potentially increasing the risk of accidents or collisions (Shapo and Levinskyi 2021).
- **General Cybersecurity Vulnerabilities:** Amro *et al.* state that vulnerabilities such as weak encryption protocols, inadequate access controls, or outdated software can provide opportunities for unauthorised access or manipulation of the system. Exploiting these vulnerabilities can compromise the integrity and functionality of the collision avoidance system (depicted in Figure 3) (Amro and Gkioulos 2023). Ahmed *et al.* express that the lack of standardised cybersecurity protocols and regulations specific to collision avoidance systems in autonomous ships can be a challenge. Varying implementation practices across different manufacturers or ship operators may result in inconsistencies and potential security gaps. Without clear industry standards, it becomes more challenging to ensure that robust cybersecurity measures are uniformly adopted and maintained across the board (Ahmed and Gkioulos 2022). Below is a figure depicting a collision avoidance system.

5.1.4. Redundancy and fault-tolerant systems

Redundancy and Fault-Tolerant Systems are a fourth feature of autonomous ship survivability. Shipunov *et al.* state that to enhance survivability, autonomous ships often incorporate redundancy and

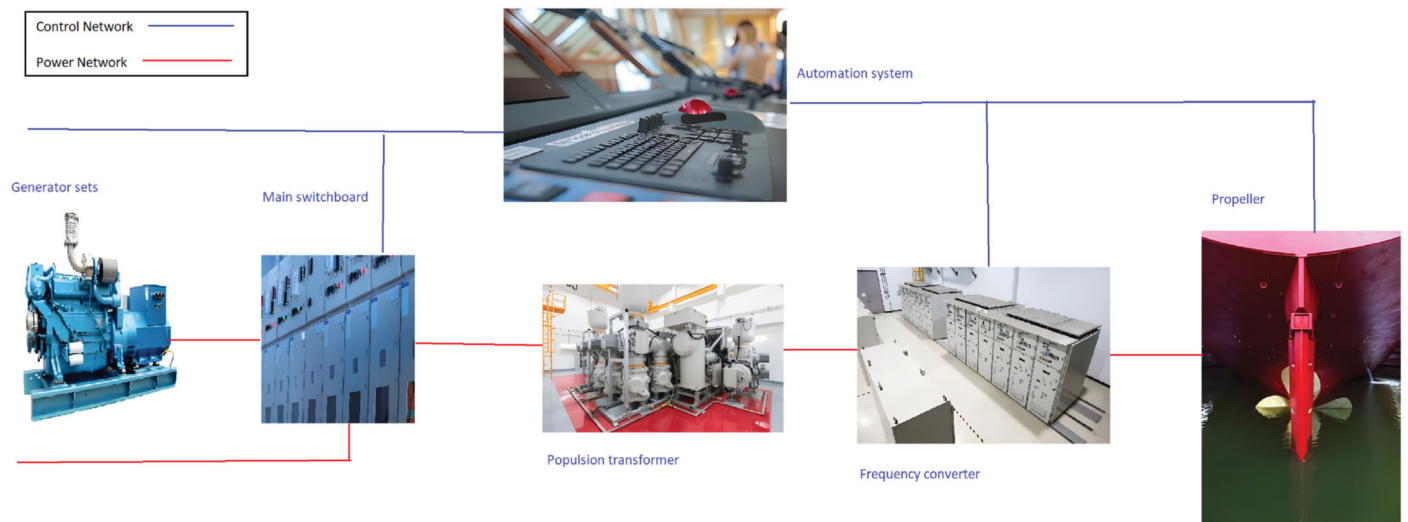


Figure 4. Fault tolerant, reconfigurable grid for a propulsion system (ABB Oy, Marine and Cranes 2022 – URL: https://library.e.abb.com/public/6c1b0250efd18e73c1257a530040dcf2/XO2100_XO2300_Product_Intro_lowres.pdf).

fault-tolerant systems. This involves duplicating critical components such as power systems (Shipunov et al. 2019). Redundancy and fault-tolerant systems are critical for ensuring the reliability and safety of autonomous ships. However, there are some issues to consider:

Increased Attack Surface: redundancy and fault-tolerant systems often involve multiple interconnected components and backups (Amro et al. 2020). Silva *et al.* state that while this redundancy helps mitigate failures and ensure system availability, it also increases the attack surface. Each additional component or backup introduces a potential entry point for cyber attackers to exploit, making the system more susceptible to unauthorised access or manipulation (Silva et al. 2022).

Complexity and Configuration Challenges: Silverajan *et al.* advise that redundancy and fault-tolerant systems can be complex, requiring meticulous configuration and integration (Silverajan et al. 2018). Tam *et al.* state that the more components and backups involved, the more intricate and challenging it becomes to ensure that all aspects are properly secured. Complexity can lead to misconfigurations or overlooked vulnerabilities, inadvertently creating weak points that cyber attackers could exploit (Tam and Jones 2018).

Maintenance and Patching Difficulties: redundancy and fault-tolerant systems often require continuous monitoring and maintenance to ensure optimal performance and security (Ben Farah et al. 2023). Jung *et al.* state that applying updates, patches and security fixes to interconnected components and backups can be more challenging than for a single, standalone system (Jung et al. 2022b). Failure to promptly address vulnerabilities in all redundant components increases the risk of cyber-attacks targeting those specific weaknesses (Titov et al. 2019).

Synchronisation and Consistency: maintaining synchronisation and consistency among redundant components can pose challenges in terms of cyber security (Ahmed and Gkioulos 2022). Any discrepancies or inconsistencies in the configuration or behaviour of redundant systems can create vulnerabilities that can be exploited by cyber attackers (Amro et al. 2023). Titov *et al.* advise that ensuring that all redundant components remain up to date, properly configured, and secure can be a complex task that requires careful monitoring and management (Titov et al. 2019).

Insider Threats and Malicious Insiders: redundancy and fault-tolerant systems may require privileged access to manage and configure the different components (Amro et al. 2022). This can introduce

the risk of insider threats, where authorised individuals with elevated privileges may misuse their access for malicious purposes (Anatoliy et al. 2018). Tusher *et al.* state malicious insiders could potentially compromise or manipulate redundant systems, bypass security measures, or introduce vulnerabilities that are difficult to detect (Tusher et al. 2022). To give the reader a better understanding of a fault tolerant system, one is depicted below in Figure 4.

5.1.5. Overview table of the technologies available for autonomous ship survivability

Table 1 gives an overview of the techniques described in section 5.1. The overview table, for the reader's convenience, gives a summary of each technique, and the positives and negatives of each technique.

5.2. Technology available to combat the shortcomings of the above features

The above four features used by autonomous vessels all have significant disadvantages concerning cyber security threats. However, there are software and hardware systems available to combat some of the shortcomings. Below literature related to the systems available to combat the cyber security threats detailed previously is investigated.

5.2.1. Intrusion detection systems

Intrusion Detection Systems (IDS) can monitor network traffic and identify any abnormal activities or potential cyber threats (Pitropakis et al. 2020). An intrusion detection system (IDS) on an autonomous ship has several positives. Firstly, it enhances the overall security of the ship by detecting and alerting any unauthorised access attempts or suspicious activities, allowing for timely response and prevention of potential threats. This helps protect the ship's valuable assets and sensitive information (Anatoliy et al. 2018). Secondly, an IDS can help ensure the safety of passengers and crew members by continuously monitoring the ship's network and systems for any anomalies or potential breaches (Ahmed and Gkioulos 2022). Vagale *et al.* state that quickly identifying and addressing security risks, helps maintain a secure environment onboard (Vagale 2022). Moreover, Yoo *et al.* state that an IDS plays a crucial role in maintaining the integrity of the ship's systems and preventing disruptions to its operations. By proactively identifying and mitigating any malicious activities, it helps minimise downtime, reduce maintenance costs and ensure

Table 1. Overview table of technologies.

Technology	Description	Positives	Negatives
Sensor Systems	Radars, LiDARs, cameras and sonars used to perceive the surroundings	<ul style="list-style-type: none"> • Gather real-time data for navigation 	<ul style="list-style-type: none"> • Vulnerable to cyber attacks (unauthorised access, data breaches, manipulation) • Susceptible to sensor spoofing (fake data) • Vulnerable to denial-of-service attacks • Inconsistent security implementations across manufacturers • Challenges in updating and patching vulnerabilities
AI and Machine Learning	Process sensor data, make decisions, adapt to situations	<ul style="list-style-type: none"> • Identify hazards, interpret data, make real-time adjustments 	<ul style="list-style-type: none"> • Vulnerable to adversarial attacks (deception, exploitation) • Susceptible to data poisoning (compromised training data) • Lack of transparency in decision-making. • Limited adaptability to new threats • Overreliance on training data quality • Complexity hinders security assessment
Collision Avoidance Systems	Use sensor data and AI to detect and avoid collisions	<ul style="list-style-type: none"> • Proactive measures to ensure safety 	<ul style="list-style-type: none"> • Vulnerable to sensor manipulation (providing false data) • Susceptible to sensor spoofing (fake obstacles) • Vulnerable to communication interference • General cybersecurity weaknesses (encryption, access control)
Redundancy and Fault-Tolerant Systems	Duplication of critical components for reliability	<ul style="list-style-type: none"> • Mitigate failures, ensure system availability 	<ul style="list-style-type: none"> • Lack of standardised cybersecurity protocols • Increased attack surface (more entry points for attackers) • Complexity in configuration and integration • Challenges in maintenance and patching • Difficulties in synchronisation and consistency • Risk of insider threats

smooth and uninterrupted voyages (Yoo and Park 2021). In addition, an IDS can provide valuable insights and data about potential vulnerabilities or attack patterns, enabling the ship's operators to strengthen the ship's security infrastructure and implement necessary measures to prevent future incidents (Ben Farah et al. 2023). While IDSs on autonomous ships offer numerous benefits, it is important to consider some potential drawbacks as well such as:

- **False Positives:** Zhou *et al.* raise the issue that IDS systems can occasionally generate false positive alerts, flagging normal network activities as suspicious or malicious. These false alarms can lead to unnecessary disruptions or distractions for the ship's crew, diverting their attention from other critical tasks (Zhou et al. 2018).
- **Performance Impact:** implementing an IDS requires computational resources to continuously monitor and analyse network traffic (Bolbot et al. 2020). Zhou *et al.* state that depending on the system's design and implementation, it can potentially impact the ship's overall performance, including network latency or processing speed. Striking the right balance between security and performance is crucial (Zhou et al. 2021).
- **Complexity and Maintenance:** IDS systems typically involve complex configurations and require ongoing maintenance and updates to stay effective against evolving threats (Yoo and Park 2021). Alop *et al.*, in a discussion, state that this can place additional burdens on the ship's IT team, necessitating specialised knowledge and resources to manage and keep the IDS up to date (Alop 2019).
- **Cost Considerations:** Boudehenn *et al.* state that IDS can involve significant upfront costs, including hardware, software, and implementation expenses. Additionally, ongoing licence fees and maintenance costs can be a part of the long-term investment. Balancing the cost of implementing an IDS with the perceived security benefits is an important consideration for ship operators (Boudehenn et al. 2023). Chang *et al.* advise that it is crucial to evaluate the potential Return On Investment (ROI) in terms of improved security and risk reduction. Conducting a cost-benefit analysis can help determine whether the benefits of implementing an IDS outweigh the associated costs (Chang et al. 2021). Furthermore, the cost of training personnel to effectively operate and maintain the IDS should be considered (Vagale et al. 2021b). Adequate training and expertise are essential for maximising the

system's potential and ensuring its optimal performance (Ahmed and Gkioulos 2022).

Lastly, it is worth considering that the effectiveness of an IDS relies on its ability to keep up with emerging threats (Amro et al. 2023). As new attack techniques and vulnerabilities emerge, regular updates and patches are necessary to maintain the system's efficacy (Amro et al. 2022). Vagale *et al.* state that these ongoing licence fees and maintenance costs should be factored into the overall cost considerations (Vagale et al. 2021a). Figure 5 depicts a Serial Guard intrusion detection system.

5.2.2. Secure communication protocols

Secure Communication Protocols: encryption technology can be implemented to secure data transmission between various onboard systems and shore-side control centres (Bolbot et al. 2020). Secure communication protocols on an autonomous ship offer numerous positives. The main positives will be evaluated from the literature referenced below:

Data Confidentiality: Zhou *et al.* state that secure communication protocols employ encryption techniques to protect the confidentiality of sensitive data transmitted over networks. This ensures that critical information, such as navigational data, control commands, or passenger details, remains confidential and cannot be intercepted or accessed by unauthorised entities (Zhou et al. 2021).

Data Integrity: secure protocols use mechanisms like checksums and digital signatures to verify the integrity of transmitted data (Ahvenjarvi et al. 2019). Amro *et al.* state that this prevents unauthorised modification or tampering during transit, ensuring that the information received is accurate, reliable and unaltered (Amro and Gkioulos 2023).

Authentication: secure communication protocols facilitate strong authentication mechanisms to verify the identity of communicating entities (Amro and Gkioulos 2023). Badki *et al.* state that this helps prevent unauthorised access and protects against spoofing or impersonation attacks. By validating the identities of devices, systems and users, secure protocols ensure that only trusted entities can participate in communication (Bolbot et al. 2023).

