TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 20
Number 1
March 2026

DOI: 10.12716/1001.20.01.25

SAFE-MASS Sociotechnical Array Framework for Evolving Maritime Autonomous Surface Ships

B. Praestegaard Larsen, P. Rauffet & D. Espes
Southern Brittany University, Lorient, France

ABSTRACT: This paper explores the sociotechnical risk management challenges faced by Maritime Autonomous Surface Ships (MASS) with an emphasis on cybersecurity. As the maritime sector increasingly embraces autonomous vessels to enhance efficiency and safety, it confronts new cybersecurity vulnerabilities and challenges. The paper outlines a comprehensive approach to identifying and mitigating cyber risks by examining the sociotechnical considerations within MASS. It underscores the importance of understanding how cyber threats can compromise the interaction between humans and systems, potentially impacting vessel operations performance and safety. Through a detailed description of the Sociotechnical Array Framework for Evolving Maritime Autonomous Surface Ships (SAFE-MASS), which functions as a sociotechnical transition taxonomy, and by explaining how this can be used for securing MASS this research contributes valuable insights into developing safer and more efficient maritime operations, signaling a trans-formative shift in the industry's future, especially by examining information technology (IT) and operational technology (OT) integration within MASS highlights the critical need for robust cybersecurity measures in this emerging field.

1 INTRODUCTION

As Maritime Autonomous Surface Ships (MASS) reshape the global maritime domain, traditional approaches to cybersecurity risk assessment prove insufficient in capturing the complex interplay between human, technical, and organizational elements. This paper introduces the Sociotechnical Array Framework for Evolving Maritime Autonomous Surface Ships (SAFE-MASS) not merely as a descriptive taxonomy, but as a novel analytic tool designed to operationalize sociotechnical cybersecurity thinking across all levels of MASS autonomy. The key innovation lies in how the framework enables systematic integration of both IT and OT threat landscapes with human-system interaction and regulatory dimensions. By explicitly addressing how sociotechnical variables influence cybersecurity posture and decision-making across the IMO's four Levels of Autonomy (LoA), SAFE-MASS facilitates anticipatory and adaptive risk management. This framework empowers stakeholders, designers, regulators, and operators to better identify and mitigate vulnerabilities that emerge from increasingly automated task-sharing between humans and machines. Through a use-case scenario, we illustrate not only how the framework can be applied in practice, but also how it improves efficiency and effectiveness in securing evolving maritime systems. Ultimately, SAFE-MASS contributes a much-needed lens for understanding and governing the cybersecurity challenges inherent to the digital transition of maritime transport.

2 CHALLENGES AND INDUSTRIAL NEEDS FOR MANAGING SOCIOTECHNICAL CYBER RISKS OVER THE DIFFERENT LEVELS OF MASS AUTONOMY

Maritime shipping is a favored mode of transport, notably accounting for 90% of global international trade (Baumler et al., 2021; Bui and Nguyen, 2021; Christiansen et al., 2020; Jacq et al., 2018; Jiang et al., 2018; Kosowska-Stamirowska et al., 2016; Sharma et al., 2019; Stannard, 2020; Tam and Jones, 2019a; Zhang et al., 2023). Furthermore, it is estimated that between 80-90% of all incidents involving maritime vessels can be attributed to Human Factors (HF), either directly or indirectly (Chang et al., 2021). Considering this, it's hardly surprising that the maritime sector is keenly looking forward to embracing autonomous vessels. This innovation is viewed as a strategic move to shape the future of maritime operations (Ahvenjärvi, 2016). The idea of having uncrewed vessels trafficking our oceans is already a reality (Stepien´, 2023; Xu et al., 2023). Undoubtedly, the future of the maritime shipping industry will not be anything even close to where it is today (Sencila, 2019).

The maritime industry is undergoing a transformative shift with the increasing adoption of Maritime Autonomous Surface Ships (MASS) (Kim et al., 2020). MASS are envisioned as vessels that can operate without onboard crews, utilizing advanced technologies such as sensors, Artificial Intelligence (AI), and sophisticated communication systems for autonomous navigation and task execution (Deling et al., 2020; Felski and Zwolak, 2020). While these advancements promise to enhance operational efficiency, safety, and sustainability, they simultaneously introduce a range of cybersecurity challenges that threaten vessel integrity, navigation accuracy, and overall maritime security (Tabish and Chaur-Luh, 2024). Unlike traditional crewed vessels, MASS relies on a complex interplay of Information Technology (IT) and Operational Technology (OT), making them particularly susceptible to cyber threats that can disrupt critical operations (Murray et al., 2017). One of the pressing cybersecurity concerns for MASS is their reliance on Global Navigation Satellite Systems (GNSS), including the Global Positioning System (GPS), the Vessel Integrated Navigation System (VINS), and the Automatic Identification System (AIS) (Tabish and Chaur-Luh, 2024). These systems provide essential data for navigation, collision avoidance, and route optimization (Androjna and Perkovič, 2021). These autonomous vessels are being designed to function across diverse maritime environments, including commercial shipping, military operations, and scientific research (Barrera et al., 2021; Kim et al., 2020). MASS technology is in its early developmental stages (Li and Fung, 2019), it holds significant potential to revolutionize the maritime industry by reducing operational costs, enhancing efficiency, and improving safety standards (Horne, 2021).

One of the key advantages of MASS is their ability to operate continuously without the need for crew rest periods or rotations. This capability could significantly increase the speed and efficiency of cargo transport while simultaneously reducing the risk of accidents caused by human error (Chang et al., 2021; Rødseth et al., 2023). The versatility of MASS is evident in their various forms, ranging from small drones and unmanned surface vessels (USVs) to large cargo ships and naval vessels (Barrera et al., 2021). The applications of MASS are diverse, encompassing cargo transport, ocean research, surveillance and security operations, and environmental monitoring (Komianos, 2018)). The development of MASS is being spearheaded by countries at the forefront of maritime research, including Norway, South Korea, and China (Lind et al., 2021; Munim and Haralambides, 2022). International organizations such as the IMO have been actively discussing MASS since 2017 in official meetings (Fonseca et al., 2021; Larsen and Lund, 2021; Pietrzykowski and Hajduk, 2019). Research institutions (Abilio Ramos et al., 2019; Fonseca et al., 2021), including the Norwegian University of Science and Technology (NTNU), are contributing significantly to MASS development (Kim et al., 2020). Major companies like Rolls-Royce and Kongsberg are also driving innovation in this field (Kim et al., 2020; Komianos, 2018). While the growth and adoption of MASS technology are expected to continue, the rate and model of growth vary considerably among different nations (World Maritime University, 2019).

MASS is vulnerable to cyber-attacks such as GPS spoofing, jamming, and data manipulation, which can lead to erroneous positioning, misrouted voyages, or even direct collisions (Androjna et al., 2020). AIS, which has been a standard installation on vessels worldwide since 2002, lacks authentication mechanisms, making it susceptible to data injection attacks that can mislead autonomous decision-making processes (Balduzzi et al., 2014). The Electronic Chart Display and Information System (ECDIS), an essential tool for digital navigation, presents another cybersecurity risk (Svilicic et al., 2019b). A compromised ECDIS system can manipulate nautical chart data, obscuring obstacles or falsifying depth readings, leading to potential grounding or collision hazards (Androjna and Perkovič, 2021). The Integrated Bridge System (IBS), which interconnects multiple navigation and control systems, further compounds these risks, as it provides a single point of failure that cyber attackers can exploit to manipulate multiple vessel functions simultaneously (Awan and Al Ghamdi, 2019). The shift towards remote monitoring and control in higher Levels of Autonomy (LoA) introduces additional vulnerabilities (Ramos et al., 2020b). Remotely operated MASS rely on secure and continuous data exchange between the vessel and shore-based control centers (Constanta Maritime University et al., 2022). These communication channels are prime targets for cybercriminals seeking to intercept, disrupt, or manipulate data transmissions (Tabish and Chaur-Luh, 2024). Attacks on the Heading Control System (HCS) or Bridge Alert Management System (BAMS) could cause a vessel to veer off course or prevent critical alerts from reaching human operators, undermining safe navigation (Tam et al., 2012).