Mitigation of Cyber Threats: Epikhin *et al.* advise that with the increasing sophistication of cyber threats, secure communication protocols play a vital role in mitigating these risks (Epikhin and Modina 2021). By employing robust security measures like encryption,

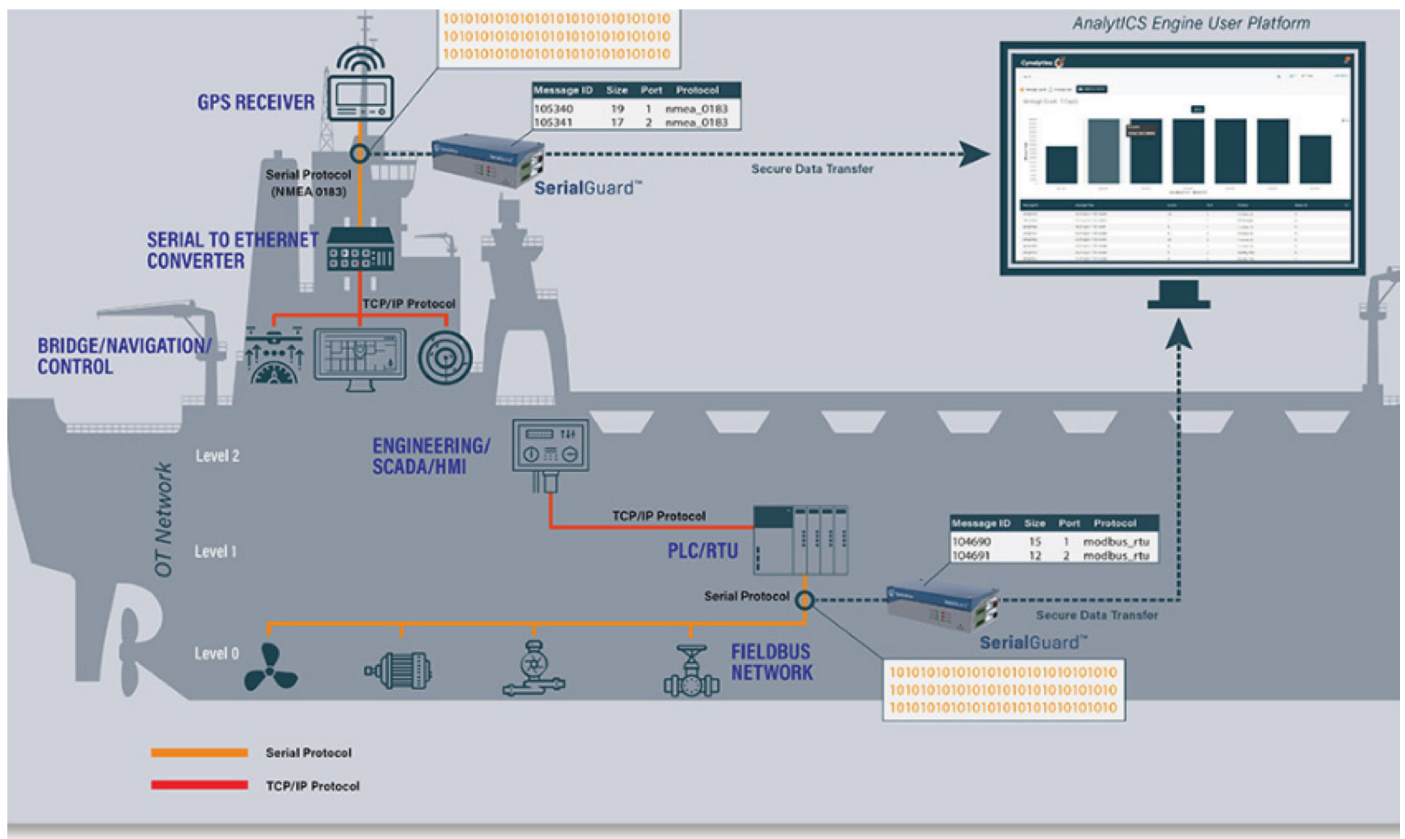


Figure 5. Serial Guard intrusion detection system (Cynalytica 2024).

message authentication and secure key exchange, they help safeguard against eavesdropping, data breaches and unauthorised access attempts (Alop 2019).

Compliance with Regulations: implementing secure communication protocols ensures compliance with industry regulations and standards (Fang et al. 2022). In the maritime sector, there are specific regulations and guidelines, such as the International Maritime Organization's (IMO) Guidelines on Cyber Risk Management, that mandate the implementation of robust security measures, including secure communication protocols (Qiu et al. 2021).

Trust and Reputation: secure communication protocols can significantly enhance the trustworthiness and reputation of an autonomous ship operator (Kardakova et al. 2020). When customers, stakeholders and partners know that their data and communications are protected by strong security measures, they gain confidence in the ship's operations and are more likely to trust and engage with the operator (Vagale et al. 2021b). This can lead to improved business relationships, customer satisfaction and market competitiveness (Hopcraft et al. 2023).

While secure communication protocols offer significant advantages, it is important to consider some potential disadvantages. A few negative aspects are given below:

Complexity: Yoo et al. state that implementing and managing secure communication protocols can be complex and require technical expertise (Yoo and Jo 2023). Proper configuration, key management and ongoing maintenance of the protocols may pose challenges for ship operators, especially those without extensive cybersecurity knowledge (Anatoliy et al. 2018). It may necessitate additional resources, personnel and training to ensure that the protocols are correctly implemented and maintained (Vagale 2022).

Performance Impact: secure communication protocols often introduce additional computational overhead due to encryption, decryption and authentication processes (Ahmed and Gkioulos 2022). Amro et al. advise that this can lead to increased latency and reduced network performance (Amro et al. 2020), especially in scenarios where real-time communication is crucial (Anatoliy et al. 2018), such as navigation or control systems (Alop 2019). Striking the right balance between security and performance becomes a critical consideration (Kavallieratos et al. 2020b).

Compatibility and Interoperability: Tusher et al. state that secure protocols may require specific hardware or software implementations (Tusher et al. 2022), which can lead to compatibility issues with existing systems or devices on the autonomous ship (Tam and Jones 2018). Integrating different protocols and ensuring seamless interoperability among various systems can be challenging, potentially requiring additional investments in hardware or software upgrades (Amro and Gkioulos 2023).

User Experience: depending on the level of security implemented, secure communication protocols can introduce additional steps or authentication measures that may negatively impact the user experience (Anatoliy et al. 2018). This can create inconvenience or frustration for users who are accustomed to a more seamless and effortless communication process (Serru et al. 2023). Meland et al. state that complex authentication procedures, such as multiple layers of verification or frequent password changes, can slow down user interactions and potentially lead to user errors or forgotten credentials (Meland et al. 2021).

Cost Considerations: implementing and maintaining secure communication protocols can involve additional costs. This includes investing in security hardware, software licences, regular updates, and ongoing monitoring and maintenance. These expenses can add

up, especially for smaller ship operators with limited budgets, and may require careful financial planning (Issa et al. 2022).

Potential False Sense of Security: while secure communication protocols significantly improve the security posture of an autonomous ship (Kavallieratos et al. 2021), it is important to remember that no security measure is foolproof (Li and Yu 2020). Jung *et al.* state that operators and users should not solely rely on these protocols and must remain vigilant against emerging threats, social engineering attacks, or other vulnerabilities that these protocols may not address (Jung et al. 2022b).

5.2.3. Access control systems

Access Control Systems: these systems help regulate and control access to critical ship systems, ensuring only authorised personnel can make changes or access sensitive data (Schinas and Metzger 2023). Access control systems on an autonomous vessel offer several positives as outlined below:

Enhanced Security: access control systems provide a robust layer of security by regulating and restricting access to different areas of the ship (Amro and Gkioulos 2023). By implementing authentication mechanisms such as key cards (Anatoliy et al. 2018), biometrics (Amro et al. 2022), or PIN codes (Alop 2019), these systems ensure that only authorised personnel can enter specific zones (Anatoliy et al. 2018). Ahmed *et al.* state that this helps prevent unauthorised individuals from gaining access to sensitive areas or critical systems, thereby enhancing overall security (Ahmed and Gkioulos 2022).

Safety and Emergency Response: access control systems play a vital role in ensuring the safety of passengers and crew members (Ahmed and Gkioulos 2022). By controlling access to areas such as emergency exits, lifeboats, or safety equipment storage, these systems help prevent unauthorised interference or misuse during emergency situations (Dittman et al. 2021). They also enable efficient emergency response by providing accurate information on the location and status of individuals within the ship (Kavallieratos et al. 2020b).

Theft and Loss Prevention: access control systems help deter theft and prevent loss of valuable assets onboard (Kavallieratos et al. 2020a). By restricting entry to areas where valuable equipment or supplies are stored, these systems act as a deterrent to potential thieves. Additionally, access logs generated by the system can aid in investigations should any theft or loss occur, assisting in identifying potential culprits (Schinas and Metzger 2023).

Accountability and Auditability: Chiu *et al.* state that access control systems provide a means to establish accountability and ensure auditability (Chiu et al. 2011). By logging and recording access events, these systems create a trail of who has accessed specific areas and when. This enables ship operators to track and monitor the movement of personnel, ensuring compliance with safety protocols and regulations (Alop 2019). Loukas *et al.* state that, in the event of an incident or breach, access control logs can serve as valuable evidence for investigations and audits, helping to identify the responsible individuals and take appropriate actions (Loukas 2019).

Customisation and Flexibility: access control systems offer the flexibility to customise access privileges based on roles and responsibilities (Onishchenko et al. 2022). This allows ship operators to define and enforce access policies tailored to their specific needs. Different levels of access can be granted to crew members, passengers, maintenance personnel, or other authorised individuals, ensuring that everyone has access to the necessary areas while maintaining appropriate restrictions (Amro and Gkioulos 2023).

Integration with Other Systems: access control systems can be integrated with other ship systems, such as surveillance cameras or alarm systems (Alop 2019). Ahmed *et al.* advise that this integration allows for a more comprehensive security infrastructure, where access events can trigger corresponding actions, such as capturing

video footage or raising alerts in case of unauthorised access attempts or suspicious activities (Ahmed and Gkioulos 2022). Such integration enhances overall situational awareness and response capabilities (Anatoliy et al. 2018). While access control systems on an autonomous ship offer numerous benefits, it is important to consider potential negatives as well. Here are some aspects to evaluate:

Implementation Complexity: implementing access control systems can be complex, especially on a large-scale autonomous ship with multiple access points. It requires careful planning, installation of hardware and software, and system integration. The complexity of implementation may increase costs and require specialised expertise (Amro et al. 2022).

User Convenience and Productivity: access control systems can introduce additional steps and authentication measures, which may inconvenience users and impact productivity (Ahvenjarvi et al. 2019). Crew members or passengers may need to present credentials, such as key cards or undergo biometric scans, slowing down access to areas or systems. Balancing security with user convenience is crucial to maintaining a positive experience (Bolbot et al. 2020).

System Malfunctions and Downtime: Fang *et al.* state that, like any technology, access control systems can experience malfunctions or downtime. Hardware failures, software glitches, or power outages can disrupt the system's operation and potentially lead to access issues or delays (Fang et al. 2022). Robust backup plans and regular maintenance are necessary to minimise the impact of such incidents (Liou 2011).

False Sense of Security: Silva *et al.* state that while access control systems significantly enhance security, they should not be viewed as the sole solution (Silva et al. 2022). Martelli *et al.* advise that users may develop a false sense of security, assuming that unauthorised access is impossible (Martelli et al. 2021). It is important to remember that determined individuals or sophisticated attackers may find ways to bypass or circumvent access control measures (Ahmed and Gkioulos 2022). This highlights the importance of maintaining a comprehensive security posture that includes other layers of protection, such as intrusion detection systems, surveillance cameras, and ongoing security awareness training for personnel (Pitropakis et al. 2020).

Cost Considerations: implementing access control systems involves upfront costs for hardware, software, installation and ongoing maintenance. Additionally, there may be costs associated with training personnel on how to effectively use the system and manage access permissions (Kardakova et al. 2020). Smaller ship operators with limited budgets may need to carefully evaluate the cost-benefit ratio of implementing such systems (Schinas and Metzger 2023).

System Complexity and Integration: integrating access control systems with other ship systems, such as surveillance cameras or alarm systems, may require additional effort and compatibility considerations. Ensuring seamless integration and avoiding potential conflicts or interoperability issues can be a challenge, requiring technical expertise and careful planning (Alop 2019).

5.2.4. Behavioural analytics

Behavioural Analytics: by analysing patterns and behaviours, AI algorithms can detect anomalies and suspicious activities, providing an early warning system against cyber-attacks (Shipunov et al. 2019). Using behavioural analytics on an autonomous ship can bring several positives when it comes to cyber security such as:

- **Intrusion Detection:** behavioural analytics helps in identifying abnormal patterns of behaviour, enabling the system to detect potential cyber threats or intrusions. This proactive approach can prevent cyberattacks before they cause significant damage (Li and Yu 2020).

- **Anomaly Identification:** Liou *et al.* state that by analysing the behaviour of the ship's systems, behavioural analytics can quickly identify unusual or suspicious activities that may indicate a cyber-attack (Liou 2011). This allows for immediate action to be taken to mitigate the threat (Issa *et al.* 2022).
- **Real-time Monitoring:** Park *et al.* state that behavioural analytics provides continuous monitoring and analysis of the ship's systems, allowing for real-time detection of any abnormal behaviour (Park and Kontovas 2023). This enables the crew to respond swiftly to any potential cyber threat and take appropriate measures (Qiao *et al.* 2020).
- **Predictive Analysis:** behavioural analytics can also help in predicting potential cyber threats by analysing historical data and patterns (Alop 2019). This proactive approach allows for preemptive measures to be taken to prevent cyber-attacks, keeping the ship and its systems secure (Amro and Gkioulos 2023).
- **User Behaviour Analysis:** Anatioly *et al.* state that by analysing the behaviour of the ship's crew members or authorised users, behavioural analytics can flag any suspicious or unauthorised activities (Anatoliy *et al.* 2018). This helps in ensuring that only authorised individuals have access to critical systems, minimising the risk of cyber-attacks (Ahmed and Gkioulos 2022).