The integration of AI-driven decision-making within MASS increases the risk of adversarial attacks targeting machine-learning models (Lee and Lee, 2023). By exploiting weaknesses in these algorithms, cyber attackers could alter a vessel's decision-making logic, resulting in hazardous operational behavior (Longo et al., 2024). The absence of onboard crew in

fully autonomous vessels further complicates cybersecurity risk mitigation, as immediate human intervention is no longer feasible in case of an attack (Walter et al., 2023).

2.1 *Challenges*

This shift towards MASS is largely motivated by the critical role that maritime shipping plays in global commerce, underscored by its substantial contribution to international transport (Komianos, 2018). The move to autonomy promises to reduce human error, which is a major cause of maritime incidents (Wróbel et al., 2017). While this technological advancement presents opportunities for safer and more efficient operations, it simultaneously introduces significant vulnerabilities, especially concerning cybersecurity (Kavallieratos et al., 2019). Autonomous vessels, with their reliance on advanced digital systems, remote communication, and software, are increasingly exposed to cyber threats (Tam and Jones, 2019b). These threats could undermine the safety, and efficiency gains that MASS aims to deliver (Bolbot et al., 2019).

With the extensive material provided by the IMO (2021) MSC.1/Circ.1638 document and the exhaustive exploration made within this about evaluating how different regulatory instruments are affected by changes of the LoA for the MASS, these documents serve as a core resource. The documents hold a huge amount of dependencies between different regulatory International Maritime Organization (IMO) instruments, and the IMO (2021) MSC.1/Circ.1638 document considers all the IMO regulatory instruments, which should specifically be taken into consideration before the advancement of MASS between levels. These regulatory documents have been analyzed for gaps by the Maritime Safety Committee, and the results are presented within the MSC.1/Circ.1638 document (IMO, 2021). The gaps are addressed in the form of recommendations on how to improve the different regulatory instruments to amend for MASS. In this, certain sociotechnical aspects have been considered, such as the absence of personnel on higher MASS levels, and relationships between personnel and automated processes on lower MASS levels.

2.2 *Existing frameworks*

The BIMCO Guidelines (BIMCO, 2020) offer practical recommendations for maritime cybersecurity, including risk assessments and mitigation strategies. However, they fall short in addressing the sociotechnical complexities arising from increasing autonomy in MASS. Similarly, the IMO Maritime Safety Committee highlights the need to retain a human master for oversight across all autonomy levels (IMO, 2023), acknowledging legal and jurisdictional challenges of Remote Operating Centers (ROC) and calling for further research into sociotechnical aspects. The SOLAS Convention (IMO, 2009) does not explicitly require cybersecurity measures or offer a holistic sociotechnical framework, though it implies broader safety practices that could encompass cybersecurity. The IMO Code of Practice (Boyes and Isbell, 2017) supplements this by offering cybersecurity guidance to ship operators.

Svilicic et al. (2019a) presents a cyber risk assessment of the training ship Fukaemaru using crew interviews and Nessus Professional scans. The study reveals critical vulnerabilities, especially in ECDIS, due to outdated software. It underscores the importance of robust cybersecurity policies, crew training, and ongoing evaluations. While focused on conventional ships, it does not address autonomous levels, centering instead on cybersecurity management and technological vulnerabilities aboard vessels.

Tam and Jones (2018a) explores the evolving cyber-risk landscape for autonomous ships, emphasizing the need to identify key vulnerabilities. It introduces the MaCRA (Maritime Cyber Risk Assessment) framework, tailored to maritime environments, and considers its application to autonomous vessels. Case studies of near-future prototypes reveal critical threats tied to system interconnectivity and satellite reliance. As the article predates MSC.1/Circ.1638 (IMO, 2021), it adopts SAE levels of automation adapted from the automotive sector, instead of the IMO's now-standardized levels.

Erstad et al. (2023) article does not mention autonomous surface ships levels instead it introduces a maritime cyber incident response framework, called the Cyber Emergency Response Procedure (CERP), which focuses on guiding crew members through the response process in the event of a cyber incident.

Fenton and Chapsos (2023) discusses the essential skills and competencies required to operate autonomous ships securely and even though the article supports the sociotechnical risk perspective by emphasizing the need for operator training and adaptation to evolving cybersecurity challenges, it lacks the overarching holistic view.

Emad and Ghosh (2023) does not primarily focus on cyber risks, instead, it centers on the skills and competencies required for shore-based operators of unmanned and autonomous ships, as well as the challenges faced in maritime education and training (MET) to prepare for these advancements, while it discusses the technological changes associated with automation in the maritime industry and mentions the need for technical competencies related to these systems, it does not explicitly delve into cyber risks.

Issa et al. (2022) analyzes regulatory responses to cybersecurity threats in autonomous shipping and emphasizes the role of communication system security within the sociotechnical risk categories of MASS. Poornikoo and Øvergård (2022) addresses regulatory challenges in implementing MASS and the necessity to align cybersecurity measures with international maritime laws. IMO (2021) discusses the gradual adaptation required in HMI as ships move through different LoA, supporting the need for risk models like SAFE-MASS.

While existing maritime cybersecurity frameworks contribute significantly, they fall short in addressing the sociotechnical challenges of Maritime Autonomous Surface Ships (MASS). The BIMCO Guidelines offer practical advice but overlook issues like human oversight, remote operations, and automation complexities (BIMCO, 2020). Similarly, the IMO Maritime Safety Committee report stresses the need for human involvement but inadequately covers

sociotechnical risks such as those linked to Remote Operating Centers and cognitive workload (IMO, 2023). SOLAS and related IMO guidelines outline general safety measures but lack a holistic, sociotechnical cybersecurity approach (IMO, 2009). Risk models like MaCRA and CERP focus on manned vessels or are outdated, while studies on operator competencies emphasize training without fully integrating cyber governance. As autonomy advances, cybersecurity must shift from human-machine to machine-to-machine security (Hamad and Steinhorst, 2023), demanding a new framework that bridges technological and human factors. This includes addressing AI-driven decisions, evolving operator roles, and ensuring continuous upskilling for managing integrated autonomous systems (Hollnagel and Woods, 2005).

2.3 *Problem statement*

In the context of cybersecurity for MASS, it's crucial to perform comprehensive risk evaluations and apply robust risk management practices (Kanwal et al., 2022; Kim et al., 2020; Lee and Lee, 2024). These steps are essential for pinpointing possible cyber threats, assessing their impact, and crafting suitable countermeasures to mitigate them (Alcaide and Llave, 2020; Boyes and Isbell, 2017). The initial phase in cybersecurity sociotechnical risk management for MASS involves identifying potential cyber risks and vulnerabilities by examining the ship's technological setup, network, software, communication systems, and possible threat avenues (Mednikarov et al., 2020). The main purpose of this is to understand how cyber-attacks, threats and vulnerabilities might affect human-system interactions and by doing compromises the performance, and maybe even the safety, of specific vessel operations (Kechagias et al., 2022; Martínez et al., 2024; Yu et al., 2023). Following such risk identification, an analysis must be carried out to determine the potential impact and probability of these risks as the human-machine interaction transfers more toward machine than human, evaluating how cyber incidents could affect MASS's safety, potential crew, cargo, and the environment, alongside the likelihood of such risks occurring based on the current autonomous levels, the threat environment, which security measures are in place, and identified system weaknesses (Kim et al., 2020).