While behavioural analytics on an autonomous ship offers several benefits for cyber security, it is important to consider potential drawbacks as well. Here are a few negatives to keep in mind:

- **False Positives:** Pitropakis *et al.* state that behavioural analytics may generate false positive alerts, flagging normal behaviour as suspicious or unauthorised (Pitropakis *et al.* 2020). Amro *et al.* state that this can lead to unnecessary interventions or disruptions, potentially impacting the ship's operations and causing inconvenience for the crew members (Amro *et al.* 2020).
- **Privacy Concerns:** Serru *et al.* state that implementing behavioural analytics requires collecting and analysing data related to crew members' behaviour (Serru *et al.* 2023). This raises privacy concerns, as individuals may feel their actions are constantly being monitored or scrutinised. It is crucial to establish clear policies and safeguards to protect the privacy of crew members while balancing the need for security (Amro *et al.* 2023).
- **Resource Intensive:** behavioural analytics relies on advanced technology and algorithms, which may require substantial computational power and resources. Implementing and maintaining the necessary infrastructure can be costly and may require ongoing investments in hardware, software, and skilled personnel (Anatoliy *et al.* 2018).
- **Adaptive Threats:** cyber threats are constantly evolving, and attackers may modify their behaviour to bypass behavioural analytics systems. This means that behavioural analytics must continuously adapt and update to stay effective against emerging threats, requiring regular maintenance and updates (Greiman 2019).
- **Overdependence:** Li *et al.* state that relying solely on behavioural analytics may create a false sense of security. While behavioural analytics is a powerful tool, it should not be the sole defence mechanism against cyber threats (Li and Yu 2020). Overdependence on any single security measure can leave the autonomous ship vulnerable to attacks that may bypass or evade behavioural analytics systems (Ahvenjarvi *et al.* 2019).

5.2.5. Cybersecurity training and awareness

Educating the crew and personnel about best practices for cybersecurity is crucial in terms of cybersecurity training and awareness.

Regular training sessions can help prevent accidental breaches and improve overall cyber resilience (Alop 2019). Cyber security training and awareness on an autonomous ship offer several positives when it comes to enhancing cyber security. The following are among the key benefits:

- **Threat Recognition:** Amro *et al.* state that training and awareness programmes educate crew members about various cyber threats, such as phishing, social engineering, or malware attacks. This empowers them to recognise and report suspicious activities promptly, reducing the risk of successful cyber-attacks (Amro *et al.* 2022).
- **Best Practices:** Anatoliy *et al.* state that, training equips crew members with knowledge of cyber security best practices, such as strong password management, regular software updates and safe browsing habits (Anatoliy *et al.* 2018). By following these practices, they can mitigate potential vulnerabilities and contribute to a more secure ship environment (Amro *et al.* 2023).
- **Incident Response:** cyber security training prepares crew members to respond effectively to cyber incidents (Tam and Jones 2018). They learn how to identify and contain threats, report incidents to the appropriate authorities, and initiate appropriate recovery procedures (Ahvenjarvi *et al.* 2019). This ensures a coordinated and efficient response to minimise the impact of cyber-attacks (Zhou *et al.* 2018).
- **Secure Behaviour:** training and awareness programmes encourage responsible behaviour and cultivate a cyber security-conscious culture on the ship. Crew members become more conscious of their actions, such as avoiding risky online activities or connecting unauthorised devices to critical systems. This reduces the likelihood of unintentional security breaches (Zhou *et al.* 2021).
- **Compliance and Regulations:** by providing cyber security training, the autonomous ship can demonstrate its commitment to compliance and adherence to industry regulations (Ahmed and Gkioulos 2022). Many regulatory frameworks, such as the International Maritime Organization's (IMO) Guidelines on Maritime Cyber Risk Management, emphasise the importance of cyber security training (Ahmed and Gkioulos 2022). By ensuring that crew members are well-versed in cyber security protocols, the ship can demonstrate its dedication to meeting these requirements (Amro *et al.* 2020).
- **Risk Reduction:** cyber security training plays a vital role in reducing overall cyber risk (Pitropakis *et al.* 2020). Shapo *et al.* state that by equipping crew members with the knowledge and skills to identify and respond to potential cyber threats, the ship can significantly decrease the likelihood of successful attacks. This proactive approach helps safeguard critical systems, data and operations (Shapo and Levinskyi 2021).
- **Knowledge Sharing:** cyber security training fosters a collaborative environment where crew members can openly discuss and share their experiences, insights and concerns regarding cyber security. This facilitates the exchange of valuable information and promotes ongoing learning, enabling the ship to stay updated on emerging threats and countermeasures (Ahmed and Gkioulos 2022).
- **Continuous Improvement:** training and awareness programmes can be regularly updated to reflect the evolving cyber threat landscape. By staying current with the latest trends and tactics used by cyber criminals, the ship can adapt its training modules to address new vulnerabilities and ensure that crew members are well-prepared to handle emerging risks (Ahvenjarvi *et al.* 2019). While cyber security training and awareness on an autonomous

ship have numerous benefits, it is important to consider potential negatives as well. Here are a few:

- **Human Error:** despite training, human error can still occur (Amro et al. 2022). Amro *et al.* state that crew members may unintentionally make mistakes or overlook security protocols, potentially leading to security breaches. Training alone cannot eliminate the risk of human error completely (Amro and Gkioulos 2023).
- **Resource Constraints:** implementing comprehensive cyber security training programmes requires time, effort, and resources. Autonomous ships may face challenges in allocating sufficient resources for regular training sessions, especially if they have a large and rotating crew. Additionally, conducting effective training may require specialised personnel or external experts, adding to the cost and logistical complexities (Martelli et al. 2021).
- **Training Effectiveness:** the effectiveness of training programmes relies on factors such as the quality of the curriculum, delivery methods and engagement of participants. Inadequate or ineffective training can result in a false sense of security, where crew members may not fully grasp the seriousness of cyber threats and fail to apply the training effectively in practice (Schinas and Metzger 2023).
- **Changing Threat Landscape:** Jung *et al.* state, that cyber threats evolve rapidly, and training programmes must keep pace with these changes. Outdated or insufficiently comprehensive training materials may not adequately prepare crew members to recognise and respond to emerging threats (Jung et al. 2022b). Regular updates and ongoing education are essential to ensure that cyber security training remains effective. However, maintaining up-to-date training materials and delivering regular updates can be challenging, especially in an ever-changing threat landscape (Ahvenjarvi et al. 2019). Ahmed *et al.* state that failure to provide timely and relevant training can undermine the effectiveness of the programme and leave crew members ill-prepared to address new and sophisticated cyber threats (Ahmed and Gkioulos 2022).
- **Resistance to Change:** some crew members may resist or be less receptive to cyber security training, perceiving it as an additional burden or disruption to their routine duties (Ahvenjarvi et al. 2019). This resistance can undermine the effectiveness of the training programme and hinder the development of a strong security culture on the ship (Amro et al. 2020).
- **Limited Skill Sets:** not all crew members may have a technical background or extensive knowledge of cyber security (Alop 2019). Tailoring training programmes to accommodate crew members with varying skill sets and providing accessible and understandable content can be a challenge. Ensuring that the training material is relevant and accessible to all crew members is essential for comprehensive cyber security awareness (Issa et al. 2022).

There are security concerns surrounding remote operation centres (ROC). These centres play a crucial role in the higher levels of maritime autonomy. The research in (Palbar Misas et al. 2024) explores cybersecurity challenges for ROCs managing increasingly autonomous ships. As these vessels rely heavily on digital systems and data exchange, ROCs become prime targets for cyberattacks. Data breaches, communication disruptions and manipulated sensor data all pose safety risks and threaten intellectual property. Concerns are also raised about reduced situational awareness for ROC personnel compared to traditional crews, potentially hindering their ability to respond to cyber incidents effectively (Palbar Misas et al. 2024). The rise of autonomous ships brings cybersecurity challenges to ROCs. As previously stated, data breaches, communication disruptions and manipulated sensor data from cyberattacks can cripple these centres. Palbar Misas et al state that to address this, it is

necessary to have robust cybersecurity measures, data minimisation, secure communication channels, system redundancy and cybersecurity training for ROC personnel (Palbar Misas et al. 2024). Additionally, advanced sensor technology, cyber-resilient sensor systems and international regulations can bolster situational awareness and overall security. Finally, cyber insurance and international collaboration can further mitigate risks and build trust in this developing field.

5.2.6. Overview table of the techniques to ensure autonomous ship survivability

Table 2 depicts an overview of the techniques described in section 5.2. The techniques, along with the positives and negatives of each are summarised for the readers' convenience.

5.3. Autonomous ship systems vulnerable to cyber attacks

Based on the findings above, this section will be used to demonstrate the systems that autonomous ships consist of that are vulnerable to cyber attacks. Figure 6 depicts the system locations on differing types of autonomous vessels, how they are interconnected and how they can be intruded.

While MASS vessels introduce new complexities due to their autonomous nature, they also share many vulnerabilities with traditional container ships. This is primarily due to the similarities in their underlying infrastructure and systems.

Ship Network:

Cybersecurity breaches: Both types of vessels rely on networks to connect various systems onboard. This creates potential entry points for cyberattacks, such as malware, ransomware and unauthorised access.

Network vulnerabilities: Weak passwords, outdated software and unpatched systems can expose both ship types to cyber threats.

Navigation Systems:

GPS spoofing: Both traditional and MASS vessels can be vulnerable to GPS spoofing, which can lead to navigation errors and collisions.

Sensor failures: Malfunctions in radar, sonar, or other navigation sensors can impact the safety of both types of vessels.

Communication Systems:

Interception: Communications between ships and shore-based facilities can be intercepted, leading to information leakage or manipulation.

Jamming: Communication systems can be jammed, disrupting operations and potentially causing safety hazards.

Crew Network (for traditional ships):

Human error: Crew members can introduce vulnerabilities through mistakes, negligence, or unauthorised actions.

Social engineering: Cyberattacks targeting crew members through phishing or other social engineering tactics can compromise ship security.

Network Backbone:

Infrastructure failures: Both types of vessels rely on robust network infrastructure, which is susceptible to failures due to hardware malfunctions, software bugs, or natural disasters.

Cyberattacks: The network backbone can be a target for DDoS attacks or other cyber threats, disrupting operations.

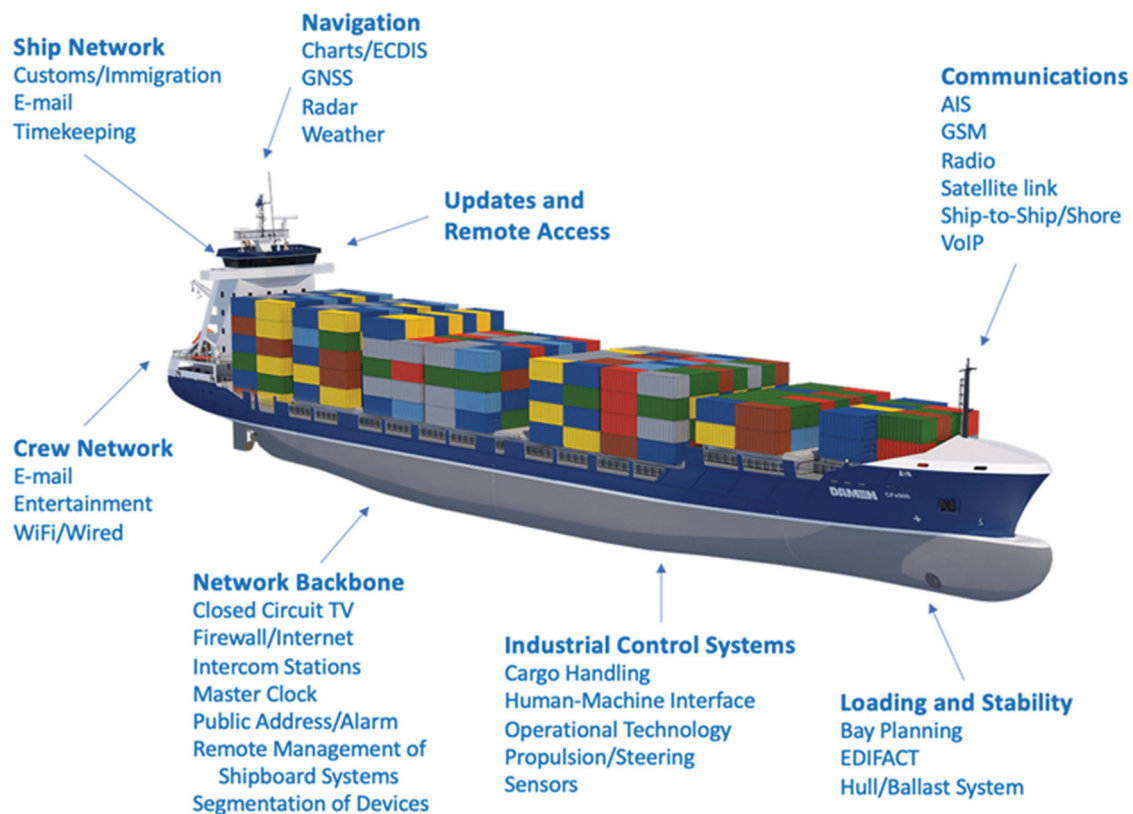
Industrial Control Systems (ICS):

Cybersecurity risks: ICS systems, which control critical ship functions, are vulnerable to cyberattacks that could lead to equipment damage or safety hazards.

Remote access vulnerabilities: Remote access to ICS systems for maintenance or troubleshooting creates potential entry points for malicious actors.

Table 2. Overview table of techniques.

Technology	Positives	Negatives
Intrusion Detection Systems (IDS)	<ul style="list-style-type: none"> • Detects and alerts of unauthorised access or suspicious activities – Protects valuable assets and crew. • Provides insights for strengthening security 	<ul style="list-style-type: none"> • False positives can waste time and resources. • Performance impact • Complexity and maintenance burden.
Secure Communication Protocols	<ul style="list-style-type: none"> • Protects confidentiality of data (navigation, control commands) • Ensures data integrity (prevents modification) • Authenticates communicating entities (prevents spoofing) • Mitigates cyber threats. • Improves trust and reputation 	<ul style="list-style-type: none"> • Cost considerations (hardware, software, personnel) • Complexity in implementation and management • Performance impact (latency, network speed) • Compatibility and interoperability issues • User experience (additional steps, authentication) • Cost considerations (hardware, software, updates) • Potential false sense of security
Access Control Systems	<ul style="list-style-type: none"> • Enhances security by restricting access to critical systems. • Improves safety and emergency response. • Deters theft and prevents loss of assets. • Provides accountability and auditability. • Offers customisation and flexibility for access privileges. • Integrates with other security systems. 	<ul style="list-style-type: none"> • Implementation complexity (planning, installation) • User inconvenience and impact on productivity • System malfunctions and downtime – False sense of security • Cost considerations (hardware, software, training) • System complexity and integration challenges
Behavioural Analytics	<ul style="list-style-type: none"> • Detects intrusions and suspicious activities. • Identifies anomalies in system behaviour. • Provides real-time monitoring for threats. • Enables predictive analysis for proactive measures. • Analyses user behaviour for unauthorised activities. 	<ul style="list-style-type: none"> • False positives can disrupt operations. • Privacy concerns due to data collection • Resource intensive (computational power, skilled personnel) • Adaptive threats require continuous updates. • Overdependence can create a false sense of security
Cybersecurity Training and Awareness	<ul style="list-style-type: none"> • Educates crew on cyber threats and best practices. • Improves threat recognition and reporting. • Equips crew to respond effectively to incidents. • Encourages secure behaviour and cyber-conscious culture. • Demonstrates compliance with regulations. • Reduces overall cyber risk. • Fosters knowledge sharing and continuous improvement. 	<ul style="list-style-type: none"> • Human error can still occur. • Resource constraints (time, personnel, cost) • Training effectiveness relies on quality and engagement. • Difficulty keeping pace with evolving threats. • Resistance to change from crew. • Limited skill sets of crew members

**Figure 6.** Autonomous container ship and its vulnerable systems (Loomis et al. 2021).

5.3.1. Ship network

As shown in Figure 6 above, an autonomous ship's network can be quite complex, but typically consists of several interconnected segments:

- **Operational Technology (OT Network):** This network carries critical data for running the ship, like navigation systems, engine controls and cargo management.
- **Bridge Systems:** This network connects equipment on the bridge, like radars, communication systems and electronic charts.
- **Passenger/Crew Network:** This separate network provides internet access, email and entertainment systems for passengers and crew.
- **Administrative Network:** This network is used for business functions like payroll and inventory management.

These networks often connect to each other and sometimes to shore via satellite for remote monitoring or updates.

There are several ways cyber attackers can infiltrate a ship's network. The interconnected nature of autonomous ship networks presents a vulnerability that cyber attackers can exploit through various means. These methods can be broadly categorised into two categories: human-centric and technological.

Human-centric attacks rely on manipulating or compromising crew members. This could involve introducing malware through physical means like infected USB drives or exploiting social engineering tactics like phishing emails to trick the crew into granting unauthorised access.

Technological vulnerabilities arise from unpatched software or weak network security protocols. These gaps in a ship's digital defences can be exploited by attackers to infiltrate the system and gain control of critical functions. Furthermore, the reliance on satellite communication for remote data transmission introduces the possibility of satellite attacks, where attackers could potentially intercept or manipulate data transmissions.

As mentioned above, while traditional and MASS vessels share some similarities in their fundamental systems, the degree of complexity, reliance, and integration is significantly different.

Traditional ship networks are primarily used for internal communication, such as data exchange between equipment and systems onboard. They are often isolated from external networks. MASS ship networks are far more complex, serving as the backbone for autonomous operations. They connect various sensors, actuators, control systems and communication modules. These networks are typically integrated with shore-based control centres for remote monitoring and control. Traditional ship Communication systems primarily focus on voice communication (VHF, HF), data transfer (satellite communication) and safety systems (GMDSS). Human interaction is crucial for most communication tasks. MASS vessel communication systems are heavily reliant on data transmission, with high-speed connections to shore-based control centres. These systems enable real-time data exchange, remote control and over-the-air updates. Autonomous vessels often employ advanced communication protocols like 5G or satellite broadband for reliable connectivity. Traditional ship navigation systems rely primarily on human expertise, with electronic aids like radar, GPS, and electronic chart display systems (ECDIS) supporting decision-making. MASS vessels navigation systems are highly automated, with advanced sensors, AI, and machine learning algorithms taking over many navigational tasks. These systems can process data from multiple sources, including radar, lidar, cameras, and GPS, to create a comprehensive situational awareness picture. Autonomous vessels often employ dynamic positioning systems for precise station-keeping.

5.3.2. Ship navigation systems

Modern autonomous ships rely on a complex interplay between three key navigation systems: Electronic Chart Display and Information System (ECDIS), Global Navigation Satellite System (GNSS) and radar. These systems work in a coordinated fashion to ensure safe and efficient navigation:

- **ECDIS:** This computer-based system displays electronic navigational charts overlaid with real-time vessel position data received from GNSS. ECDIS also integrates with autopilot systems to guide the ship along a pre-programmed route.
- **GNSS:** This global positioning system utilises a network of satellites to provide highly accurate positioning data, including latitude, longitude, and time. This data feeds directly into ECDIS for course plotting and autopilot control.
- **Radar:** This sensor system emits radio waves and analyses reflections to detect and track surrounding objects like other vessels, landmasses and potential hazards. Radar data is displayed on a dedicated console or integrated with ECDIS to provide a comprehensive picture of the surrounding environment.

These systems are interconnected through a network that allows for data exchange and coordinated decision-making. Typically, GNSS data serves as the primary source of positioning information for ECDIS, which then guides the autopilot system. Radar data supplements this information by providing real-time situational awareness and enabling the autonomous ship to react to unforeseen obstacles.

Despite the technological advancements in autonomous navigation, these systems are susceptible to cyber intrusion through various methods:

- **GNSS Spoofing:** Attackers can manipulate GNSS signals, feeding the ECDIS with inaccurate positioning data. This could cause the autonomous ship to deviate from its intended course and potentially collide with other vessels or run aground.
- **ECDIS Manipulation:** Malicious actors could exploit software vulnerabilities in ECDIS to alter pre-programmed routes or disable safety features. This could lead to the autonomous ship navigating into dangerous waters or failing to respond to potential hazards detected by radar.
- **Network Intrusion:** By gaining access to the ship's internal network, attackers could disrupt communication between navigation systems, hindering their ability to function effectively. This could lead to confusion, erratic manoeuvring and potential accidents.
- **Denial-of-Service (DoS) Attacks:** Cyber attackers could overwhelm the ship's navigation systems with a flood of data, rendering them inoperable and hindering the autonomous ship's ability to navigate safely.

5.3.3. Ship communication systems

Autonomous ships rely on a complex network of communication systems to maintain operational awareness, transmit data and facilitate remote control. The following is a breakdown of the key systems and their interconnectivity:

- **Automatic Identification System (AIS):** This critical system transmits vessel identification, position, course and speed data to nearby ships and coastal authorities. It operates on a dedicated VHF frequency and does not directly connect to the ship's internal network.
- **Global System for Mobile Communications (GSM):** This cellular network provides voice and data communication capabilities

for the crew (if applicable) or shoreside personnel. GSM typically functions as a separate network onboard.

- Voice over Internet Protocol (VoIP): This technology allows for voice communication over the internet, potentially used for ship-to-shore calls or crew communication. VoIP systems might connect to the ship's internal network for internet access.
- Satellite Communication: Satellites provide a communication link beyond the range of terrestrial networks like GSM. This enables long-range data transmission for remote monitoring, mission updates, and communication with shoreside personnel. Satellites can connect directly to the ship's internal network or utilise a dedicated communication device.
- Ship-to-Ship (S2S) and Ship-to-Shore (S2S) Communication: Dedicated VHF or UHF radios facilitate direct communication between vessels or with shore stations for operational coordination, safety messages, or emergencies. These radios may interface with the ship's internal network for routing messages or logging communication.

This network of interconnected communication systems presents potential entry points for cyber attackers:

- AIS Spoofing: Malicious actors could manipulate AIS data to disguise the autonomous ship's identity, location, or course of travel. This could mislead other vessels and create a risk of collision or impede search and rescue efforts.
- Interception of Data: Attackers could exploit vulnerabilities in the ship's internal network or communication protocols to intercept sensitive data transmitted via GSM, VoIP, or satellite links. This data could include sensor readings, navigation information, or even remote control commands.
- Man-in-the-Middle Attacks: Cyber criminals could insert themselves into the communication channel between the ship and shore, potentially altering or manipulating data transmissions. This could lead to the transmission of erroneous commands or the disruption of critical communication during emergencies.
- Satellite Network Attacks: While less common, attackers with specialised capabilities could potentially target vulnerabilities in the satellite network itself to disrupt communication or intercept data transmissions.

5.4. Cyber security techniques available outside of the maritime sector

Sections 5.1 and 5.2 look specifically at the technologies and techniques with respect to the maritime sector. The technologies available to industry outside of the maritime sector will be investigated in this section. Taking a holistic approach to cyber security by looking at other fields may provide insight into techniques that could potentially be applied to autonomous vessels.

The scope of the literature review covers the current technologies available to the industry to mitigate the risk of cyber security attacks.

5.4.1. Next generation firewalls (NGFWs)

Traditional firewalls have long served as the first line of defence in securing computer networks. These perimeter security solutions operate by filtering incoming and outgoing traffic based on predefined rules and access control lists (ACLs). However, the evolving threat landscape, characterised by sophisticated malware and targeted attacks, necessitates a more comprehensive approach to network security. Next-generation firewalls (NGFWs) address this challenge by offering a significant leap in network protection capabilities (Uçtu et al. 2021).

NGFWs surpass the limitations of traditional firewalls by employing deep packet inspection (DPI) technology. This advanced technique goes beyond basic packet filtering, analysing the content within data packets to identify malicious traffic patterns, malware signatures, and other hidden threats. By dissecting the very essence of network traffic, NGFWs can detect and block sophisticated attacks that traditional firewalls might overlook (Park et al. 2022). Furthermore, NGFWs often integrate intrusion detection/prevention systems (IDS/IPS) to actively monitor network activity and identify suspicious behaviour indicative of potential intrusions.

Beyond threat detection, NGFWs offer enhanced application control functionalities. They can restrict or block specific applications or functionalities based on pre-defined security policies. This granular control over network traffic by application type significantly reduces the attack surface and hinders unauthorised access attempts. Additionally, NGFWs may integrate features like web filtering, anti-malware scanning, and data loss prevention (DLP) capabilities, providing a more comprehensive security solution.

However, the increased functionality of NGFWs comes at the cost of complexity. Their extensive feature set necessitates meticulous configuration and ongoing management. Security teams require specialised technical skills to navigate the intricate settings and ensure optimal performance. Furthermore, the reliance on DPI can potentially impact network performance, particularly on resource-constrained systems. Careful configuration and resource allocation are crucial to mitigate this potential performance bottleneck. Another vulnerability lies in the requirement for regular updates to threat intelligence and signature databases. Failure to maintain these updates can render NGFWs ineffective against new and evolving threats (da Rocha et al. 2021).

In conclusion, NGFWs represent a significant advancement in network security solutions. Their deep packet inspection, advanced threat detection, and application control capabilities offer a powerful defence against a wide range of cyberattacks. However, their complexity and reliance on ongoing updates necessitate careful consideration during implementation. When deployed and managed effectively, NGFWs can be a critical component of a layered security strategy, safeguarding sensitive data and ensuring the integrity of critical network infrastructure.

5.4.2. Endpoint detection and response (EDR)

The rise of sophisticated cyber attacks and the increasing proliferation of endpoint devices within organisational networks necessitate a paradigm shift in security strategies. Traditional antivirus solutions, reliant on signature-based detection, often struggle to keep pace with the evolving tactics of cybercriminals. Endpoint detection and response (EDR) technology addresses this challenge by offering a proactive and comprehensive approach to endpoint security.

EDR solutions function as vigilant guardians of individual devices within a network. They continuously monitor endpoint activity for signs of suspicious behaviour indicative of potential threats, including malware infections, unauthorised access attempts, or lateral movement within the network (Ministr et al. 2020). Unlike traditional antivirus software, EDR goes beyond signature-based detection, employing a multifaceted approach that leverages techniques such as:

- Advanced Behavioural Analysis: EDR monitors system processes, network behaviour, and file modifications to identify anomalous activity that deviates from established baselines. This allows for the detection of even previously unknown malware strains that traditional signature-based methods might miss.
- Endpoint Vulnerability Assessment: EDR solutions can proactively scan endpoints for known vulnerabilities within operating

systems, applications and firmware. Early identification of these vulnerabilities allows for timely patching and remediation, mitigating potential attack vectors and bolstering the overall security posture.

- **Forensic Analysis and Incident Response:** In the event of a suspected security breach, EDR facilitates forensic analysis by collecting and storing detailed endpoint data. This comprehensive data serves as a vital resource for security teams investigating the nature and scope of the attack, enabling a faster and more effective incident response.
- **Integration with Security Information and Event Management (SIEM):** EDR can integrate with SIEM systems, centralising the collection and analysis of security data from various network sources. This holistic view strengthens threat detection capabilities by correlating events across the network and facilitating coordinated response efforts (Chen et al. 2023a).