In conducting a review based upon the outcome presented within the IMO (2021) MSC.1/Circ.1638 document, there are a few obvious considerations which needs to be addressed. The SOLAS Convention primarily focuses on the physical safety aspects of maritime vessels, including construction, fire protection, life-saving appliances, navigation safety, carriage of cargoes, and more. The convention does not explicitly address cybersecurity concerns, particularly those unique to autonomous or remotely operated vessels. The maritime industry's increasing reliance on networked systems for vessel operations makes it a prime target for cybercriminals and nation-state actors (Li et al., 2024). As MASS becomes more prevalent, the integration of digital and operational technologies necessitates not only advanced technical defenses but also a rethinking of organizational policies and global collaboration (Palbar Misas et al., 2024). The complexity of these systems requires cross-disciplinary approaches that factor in geopolitical risks and the growing sophistication of cyberattacks targeting critical infrastructure (Sarker, 2024a; Shafqat and Masood, 2016). The trajectory of MASS development underscores the importance of aligning technical innovations with practical operational frameworks (Fonseca et al., 2021; Zhang et al., 2023).

The research presented in this article on sociotechnical cyber risk management for MASS underscores several critical gaps and emerging challenges that merit significant attention from the scientific and technological communities. This research is driven not only by the necessity to enhance maritime transport but also by the urgent need to address the cybersecurity risks that accompany the transition to autonomous systems. By exploring the cybersecurity challenges and potential vulnerabilities that MASS face, particularly in light of their interaction with HFs, this study aims to contribute to a more secure and resilient future for maritime operations. The focus on the intersection between autonomy, human elements, and cyber threats underscores the need for a comprehensive approach to ensure the safe integration of MASS into global shipping networks (Hogg and Ghosh, 2016).

3 DEVELOPMENT OF A TAXONOMY FOR CHARACTERIZING SOCIOTECHNICAL CYBER RISKS

This section outlines the methodological foundation for the SAFE-MASS framework, detailing the key structuring dimensions, system decomposition, levels of autonomy, and the interaction between human operators and automated systems. By analyzing existing cybersecurity frameworks, regulatory guidelines, and technological constraints, SAFE-MASS is positioned as a comprehensive taxonomy for evaluating cyber risks across different levels of autonomy. This describes the core elements of this methodology, including risk assessment strategies, IT/OT integration, and the sociotechnical considerations necessary for secure and resilient MASS operations.

3.1 *Literature review methodology*

Though broad in scope, the taxonomy is designed to provide a focused and structured approach to understanding and mitigating cybersecurity risks in MASS across different autonomy levels. To support this, an extensive literature review was conducted, drawing from academic research, industry reports, and regulatory sources on cyber threats, human-system interaction, legal frameworks, and technological vulnerabilities. The outcome is a coherent framework built on recurring themes and strategies to guide both analysis and practical application.

The taxonomy is structured as a matrix integrating eight dimensions, including IT/OT systems, location, HMI, human factors, vessel functions, cyber risks, regulatory considerations, and technological solutions. Each dimension includes specific elements to define risk attributes, for example, operator workload and

training in the human domain, data integrity and redundancy in technology, and compliance or certification issues in regulation. This structure allows for a comprehensive analysis of vulnerabilities across autonomy levels.

The matrix's cells represent the interaction between dimensions, autonomy levels, and operational scenarios, each highlighting specific vulnerabilities, contextual factors, and related mitigation strategies. These range from technical controls like encryption and intrusion detection, to human-focused measures such as training, and organizational actions including audits and incident response planning. By linking each risk to practical safeguards, the taxonomy serves as both an analytical and prescriptive tool. It offers a structured approach to cybersecurity in MASS, mapping risks and countermeasures across sociotechnical dimensions.