However, the implementation of EDR solutions is not without its complexities. The vast amount of data collected by EDR systems can overwhelm security teams, requiring skilled personnel with the expertise to analyse and prioritise potential threats. Additionally, false positives generated by EDR systems can lead to wasted resources and time spent investigating non-malicious activity. Furthermore, the effectiveness of EDR relies heavily on the active monitoring of endpoints (János and Dai 2019). Devices that are not properly enrolled or configured within the EDR system remain vulnerable and unprotected (Kim et al. 2019).

In conclusion, EDR technology represents a significant advancement in endpoint security. Its ability to proactively detect and respond to a wide range of threats, coupled with its forensic analysis capabilities, empowers security teams to defend against cyberattacks more effectively. However, successful implementation requires careful consideration of resource allocation, analyst training, and ongoing system optimisation to minimise false positives and maximise threat detection accuracy. When deployed and managed effectively, EDR solutions can be a critical component of a layered security strategy, safeguarding individual devices and strengthening the overall network security posture.

5.4.3. Security information and event management (SIEM)

The ever-expanding digital landscape necessitates a central nervous system for security operations. Security information and event management (SIEM) systems fulfil this crucial role, acting as the conductor of an orchestra, bringing together the disparate instruments of network security. SIEMs ingest a symphony of security data – log files, alerts, network traffic information and endpoint activity – from firewalls, intrusion detection systems, and various other security sensors (Thakur et al. 2016). By consolidating this data into a single platform, SIEM empowers security teams to gain a panoramic view of their network activity, fostering a deeper understanding of potential threats.

SIEM operates through a series of intricate processes. First, it acts as a central repository, meticulously collecting security data from across the network. This eliminates the need for security personnel to juggle multiple, disparate sources, streamlining the analysis process. Next, SIEM employs event correlation and normalisation techniques, transforming the cacophony of data from various formats and languages into a cohesive whole (Navajas-Adán et al. 2024). This allows for the identification of patterns and anomalies within the data, potentially revealing hidden threats lurking within the network.

SIEM then leverages its analytical prowess and threat intelligence feeds to identify suspicious activity within the consolidated data pool. By correlating events across diverse sources and comparing them against known threats, SIEM prioritises high-risk occurrences,

alerting security teams for further investigation. In the event of a suspected breach, SIEM acts as a war room, providing a centralised view and timeline of events, enabling security teams to rapidly investigate the nature and scope of the incident and implement effective response measures (De Silva 2022). Additionally, SIEM can generate comprehensive security reports, offering valuable insights into network activity, attack trends and the overall security posture.

However, implementing a SIEM solution is not without its challenges. The sheer volume of data collected can be overwhelming, demanding skilled security personnel who can effectively analyse and prioritise potential threats. Furthermore, the success of SIEM hinges on the proper configuration of data collection sources and the ongoing maintenance of threat intelligence feeds. Inaccurate or incomplete data can lead to missed detections and ineffective responses, akin to an orchestra playing out of tune (Kotenko et al. 2022).

In conclusion, SIEM technology forms the backbone of modern security operations centres. Its ability to aggregate, analyse and correlate security data from diverse sources empowers security teams to gain a holistic view of their network activity and identify potential threats. However, successful implementation requires careful consideration of resource allocation, analyst training, and ongoing system optimisation to ensure effective threat detection and incident response. When deployed and managed effectively, SIEM systems become the maestro of security operations, enabling proactive threat hunting and bolstering an organisation's overall security posture.

5.4.4. Zero trust network access (ZTNA)

Traditional network security models often rely on the concept of a secure perimeter, implicitly trusting any user or device within that boundary. This approach, however, becomes increasingly vulnerable in the face of sophisticated cyber attacks and the growing prevalence of remote workforces. Zero Trust Network Access (ZTNA) disrupts this paradigm by adopting a 'never trust, always verify' philosophy, fundamentally changing the way organisations approach access control (Zaid et al. 2023).

ZTNA works by using the following 3 steps:

- **Continuous Authentication:** ZTNA implements a continuous authentication and authorisation process for every user and device attempting to access resources on the network. This applies regardless of the user's location or prior authorisation within the network perimeter (Sarkar et al. 2022).
- **Micro segmentation:** Networks are segmented into smaller, more secure zones. Access is granted only to specific resources based on the principle of least privilege, ensuring users can access only what they need to perform their tasks (Alagappan et al. 2022).
- **Software-Defined Perimeter:** ZTNA often utilises a software-defined perimeter, creating a secure encrypted tunnel between the user and the specific resource they require. This eliminates the need for a traditional, physical network perimeter (Xu et al. 2023).

ZTNA revolutionises access control by adopting a 'never trust, always verify' approach. This fundamentally changes how organisations secure their networks. Unlike traditional models with a defined perimeter, ZTNA continuously verifies every user and device attempting to access resources, regardless of location (Cao et al. 2024). This approach offers several advantages.

ZTNA significantly reduces the attack surface. Even if a malicious actor breaches the network, their ability to move laterally and access sensitive data is restricted. This minimises potential damage and data leaks. Furthermore, ZTNA is ideal for today's geographically dispersed workforces. It secures access regardless of location, making it perfect for cloud-based applications and remote worker scenarios. Additionally, ZTNA can simplify compliance with data privacy

regulations. By ensuring only authorised users can access specific resources, it fosters a principle of least privilege, minimising the risk of unauthorised data disclosure.

However, implementing ZTNA is not without its challenges. The system can be more complex to manage compared to traditional methods, requiring skilled personnel to configure and maintain it effectively. Additionally, the constant authentication process might add steps to user workflows, potentially impacting user experience. Careful configuration is crucial to strike a balance between security and usability (Ali et al. 2021).

In conclusion, ZTNA offers a robust security model for the modern digital landscape. Continuously verifying access and limiting user privileges, significantly strengthens network security. However, careful consideration of its complexity and potential impact on user experience is essential. When deployed and managed effectively, ZTNA can be a valuable tool for securing access to sensitive data and resources, fostering a more secure environment in today's ever-evolving threat landscape.

5.4.5. Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is an additional security measure that goes beyond traditional username and password logins. It requires users to provide more than one verification factor to gain access to an account or system. This multi-layered approach significantly enhances security and makes it much harder for unauthorised individuals to gain access, even if they have stolen a password (Wang and Wang 2023).

Multi-factor authentication (MFA) transcends the limitations of traditional username and password logins by adding an extra layer of security. It requires users to provide more than one verification factor to access an account or system. This multi-layered approach significantly strengthens login security (Suleski et al. 2023), making it exponentially harder for unauthorised individuals to gain access, even if they possess a stolen password.

MFA elevates security by requiring not just something you know (password), but also something you have (security key, code) or something you are (biometric) (Sinigaglia et al. 2020). This additional hurdle significantly frustrates hacking attempts. Phishing attacks, which often trick users into revealing passwords, become largely ineffective against MFA since the additional factor remains out of the attacker's grasp (Sain et al. 2021).

Furthermore, MFA plays a key role in regulatory compliance for many organisations. By enforcing strong authentication for access to sensitive data, MFA helps organisations meet these requirements and safeguard sensitive information (Chen et al. 2023b).

However, MFA is not without its drawbacks. The additional authentication step can introduce a minor inconvenience, adding a few seconds to the login process. Additionally, users might face challenges if they lose their security token or forget their authentication app code, potentially hindering their ability to access accounts. It's important to acknowledge that while highly effective, MFA is not an absolute shield – sophisticated attacks might still exploit vulnerabilities.

In conclusion, MFA is a powerful security tool that significantly enhances login security. Despite some potential inconveniences, the undeniable benefits of heightened protection outweigh the drawbacks. In today's digital landscape, implementing MFA is a wise security practice for both users and organisations seeking to safeguard their data and systems.

5.4.6. Security orchestration, automation and response (SOAR)

The ever-expanding digital landscape presents a significant challenge for security teams – the sheer volume of security alerts and events

generated by various security tools. Security Orchestration, Automation and Response (SOAR) platforms emerge as a potential solution, acting as a conductor in a complex security orchestra. SOAR fosters streamlined operations by coordinating the actions of disparate security tools, automating routine tasks and facilitating efficient incident response (Kinyua and Awuah 2021).

SOAR operates through a centralised hub, collecting security alerts and events from a multitude of sources, including firewalls, intrusion detection systems and endpoint security solutions. This consolidated view empowers security teams with a holistic understanding of potential threats across the network (Lee et al. 2022). However, SOAR's true strength lies in its ability to automate routine security tasks. By leveraging automation, SOAR can streamline processes such as investigating low-priority alerts, enriching threat data with additional context, and initiating pre-defined remediation actions. This frees up valuable security personnel to focus on more complex threats and investigations, significantly improving the efficiency of security operations (Sworna et al. 2023a).

Furthermore, SOAR acts as the conductor, orchestrating the workflow between different security tools. This ensures a streamlined incident response process. SOAR can trigger automated actions based on specific events or pre-configured threat intelligence, enabling faster detection and remediation of security threats. This rapid response can potentially minimise the damage caused by an attack (Bartwal et al. 2022). Additionally, automation within SOAR helps to minimise human error in the incident response process.

However, implementing and managing a SOAR platform is not without its challenges. The system's complexity necessitates skilled personnel to configure workflows and ensure seamless integration with various security tools (Fysarakis et al. 2023). Additionally, SOAR's reliance on automation can lead to wasted resources if it triggers responses based on false positives generated by security tools. Finally, vendor lock-in can be a concern, as some SOAR platforms might not integrate well with all security solutions within an organisation's existing infrastructure. Careful selection is crucial to ensure compatibility and avoid limitations in the future (Sworna et al. 2023b).

In conclusion, SOAR platforms offer a valuable tool for modern security operations. By centralising security data, automating routine tasks, and orchestrating incident response, SOAR empowers security teams to function more efficiently and effectively. However, careful consideration of the platform's complexity and potential for vendor lock-in is essential during implementation. When deployed and managed effectively, SOAR can act as the maestro of security operations, fostering a more streamlined and responsive security posture.

5.4.7. Overview table of the techniques to mitigate cyber attacks in fields alternative to maritime.

Table 3 shows an overview of techniques used to mitigate cyber attacks. The table, for the reader's convenience, gives a summary of techniques, and the positives and negatives of each technique.

The maritime domain, characterised by the increasing adoption of MASS, presents a unique set of cybersecurity challenges. The integration of advanced technologies offers a robust framework for mitigating these risks.

Next-Generation Firewalls can fortify the perimeter of a ship's network, safeguarding against a wide array of cyberattacks targeting vulnerabilities in shipboard systems. Endpoint Detection and Response (EDR) is crucial for identifying and neutralising threats at the device level, protecting critical components such as navigation systems, propulsion systems, and communication equipment. NGFWs can be deployed to create distinct network segments, isolating critical systems like propulsion and navigation from less sensitive

Table 3. Overview table of techniques.

Technique	Description	Positives	Negatives
Next-generation firewalls (NGFWs)	Uses deep packet inspection to analyse data packets for threats. Integrates IDS/IPS, application control, and other functionalities.	<ul style="list-style-type: none"> • Powerful defence against cyber attacks. • Enhanced application control • Comprehensive security solution 	<ul style="list-style-type: none"> • Complex to configure and manage. • Potential performance impact • Relies on regular updates
Endpoint detection and response (EDR)	Monitors endpoint activity for suspicious behaviour. Uses advanced behavioural analysis, vulnerability assessment, and forensic analysis.	<ul style="list-style-type: none"> • Proactive threat detection and response – Faster incident response • Forensic analysis capabilities 	<ul style="list-style-type: none"> • Requires skilled personnel to analyse data. • Potential for false positives. • Requires active endpoint monitoring.
Security information and event management (SIEM)	Central repository for security data from various sources. Correlates events and identifies threats. Generates security reports.	<ul style="list-style-type: none"> • Holistic view of network activity • Improved threat detection • Provides valuable security insights 	<ul style="list-style-type: none"> • Requires skilled personnel to analyse data. • Can be overwhelmed by data volume. • Relies on accurate data collection
Zero trust network access (ZTNA)	'Never trust, always verify' approach. Continuously authenticates users and devices. Implements micro segmentation and software-defined perimeters.	<ul style="list-style-type: none"> • Reduces attack surface. • Ideal for remote workforces • Simplifies data privacy compliance 	<ul style="list-style-type: none"> • More complex to manage than traditional models. • Potential impact on user experience.
Multi-factor authentication (MFA)	Requires additional verification factors beyond username and password.	<ul style="list-style-type: none"> • Significantly enhances login security. • Effective against phishing attacks • Meets compliance requirements for many organisations 	<ul style="list-style-type: none"> • Minor inconvenience for users • Potential challenges if users lose authentication factors
Security orchestration, automation and response (SOAR)	A centralised hub for security alerts and events. Automates routine tasks and facilitates incident response. Orchestrates security tools.	<ul style="list-style-type: none"> • Streamlined security operations. • Improved efficiency. • Faster and more effective incident response. 	<ul style="list-style-type: none"> • Complex to implement and manage. • Potential for wasted resources due to false positives. • Vendor lock-in concerns.

functions. Advanced threat detection capabilities within NGFWs can thwart a myriad of cyberattacks.

Multi-Factor Authentication (MFA) provides a robust layer of security by demanding multiple forms of verification for accessing shipboard systems. This technology significantly reduces the risk of unauthorised access, even in the event of compromised credentials. Implementing MFA for all users, especially those with elevated privileges, significantly enhances security. Role-Based Access Control (RBAC) should be enforced to ensure users only have the necessary permissions.

Security Information and Event Management (SIEM) is indispensable for aggregating, analysing and correlating security data from diverse sources. By offering a comprehensive overview of shipboard security posture, SIEM enables timely detection of anomalies and security incidents. By correlating data from various sources, SIEM can identify anomalies and potential security incidents.

The Zero Trust security model is particularly pertinent to MASS due to their inherent complexity and distributed nature. By embracing a 'never trust, always verify' approach, organisations can mitigate the risk of lateral movement within the ship's network and safeguard critical assets. This involves continuously verifying the identity and trustworthiness of users, devices, and applications before granting access. Network segmentation, micro-segmentation and least privilege principles are core components of this approach.

Security Orchestration, Automation and Response (SOAR) can streamline incident response processes by automating repetitive tasks and expediting responses to threats. This technology is essential for preserving the resilience of MASS in the face of evolving cyber threats. SOAR platforms can automate routine tasks, accelerate incident response, and improve overall security efficiency.

5.5. Analysis of the trends of the cyber security measures available

As stated earlier, the maritime industry, like many others, faces an evolving cybersecurity landscape. Below is an analysis of prominent trends from the literature reviewed above, and how they align with various security techniques.

- Increased digitalisation: Ships are becoming increasingly reliant on automation and interconnected systems, creating a larger attack surface (Ahvenjarvi et al. 2019).
- Remote operations: The growing use of remote monitoring and control systems introduces new vulnerabilities (Alop 2019).
- Supply chain attacks: Targeting vulnerabilities in the maritime supply chain, including software providers and equipment manufacturers (Amro and Gkioulos 2023).
- Ransomware attacks: Disrupting critical operations and causing significant financial damage (Epikhin and Modina 2021).
- Data breaches: Theft of sensitive data like crew information, cargo details, and intellectual property (Kavallieratos et al. 2020a).

Given the aforementioned trends, there are several techniques/technologies mentioned in this section with a high urgency for research. The following is a list of the techniques/technologies that have a high urgency for further research and the specific research areas of the techniques/technologies that would benefit the most:

1. Sensor Systems and Artificial Intelligence (AI)/Machine Learning (ML)

Integrating sensor data with AI/ML can identify anomalies in network activity, predict cyberattacks and enable real-time threat detection (Amro et al. 2020). Research needed in this discipline would involve the development of AI/ML models specifically for maritime cybersecurity, focusing on anomaly detection in sensor data related to navigation, cargo handling, and ship operations.

2. Intrusion Detection Systems (IDS) and Endpoint Detection and Response (EDR)

Traditional perimeter defenses are shown above to be insufficient (Kardakova et al. 2020). Therefore, research would be needed to develop advanced IDS/EDR solutions specifically designed for maritime networks, considering the unique vulnerabilities and limitations of onboard computing systems.

3. Zero Trust Network Access (ZTNA) and Multi-Factor Authentication (MFA)

Remote access and crew mobility necessitate robust access control (Meland et al. 2021). Research is needed in this area to develop user-friendly ZTNA solutions for maritime environments and integrate MFA with existing maritime authentication protocols.

4. Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR)

Streamlining security operations is crucial, but data management considerations exist (Li and Yu 2020). Therefore, further research would be needed to develop lightweight and efficient SIEM/SOAR solutions suitable for resource-constrained maritime environments, while ensuring scalability for larger fleets.

5. Cybersecurity Training and Awareness

Human error remains a significant vulnerability (Symes et al. 2022). Research in the human factors field is vital. By using a neuroergonomic approach to develop immersive and engaging cybersecurity training programmes for maritime personnel, addressing specific threats and best practices relevant to their roles.

Also, the following techniques have the potential for further research, but it is the opinion of the authors that these techniques/technologies have a lower urgency:

- Collision Avoidance Systems (CAS): While cybersecurity threats to CAS exist (Qiu et al. 2021), research efforts might prioritise integration with existing safety measures.
- Redundancy and Fault Tolerant Systems: These are well-established practices for physical infrastructure security (Sain et al. 2021), but research can focus on cyber-specific redundancy solutions.
- Secure Communication Protocols: Ongoing research and adoption of secure communication protocols remain important (Corfield 2023).

5.6. Nuances of cybersecurity in maritime environments compared to other fields

Maritime cybersecurity faces unique challenges compared to other fields. Unlike land-based systems with constant connectivity, ships operate in isolated environments with limited internet access. This isolation, while offering a false sense of security, can give attackers more time to operate undetected. Additionally, the industry relies heavily on legacy control systems not designed with cybersecurity in mind, making them vulnerable. Furthermore, a critical difference lies in the data itself. Ships handle highly specific data like navigation details and cargo information, which in the wrong hands could have devastating consequences. Environmental constraints like limited crew size with less IT expertise further complicate matters, as immediate response to cyber threats might be difficult. Finally, the regulatory landscape in maritime can be uneven, with older vessels or those operating under lax flag-of-convenience rules potentially having weaker cybersecurity postures. These combined factors create a complex cybersecurity landscape unique to the maritime industry.

5.7. Data specificity

AI/ML models trained on data from terrestrial networks may struggle with maritime-specific data sets (Amro et al. 2020).

Shipboard sensors collect a wide range of data on weather conditions, ocean currents, cargo status and navigation (GPS, radar, etc.). AI/ML models require training on these unique data types to identify

anomalies indicative of cyberattacks that might manipulate sensor readings (Fysarakis et al. 2023).

Maritime communication systems often rely on specialised protocols like the Automatic Identification System (AIS) and Global Maritime Distress and Safety System (GMDSS) (Issa et al. 2022). AI/ML models need to understand these protocols to effectively analyse network traffic for suspicious activity (Kavallieratos et al. 2020b).

5.8. Environmental constraints

Ships frequently operate in areas with limited or unreliable internet connectivity (Ahmed and Gkioulos 2022). AI/ML models need to be optimised for efficiency (Ahmed and Gkioulos 2022), requiring smaller data footprints and lower processing power for onboard functionality (Amro and Gkioulos 2023).

Shipboard computing systems often have lower processing power compared to terrestrial data centres (Bolbot et al. 2020). AI/ML models must be lightweight and efficient to run smoothly on these systems (Chiu et al. 2011).

5.9. Human factors

Maritime personnel possess varying levels of technical expertise (Symes et al. 2022). Cybersecurity training programmes require tailoring to the specific roles and responsibilities of each crew member, from captains and engineers to catering staff and security personnel (Ben Farah et al. 2023). This ensures everyone understands the cybersecurity risks relevant to their tasks and can identify suspicious activity.

Maritime crews are frequently international, with personnel from diverse backgrounds and varying levels of English proficiency (Alop 2019). Therefore, training materials need to be clear, concise and potentially available in multiple languages to ensure effective communication and knowledge retention.

5.10. Regulatory landscape

The maritime industry has its own set of regulations and compliance requirements related to cybersecurity (Issa et al. 2022). Training programmes need to address these specific regulations and ensure crew members are aware of their obligations.

An AI/ML model trained on terrestrial network traffic might struggle to identify suspicious changes in a ship's GPS data caused by a cyberattack (Amro and Gkioulos 2023). However, a model specifically trained on maritime data sets can learn the normal patterns of GPS readings and flag deviations that could indicate manipulation (Goudossis and Katsikas 2019).

Training for engineers should focus on identifying cyber threats that might target shipboard automation systems or engine control systems. This differs from training for catering staff who might need to be more aware of phishing attacks or social engineering tactics.

By adapting cybersecurity techniques to address the specific data, environmental, human, and regulatory aspects of the maritime industry, organisations can build more robust defenses against cyberattacks and ensure the safe and secure operation of vessels (Amro et al. 2023).

Cybersecurity in the maritime industry demands a multi-pronged approach. Techniques leveraging AI/ML, advanced access control, and security automation are crucial areas for further research (Mission Secure 2023) due to the evolving threat landscape and unique challenges faced by maritime operations.

6. Discussion

The urgent need for further research in cyber security for autonomous ships cannot be overstated. The rise of autonomous ships presents a promising future for the maritime industry, offering improved efficiency, reduced costs and enhanced safety. However, as per the research in Section 2, the vulnerability of autonomous ships to cyber threats becomes a pressing concern. This conclusion will provide an academic perspective on why additional research in cyber security is desperately needed for autonomous ships.

Firstly, the evolving threat from cyber-attacks demands continuous research in cyber security. As technology advances, so do the capabilities and sophistication of malicious actors. Autonomous ships are no exception to these risks, as they become potential targets for cyber-attacks. Further research is necessary to stay ahead of emerging threats, understand potential attack vectors, and develop effective countermeasures. By continuously studying and analysing the ever-evolving threat landscape, researchers can proactively enhance the security posture of autonomous ships.

Unauthorised access and control pose significant risks to autonomous ships. With interconnected systems and external communication interfaces, malicious actors can exploit vulnerabilities to gain unauthorised access. This unauthorised access can lead to various detrimental consequences, including system manipulation, data theft, or possibly complete hijacking of the vessel. Further research in cyber security is desperately needed to identify and address potential entry points for unauthorised access and develop robust authentication and authorisation protocols. By conducting in-depth vulnerability assessments and implementing secure communication channels, researchers can fortify autonomous ships against unauthorised access and control.

Vessels heavily rely on complex software systems and hardware components to navigate and operate. However, these systems are not immune to malfunctions and failures. Cyber security research plays a critical role in identifying vulnerabilities in software and hardware, ensuring the reliability and resilience of autonomous ship systems. Through extensive testing, validation and the development of backup and redundancy mechanisms, researchers can mitigate the risks associated with system malfunctions and failures.

Data integrity and privacy are also major concerns in autonomous ship cyber security. These vessels generate massive amounts of data, including navigation logs, sensor readings and operational information. Ensuring the integrity and privacy of this data is paramount to protecting the interests of ship owners, operators and stakeholders. Further research in cyber security is desperately needed to develop secure data transmission protocols, encryption mechanisms and data storage solutions. By implementing robust data protection measures, researchers can safeguard the integrity and privacy of the data generated by autonomous ships.

Additionally, industry-wide collaboration and standardisation are crucial for the advancement of cyber security in autonomous ships. The complexity of autonomous ship cyber security necessitates collaboration among industry stakeholders, researchers and regulatory bodies. By sharing knowledge, experiences and insights, researchers can collectively address common challenges and develop standardised approaches to cyber security. This collaboration can foster the establishment of international standards, regulations and certification processes specific to autonomous ship cyber security. By working together, the industry can create a unified front against cyber threats and promote a culture of cyber security awareness and preparedness.

The impact on public safety and trust cannot be overlooked when considering the need for further research in cyber security for autonomous ships. Autonomous ships not only play a critical role in

the future of the maritime industry but also have a significant impact on public safety. A successful cyber-attack on an autonomous ship could result in environmental damage, threats to human lives and economic disruption. Such incidents have the potential to erode public trust in autonomous ship technology and hinder its widespread adoption. Therefore, it is essential to invest in research and innovation to mitigate these risks and ensure the safety of not only the maritime industry but also the general public.

In conclusion, further research in cyber security for autonomous ships is desperately needed to address the evolving threat landscape, mitigate unauthorised access and control, mitigate system malfunctions and failures, protect data integrity and privacy, foster industry-wide collaboration and standardisation, and ensure public safety and trust. The complexities and risks associated with autonomous ships require a proactive and comprehensive approach to cyber security.

By investing in further research, the maritime industry can stay ahead of emerging cyber threats and vulnerabilities. Researchers can identify potential entry points for unauthorised access, develop robust authentication and authorisation protocols, and establish secure communication channels to fortify autonomous ships against malicious actors. Moreover, research efforts are essential in identifying vulnerabilities in software and hardware systems, ensuring the reliability and resilience of autonomous ship operations.

Protecting data integrity and privacy is another critical aspect of cyber security research. By developing secure data transmission protocols, encryption mechanisms and data storage solutions, researchers can safeguard the sensitive information generated by autonomous ships. This is crucial to protect the interests of ship owners, operators and stakeholders, as well as to comply with regulatory requirements.

Industry-wide collaboration and standardisation are vital for a unified and effective response to cyber threats in the autonomous ship sector. By sharing knowledge, experiences and best practices, researchers, industry stakeholders and regulatory bodies can collectively establish international standards, regulations and certification processes specific to cyber security for autonomous ships. This collaboration promotes a culture of cyber security awareness and preparedness, ensuring a unified and resilient approach to protecting autonomous ships from cyber threats.

Furthermore, the impact on public safety and trust cannot be overstated. Autonomous ships have a significant impact not only on the maritime industry but also on the general public. With the potential for cyber-attacks leading to environmental damage, threats to human lives and economic disruption, it is crucial to prioritise cyber security research. By investing in innovative solutions, conducting rigorous testing and validation, and raising awareness about cyber risks, researchers can inspire confidence in the safety and reliability of autonomous ships. This, in turn, paves the way for broader acceptance and adoption of this transformative technology.

There are legal and insurance implications of cyber security in autonomous shipping. The community needs to work together and update by consensus the key legal instruments and policy documents (Fenton and Chapsos 2023). More specifically, in 2017 the IMO began a regulatory scoping exercise (RSE) where they tasked four IMO committees, the Maritime Safety Committee, the Legal Committee, the Facilitation Committee and the Maritime Environment Protection Committee to address common issues. The outcome of the RSE was to address the common gaps by implementing a MASS code instead of addressing every SOLAS instrument individually due to the potential for inconsistencies, confusion and to raise potential barriers. The main key approaches to regulating MASS as stated in (Fenton and Chapsos 2023) are:

The Marine Guidance Note 664 – Issued by the maritime and coastguard agency in 2022, the UK's Marine Guidance Note 664

creates a framework for certifying innovative technologies on ships, aiming to balance safety with encouraging development. It applies to a wide range of recent technologies, not just autonomous vessels. The process involves early engagement with regulators, prioritises safety, and allows applicants to identify areas where existing regulations might need updates. While challenges exist regarding intellectual property and interaction with humans at sea, MGN 664 marks a significant step towards regulating these new maritime technologies.

The Workboat Code Edition 3 – the UK's upcoming Workboat Code Edition 3 aims to standardise regulations for small workboats, including remotely operated uncrewed vessels (ROUVs). It clarifies the certification process, reduces assessment times, and has an annex specifically for ROUVs. The annex outlines rules for operation, maintenance, crew qualifications and cybersecurity. Some points require clarification, like the applicability to foreign vessels and the meaning of a 'safe state' during emergencies. The code also raises concerns about cost-efficiency due to staffing requirements for remote operators and potential limitations on managing multiple ROUVs simultaneously.

Maritime UK voluntary industry code of practice – the UK maritime industry created a voluntary code of practice for designing, building, and operating small autonomous and semi-autonomous vessels. This code aims to set best practices until more detailed regulations are developed. It emphasises safety, aligning with existing regulations like COLREGS and focusing on operator skills. It also considers areas like cybersecurity but is not mandatory. Industry officials see it as a way to collaborate and share ideas for this developing technology.

The liability, insurance, vehicle technology and aviation bill – This discusses liability for accidents caused by autonomous vehicles, including potentially autonomous ships. Traditional legal systems rely on fault to assign blame. Determining fault for accidents involving autonomous vehicles can be difficult. A bill in the UK Parliament aims to clarify insurance liability for accidents caused by 'automated vehicles.'

Key Points of the insurance implications of cyber security for autonomous shipping:

- Insurers are liable for damages if the autonomous vehicle is insured.
- The owner is liable if the vehicle is not insured.
- Contributory negligence applies (e.g. not updating software).

The bill targets road vehicles, but the definition of 'automated vehicle' might encompass autonomous ships. The law could clarify liability for accidents involving insured autonomous ships, paving the way for similar legislation for MASS.

The UK seems to be leading the way in regulating innovative technologies for autonomous ships. They have established certification processes, addressed insurance issues and pioneered trials. However, international regulations are lacking. The IMO needs to update conventions and reach a consensus for autonomous ships to be widely integrated. UK regulations and best practices from other countries can inform this process to establish international law and norms. Further research is needed on how other key countries are approaching autonomous ships. From the above, it can be proposed that further work in this sector should include: a focus on building cybersecurity into the design, protecting individual systems onboard, ensuring the security of AI decision-making, creating safe communication channels and developing international standards and regulations. This will be crucial to mitigating cyber threats and ensuring the safe operation of these autonomous vessels.

Conducting an analysis on the above legal and insurance implications in autonomous shipping, there are a number of key findings:

- **Regulatory Fragmentation:** The absence of a unified international regulatory framework for autonomous ships creates inconsistencies and potential barriers to innovation.
- **Liability and Insurance Uncertainties:** The traditional liability model based on fault is inadequate for autonomous ships, necessitating new legal and insurance frameworks.
- **UK Leadership:** The UK has demonstrated a proactive approach to regulating autonomous ships through initiatives such as the Marine Guidance Note 664 and the Workboat Code Edition 3.
- **Industry Collaboration:** The voluntary industry code of practice is a valuable step towards establishing best practices, but mandatory regulations will be necessary for effective oversight.

These findings bring about main challenges, but also opportunities. These challenges include:

- **International Cooperation:** Achieving consensus among different maritime nations on regulatory frameworks is complex.
- **Technological Advancements:** The rapid pace of technological development outstrips the ability of regulators to keep up.
- **Liability and Insurance:** Determining liability for accidents involving autonomous ships presents significant legal challenges.

Some of the opportunities could include; The development of new regulatory frameworks. This can create opportunities for innovation and economic growth, new and improved risk management strategies, collaboration between other nations to create strong bonds and lastly, investment in cybersecurity of MASS vessels.

Given the current regulations with respect to insurance and legalities, the authors of this document have some recommendations:

- **Accelerate International Cooperation:** The IMO should prioritise the development of a comprehensive international regulatory framework for autonomous ships.
- **Strengthen Cybersecurity Measures:** Incorporate cybersecurity into the design and operation of autonomous ships from the outset.
- **Develop Clear Liability and Insurance Frameworks:** Establish clear rules for determining liability and ensuring adequate insurance coverage.
- **Promote Industry Collaboration:** Encourage collaboration between industry stakeholders to share best practices and develop industry standards.
- **Invest in Research and Development:** Support research into autonomous ship technologies, including cybersecurity and risk management.
- **Monitor and Adapt:** Continuously monitor the evolving landscape of autonomous shipping and adjust regulations accordingly.

From the above, it can be proposed that further work in this sector should include: training developers and regulators on adversarial AI (AAI), evaluating attacks and defences in various maritime conditions, testing real-world AI systems against AAI to understand the secondary effects of attacks, consider the likelihood of different attacks in real-world maritime environments and study the misuse of AI for illegal activities.

Given the papers investigated and summarised in the literature review, it seems that a possible new area of understanding exists within the 'The Human-Machine Security Loop'. Existing research focuses on securing individual systems and communication. A new understanding could explore how the human element, in the form of remote operators, interacts with these secured systems. This would involve studying potential vulnerabilities in human-machine interfaces, the psychology of remote decision-making under cyber

threats, and the need for robust training protocols for remote operators to identify and respond to cyberattacks effectively. This would create a more holistic security approach that considers not just the technology but also the human element in the autonomous shipping ecosystem.

7. Conclusions

To re-iterate, further research in cyber security for autonomous ships is urgently needed. The evolving threat landscape, potential unauthorised access and control, system malfunctions and failures, data integrity and privacy concerns, industry-wide collaboration and the impact on public safety and trust all highlight the criticality of cyber security in this domain. By investing in research and innovation, industry stakeholders and researchers can proactively identify vulnerabilities, develop robust security measures and ensure the safe and secure operation of autonomous ships. Only through a comprehensive and collaborative research effort can we navigate the challenges, protect against cyber threats and create a future where autonomous ships thrive securely.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Disclaimer

This paper is the opinion of the authors and does not necessarily represent the belief and policy of their employers.

ORCID

Steve Symes  <http://orcid.org/0009-0008-2717-2378>

References

- ABB Oy, Marine and Cranes. 2022. Azipod® XO2100 and XO2300. Helsinki: ABB. https://library.e.abb.com/public/6c1b0250efd18e73c1257a530040dcf2/XO2100_XO2300_Product_Intro_lowres.pdf.
- Ahmed A, Gkioulos V. 2022. From click to sink: utilizing AIS for command and control in maritime cyber attacks. *Computer security- ESORICS*. p. 535–553.
- Ahvenjarvi S, Czarnowski I, Szymanski P. 2019. Safe information exchange on board of the ship. *TransNav Int J Mar Navig Saf Sea Transp*. 13(1):165–171. doi:10.12716/1001.13.01.17.
- Alagappan A, Venkatachary S, Andrews L. 2022. Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Rep*. 8(1):1309–1320. doi:10.1016/j.egy.2021.11.272.
- Ali B, Gregory M, Li S. 2021. Uplifting healthcare cyber resilience with a multi-access edge computing Zero-Trust Security Model. *2021 1st International Telecommunication Networks and Applications Conference (ITNAC)*. Sydney, Australia.
- Alop A. 2019. The main challenges and barriers to the successful ‘smart shipping’. *TransNav Int J Mar Navig Saf Sea Transp*. 13(3):521–528. doi:10.12716/1001.13.03.05.
- Amro A, Gkioulos V. 2023. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *Int J Inf Secur*. 22(1):249–288. doi:10.1007/s10207-022-00638-y.
- Amro A, Gkioulos V, Katsikas S. 2020. Connect and protect: requirements for maritime autonomous surface ship in urban passenger transportation. *Comput Secur ESORICS*. 11980:69–85. doi:10.1007/978-3-030-42048-2_5.
- Amro A, Gkioulos V, Katsikas S. 2023. Assessing cyber risk in cyber physical systems using the ATT&CK framework. *ACM Trans Priv Secur*. 2:249–288.
- Amro A, Oruc A, Katsikas S. 2022. Navigation data anomaly analysis and detection. *Information*. 13(3):7. doi:10.3390/info13030104.
- Anatoliy P, Kristina V, Aleksandr V. 2018. Technologies of safety in the Bank Sphere from cyber attacks. *ELConRUS*. Moscow.
- Bakdi A, Glad IV. 2021. Testbed scenario design exploiting traffic big data for autonomous ship trails under multiple conflicts with collision/grounding risks and spatio-temporal dependencies. *IEEE Trans Intell Transp Syst*. 22(12):7914–7930. doi:10.1109/TITS.2021.3095547.
- Bakdi A, Vanem E. 2022. Fullest COLREGs evaluation using fuzzy logic for collaborative decision making analysis of autonomous ships in complex situations. *IEEE Trans Intell*. 23(10):18433–18445. doi:10.1109/TITS.2022.3151826.
- Bartwal U, Mukhopadhyay S, Negi R, Shukla S. 2022. Security orchestration, automation, and response engine for deployment of behavioural honeypots. *2022 5th IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022)*. Edinburgh, Scotland.
- Ben Farah M, Ukwandu E, Bellekens X. 2023. Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*. 1:13.
- Bolbot V, Theotokatos G, Van Collie A. 2023. A novel risk assessment process: Application to an autonomous inland waterways ship. *IMEJRR* 2023.
- Bolbot V, Theotokatos G, Vassalos D. 2020. A novel cyber-risk assessment method for ship systems. *Saf Sci*. 131. doi:10.1016/j.ssci.2020.104908.
- Boudehenn C, Cexus J, Boudraa A. 2023. Holistic approach of integrated navigation equipment for cybersecurity at sea. *ICCSASMCS*.
- Cao Y, Pokhrel S, Zhu Y, Doss R, Li G. 2024. Automation and orchestration of zero trust architecture: potential solutions and challenges. *Machine Intell Res*. 1(1). doi:10.1007/s11633-023-1456-2.
- Chang C, Kontovas C, Yang Z. 2021. Risk assessment of the operations of maritime autonomous surface ships. *RESS*, 207.
- Chen TM, Zheng CB, Zhu TT, Xiong CL, Ying J, Yuan QX, Cheng WRLV, MQ. 2023a. System-level data management for endpoint advanced persistent threat detection: issues, challenges and trends. *Comput Secur*. 135(1):197–199. doi:10.1016/0167-4048(94)90095-7.
- Chen Z, Cheng Z, Luo W, Ao J, Liu Y, Sheng K, Chen L. 2023b. Fsmfa: efficient firmware-secure multi-factor authentication protocol for IoT devices. *Internet of things*. 21(1). 100685 (article number). doi:10.1016/j.iot.2023.100685.
- Chiu S, Provan G, Vasco D. 2011. Shipboard system diagnostics & reconfiguration using model-based autonomous cooperative agents. *Control Appl Mar Syst*. 1(1):323–329.
- Corfield G. 2023. *The Telegraph - Royal Navy contractor forced to pay off cyber criminals*. Retrieved November 2023, from <https://www.telegraph.co.uk/business/2023/07/07/royal-navy-contractor-forced-to-pay-off-cyber-criminals/>.
- Cynalytica. 2024. *Protect Your Onboard and Onshore Operations*. Retrieved April 17th, 2024, from <https://www.cynalytica.com/maritime/>.
- Damerius R, Schubert AR, Rethfeldt C, Finger G, Fischer S, Milbradt G, Jeinsch T. 2023. Consumption-reduced manual and automatic manoeuvring with the conventional vessel. *J Mar Eng Technol*. 22:55–66. doi:10.1080/20464177.2023.22154666.
- da Rocha B, de Melo L, de Sousa R. 2021. Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model. *Workshop on Communication Networks and Power Systems (WCNPS)*, (p. Unknown). New York.
- De Silva J. 2022. Cyber security and the Leviathan. *Comput Secur*. 116(1):102674 (article number). doi:10.1016/j.cose.2022.102674.
- Dittman K, Hansen P, Blanke M. 2021. Autonomy for ships: A sovereign agents architecture for reliability and safety by design. *SYSTOL*, p. 50–57.
- Ehlers T, Portier M, Thoma D. 2022. Automation of maritime shipping for more safety and environmental protection. *AT-Automatisierungstechnik*. 70(5):406–410. doi:10.1515/auto-2022-0003.
- Epikhin A, Modina M. 2021. Problems of introducing unmanned vessels on the basis of statistical studies of emergencies and ship losses. *Mar Intell Technol*. 3:77–82.
- Fang Y, PU J, Liu S. 2022. A control strategy of normal motion and self-rescue for autonomous underwater vehicle based on deep reinforcement learning. *AIP Adv*. 1:12–14.
- Fenton A, Chapsos I. 2023. Ships without crews: IMO and UK responses to cyber-security, technology, law and regulation of maritime autonomous surface ships (MASS). *Front Comput Sci*. 5. doi:10.3389/fcomp.2023.1151188.
- Fysarakis K, Lekidis A, Mavroeidis V, Lampropoulos K, Lyberopoulos G, Vidal I, Terés i Casals JC, Rodriguez E, Moreno Sancho A, Mavrelos A, Tsantekidis M, Pape S, Chatzopoulou A, Nanou C, Drivas G, Photiou V, Spanoudakis G, Koufopavlou O. 2023. PHOENIX-A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange. *2023 IEEE International Conference on Cyber Security and Resilience, CSR*. Venice, Italy.
- Gkioulos V, Ahmed A. 2021. AIS for ship survivability in maritime cyber attacks. *Computer security- ESORICS*. p. 91–119.
- Goudossis A, Katsikas SK. 2019. Towards a secure automatic identification system (AIS). *J Mar Sci Technol*. 2(24):410–423. doi:10.1007/s00773-018-0561-3.
- Greiman V. 2019. Navigating the cyber sea: dangerous atolls ahead. *14th ICCWS*. p. 87–93.
- Hopcraft R, Harish A, Jones K. 2023. Raising the standard of maritime voyage data recorder security. *J Mar Sci Eng*. 11(2). doi:10.3390/jmse11020267.
- Issa M, Ilinca A, Rizk P. 2022. Maritime autonomous surface ships: problems and challenges facing the regulatory process. *Sustainability*. 14(23). doi:10.3390/su142315630.

- János F, Dai N. 2019. Security concerns towards Security Operations centers. 2018 IEEE 12TH INTERNATIONAL SYMPOSIUM ON APPLIED COMPUTATIONAL INTELLIGENCE AND INFORMATICS (SACI). Timisoara, Romania. P. 273–278.
- Jung B, Moon S, Shin Y. 2022a. Development of autonomous recovery system for a pipeline of naval ships by using a multistage control algorithm. *Trans Mechatron.* 27(2):1150–1161. doi:10.1109/TMECH.2021.3082631.
- Jung J, Lee Y, Yeu T. 2022b. Multi-Modal sonar mapping of offshore cable lines with an autonomous surface vehicle. *J Mar Sci Eng.* 10(3). doi:10.3390/jmse10030361.
- Kardakova M, Shipunov I, Knysh T. 2020. Cyber security on sea transport. *RESS*, p. 982, 481–490.
- Kavallieratos G, Diamantopoulou V, Katsikas S. 2020a. Shipping 4.0; security requirements for the cyber-enabled ship. *IEEE Trans Ind Inf.* 16(10):6617–6625. doi:10.1109/TII.2020.2976840.
- Kavallieratos G, Katsikas S, Gkioulos V. 2020b. Modelling shipping 4.0; A reference architecture for the cyber-enabled ship. *ACIIDS*.
- Kavallieratos G, Spathoulas G, Katsikas S. 2021. Cyber risk propagation and optimal selection of cybersecurity for complex cyberphysical systems. *Sensors.* 5:21.
- Kim H, Kwon H, Kim K. 2019. Modified cyber kill chain model for multimedia service environments. *Multimed Tools Appl.* 78(3):3153–3170. doi:10.1007/s11042-018-5897-5.
- Kinyua J, Awuah L. 2021. Ai/ML in security orchestration, automation and response: future research directions. *Intell Automat soft Compu.* 28(2):527–545. doi:10.32604/iasc.2021.016240.
- Kotenko I, Doynikova E, Fedorchenko A, Desnitsky V. 2022. Automation of asset inventory for cyber security: investigation of event correlation-based technique. *Electronics (Basel).* 11(15). 2368 (article number). doi:10.3390/electronics11152368.
- Lee M, Jang-Jaccard J, Kwak J. 2022. Novel architecture of security orchestration, automation and response in internet of blended environment. *Comput Mater Continua.* 73(1):199–223. doi:10.32604/cmcc.2022.028495.
- Li J, Yu X. 2020. Robust saturated tracking control of an autonomous surface vehicle. *CCDC*, p. 3472–3477.
- Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gotzsche P, Ioannidis JP, Clarke M, Devereaux PJ, Kleijnen J, Moher D. 2009. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explain and elaboration. *J Clin Epidemiol.* 62(10):1–34. doi:10.1016/j.jclinepi.2009.06.006.
- Liou J. 2011. AUV hydrodynamics for survivability and controllability. *MTS/IEEE OCEANS Conference.* Paris.
- Longo G, Martelli M, Russo E, Merlo A, Zaccone R. 2023a. Adversarial waypoint injection attacks on maritime autonomous surface ships (MASS) collision avoidance systems. *J Mar Eng Technol.* 3:144–147. doi:10.1080/20464177.2023.2298521.
- Longo G, Russo E, Armando A, Merlo A. 2023b. Attacking (and defending) the maritime radar system. *IEEE Trans Inf Forensics Secur.* 18:3575–3589. doi:10.1109/TIFS.2023.3282132.
- Loomis W, Singh VV, Kessler DG, Bellekens DX. 2021. *A system of systems: Cooperation on maritime cybersecurity - Atlantic Council.* Retrieved April 18th, 2024, from <https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/>.
- Loukas GK. 2019. A taxonomy and survey of cyber physical intrusion detection approaches for vehicles. *AD HOC Networks*, 124–147, 84.
- Manuel R. 2023. *The Defense Post.* Retrieved October 2023, from <https://www.thedefensepost.com/2023/07/18/uk-drone-swarm-operation-seebyte/>.
- Marco B, Alessandro P, Kyle W. 2014. A security evaluation of AIS automated identification system. *The 30th annual computer security applications conference (ACSAC' 14).* New York.
- Martelli M, Cassara P, Tonello N. 2020. The internet of ships. *ERCIM NEWS*, 17–18.
- Martelli M, Virdis A, Di Summa M. 2021. An outlook on the future marine traffic management system for autonomous ships. *IEEE access*, p. 9, 157316–157328.
- McGillivray P. 2018. Why maritime cybersecurity is an ocean policy priority and how it can be addressed. *Mar Technol Soc J.* 52(5):44–57. doi:10.4031/MTSJ.52.5.11.
- Meland P, Bernsmed K, Nesheim D. 2021. A retrospective analysis of maritime cyber security incidents. *Transnav Int J Mar Navig Saf Sea Transp.* 15(3):519–530. doi:10.12716/1001.15.03.04.
- Ministr J, Pitner T, Chaplyha V. 2020. Innovation of the Endpoint Security System. *Digitalized Economy, Society And Information Management (IDIMT-2020)*, 49, 93–98.
- Mission Secure. 2023. *Mission Secure - Maritime Security.* Retrieved November 2023, from <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach>.
- Navajas-Adán J, Badia-Gelabert E, Jiménez-Saurina L, Marijuán-Martín M, Mayo-García R. 2024. Perceptions and dilemmas around cyber-security in a spanish research center after a cyber-attack. *Int J Inf Secur.* 5(1):847–947. doi:10.1007/s10207-024-00847-7.
- Onishchenko O, Shumilova K, Volianskiy Y. 2022. Ensuring cyber resilience of ship information systems. *Transnav Int J Mar Navig Saf Sea Transp.* 16(1):43–50. doi:10.12716/1001.16.01.04.
- Palbar Misas J, Hopcraft R, Tam K, Jones K. 2024. Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness. *J Mar Eng Technol.* 1. doi:10.1080/20464177.2024.2330176.
- Park C, Kontovas C. 2023. A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean Coast Manag.* 235. doi:10.1016/j.ocecoaman.2023.106480.
- Park S, Kwon S, Park Y, Kim DY. 2022. Session management for security systems in 5G standalone network. *IEEE ACCESS.* 10(1). :73421–73436. doi:10.1109/ACCESS.2022.3187053.
- Pitropakis N, Logothetis M, Lambrinouidakis C. 2020. Towards the creation of a threat intelligence framework for maritime infrastructures. *Comput Secur ESORICS.* 1:53–68. doi:10.1007/978-3-030-42048-2_4.
- Qiao S, Zheng K, Wang G. 2020. A path planning method for autonomous ships based on SVM. *Ocean Eng.* 1:3068–3072.
- Qiu Y, Li Y, Lang J. 2021. An optimal tracking control method for unmanned ship approach. *CCDC (33rd)*, 546–551.
- Sain M, Normurodov O, Hong C, Hui K. 2021. A Survey on the Security in Cyber Physical System with Multi-Factor Authentication. 2021 23rd International Conference on Advanced Communication Technology (ICACT 2021): On-Line security In Pandemic ERA. New York.
- Sarkar S, Choudhary G, Shandilya S, Hussain A, Kim H. 2022. Security of zero trust networks in cloud computing: A comparative review. *Sustainability.* 14(18). 11213 (article number). doi:10.3390/su141811213.
- Schinas O, Metzger D. 2023. Cyber-seaworthiness: A critical review of the literature. *Mar Policy.* 151. doi:10.1016/j.marpol.2023.105592.
- Sepehri A, Vandchali H, Montewka J. 2022. The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review. *Ocean Eng.* 243. doi:10.1016/j.oceaneng.2021.110162.
- Serru T, Nguyen N, Rauzy A. 2023. Modeling cyberattack propagation and impacts on cyber physical system safety: An experiment. *Electronics (Basel).* 12. doi:10.1002/elt.2.12.
- Shapo V, Levinskyi M. 2021. Means of cyber security aspects studying in maritime specialists education. Internet of things, infrastructures and mobile applications. 389–400.
- Shipunov I, Voevodskiy K, Gatchin Y. 2019. About the problems of ensuring information security on unmanned ships. *EICONRUS.* Moscow.
- Silva R, Hickert C, Sookoor T. 2022. AlphaSOC: Reinforcement learning-based cybersecurity automation for cyber-physical systems. *ICCPs.* p. 290–291.
- Silverajan B, Ocak M, Nagel B. 2018. Cybersecurity attacks and defences for unmanned smart ships. *IEEE ICC.* p. 15–20.
- Sinigaglia F, Carbone R, Costa G, Ranise S. 2020. MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols. 2nd International Workshop on Emerging Technologies for Authorization and Authentication (ETAA). Luxembourg.
- Solnor P, Volden O, Fossen T. 2022. Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field. *J Field Robot.* 39(5):631–649. doi:10.1002/rob.22068.
- Suleski T, Ahmed M, Yang W, Wang E. 2023. A review of multi-factor authentication in the internet of healthcare things. *Digital Health.* 9(1).20552076231177144 (Article number). doi:10.1177/20552076231177144
- Sworna Z, Babar M, Sreekumar A. 2023a. IRP2API: Automated Mapping of Cyber Security Incident Response Plan to Security Tools' APIs. *IEEE International Conference on Software Analysis Evolution and Reengineering.* Macao, Peoples republic of China.
- Sworna Z, Islam C, Babar M. 2023b. Apiro: A framework for automated security tools API recommendation. *ACM Trans Softw Eng Methodol.* 32(1). 24 (article number). doi:10.1145/3512768
- Symes SW, Fairclough S, Wang J, Yang Z, Blanco-Davis E. 2022. Simulator based human performance assessment in a ship engine room using functional near-infrared spectroscopy. Liverpool: Liverpool John Moores University.
- Tam K, Jones K. 2018. Cyber-risk assessment for autonomous ships. *An International Conference on Cyber Security and Protection of Digital Services.*
- Thakur K, Kopecky S, Nuseir M, Ali M, Qiu M. 2016. An Analysis of Information Security Event Managers. 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCLOUD). New York.
- The International Maritime Organisation (IMO). 2019. *Imo.org.* Retrieved October 2023, from <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx#:~:text=Maritime%20cyber%20risk%20refers%20to,being%20corrupted%2C%20lost%20or%20compromised>.
- Tidy J. 2023. *BBC News - Technology.* Retrieved November 2023, from <https://www.bbc.co.uk/news/technology-66998064>.
- Titov A, Barakat L, Kovalev O. 2019. Risk assessment of operating unmanned ships. *Mar Intell Technol.* 4(4):11–23.

- Tusher H, Munim Z, Nazir S. 2022. Cyber security risk assessment in autonomous shipping. *Mar Econ Logist.* 24(2):208–227. doi:10.1057/s41278-022-00214-0.
- Uçtu G, Alkan M, Dogru I, Dörterler M. 2021. A suggested testbed to evaluate multicast network and threat prevention performance of next generation firewalls. *Future Gen Comput Syst.* 124(1):56–67. doi:10.1016/j.future.2021.05.013.
- Vagale A. 2022. Evaluation simulator platform for extended collision risk of autonomous surface vehicles. *J Marine Sci Eng.* 10(5):10–14. doi:10.3390/jmse10050705.
- Vagale A, Bye R, Fossen T. 2021a. Path planning and collision avoidance for autonomous surface vehicles II; a comparative study of algorithms. *J Mar Sci Technol.* 26(4):1307–1323. doi:10.1007/s00773-020-00790-x.
- Vagale A, Bye R, Fossen T. 2021b. Path planning for autonomous surface vehicles II: a comparative study of algorithms. *J Mar Sci Technol.* 26(4):1307–1323. doi:10.1007/s00773-020-00790-x.
- Walter M, Barrett A, Walker D, Tam K. 2023. Adversarial AI testcases for maritime autonomous systems. *AI Comput Sci Robot Technol.* 1. doi:10.5772/ACRT.15
- Wang Q, Wang D. 2023. Understanding failures in security proofs of multi-factor authentication for mobile devices. *IEEE Trans Inf Forensics Secur.* 18(1):597–612. doi:10.1109/TIFS.2022.3227753.
- Xu M, Guo J, Yuan H, Yang X. 2023. Zero-Trust security authentication based on SPA and endogenous security architecture. *Electronics (Basel).* 12(4). 782 (article number). doi:10.3390/electronics12040782
- Yoo J, Jo Y. 2023. Formulating cybersecurity requirements for autonomous ships using SQUARE methodology. *Sensors.* 11(1). Chapter 23.
- Yoo Y, Park H. 2021. Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ships. *J Mar Sci Eng.* 6:9.
- Zaccone R, Martelli M. 2020. A collision avoidance algorithm for ship guidance applications. *J Mar Eng Technol.* 19:62–75. doi:10.1080/20464177.2019.1685836.
- Zaid B, Sayeed A, Bala P, Alshehri A, Alanazi A, Zubair S. 2023. Toward secure and resilient networks: A zero-trust security framework with quantum fingerprinting for devices accessing network. *Mathematics.* 11(12). 2653 (article number). doi:10.3390/math11122653.
- Zhou X, Liu Z, NI S. 2018. Collision risk identification of autonomous ships based on the synergy ship domain. 2018 *CCDC.* Beijing.
- Zhou X, Liu Z, Wu Z. 2021. A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Eng.* 222. doi:10.1016/j.oceaneng.2021.108569.