3.1.1 *Keyword Selection*

To ensure a comprehensive review, a combination of primary keywords (directly related to the research focus) and secondary keywords (supporting broader topics such as cybersecurity frameworks, risk assessment, and maritime regulations) were utilized. These search terms were chosen based on their relevance to the evolving cybersecurity challenges in MASS.

Primary Keywords: Maritime Autonomous Surface Ships, Autonomous Ships Cybersecurity, Sociotechnical Risk Management in MASS, Cyber Threats in Autonomous Maritime Operations, Human-Machine Interaction in MASS, Operational Technology security in Maritime, Information Technology integration in MASS.

Secondary Keywords: MASS Regulatory, Cyber Risk Assessment in Maritime Industry, Artificial Intelligence in Autonomous Shipping, Levels of Autonomy in Maritime Transport, GPS Spoofing and Jamming in Marine Navigation, Human Factors in Maritime Cybersecurity, Remote Operation Centers

3.1.2 *Source Selection Criteria*

The articles were selected based on several parameters. Priority was given to research published between 2020-2025 to ensure up-to-date cybersecurity risk analysis in MASS. Foundational works predating this period were also included to establish a theoretical and regulatory background. Peer-Reviewed Sources such as Journals, conference proceedings, and also books were prioritized, ensuring scientific rigor. Industry standards and guidelines like official documents from IMO, BIMCO, and other maritime regulatory bodies were reviewed to understand cybersecurity policies relevant to MASS. Cross-Disciplinary Studies of articles incorporating insights from cybersecurity, automation, AI, and human factors were also included to maintain a holistic perspective.

3.1.3 *Database and Search Engines Utilized*

A wide range of specific academic and industry-recognized databases was used for this. Scopus, IEEE Xplore, ScienceDirect, Google Scholar and also specific material such as IMO and BIMCO Publications, for regulatory and industry guidelines.

3.1.4 *Search Query Structure*

The search queries combined Boolean operators to refine results. An example of a structured query used would be as follows (”Maritime Autonomous Surface Ships” OR ”MASS”) AND (”cybersecurity” OR ”cyber risk management”) AND (”human machine interaction” OR ”human factors”) AND (”GPS spoofing” OR ”remote operations”). Numerous different variations of this query and similar ones were executed and adjusted based on specific search engines to retrieve the relevant results.

3.1.5 *Article Screening and Selection*

The article ”How to Read a Paper” by Keshav (2007) was instrumental in shaping the article screening and selection process for this study. The three-pass reading method provided a structured approach to evaluating research papers efficiently, ensuring that only the relevant and high-quality sources were incorporated into the SAFE-MASS framework.

This initial step was used to rapidly assess each paper's relevance by examining the title, abstract, introduction, section headings, and conclusion. This allowed for the identification of whether a paper was related to key themes such as MASS cybersecurity, IT/OT integration, regulatory frameworks, or HMI. Papers that lacked relevance or were outside the research scope were discarded at this stage.

For papers that passed the first screening, a more detailed review was conducted, focusing on figures, key arguments, and supporting evidence. At this stage, particular attention was paid to whether the research methods, datasets, and assumptions aligned with the objectives of the SAFE-MASS framework.

The final stage involved a deep analysis of selected papers, critically evaluating methodologies, identifying potential biases, and cross-checking findings with existing regulatory documents (e.g., IMO's MSC.1/Circ.1638). This pass ensured that the research findings were not only relevant but also methodologically sound and directly applicable to the risk assessment and cybersecurity strategies of MASS.

3.2 *Identification of the key dimensions and proposal of a taxonomy to characterize sociotechnical cyber risks in MASS*

The taxonomy visually represented in Figure 1 is a synthesis of the key dimensions identified through the review of relevant literature. It is therefore crucial for succeeding in this endeavor, as it delineates the organizational structure necessary for navigating the cybersecurity landscape of MASS. This taxonomy serves as a foundational framework that categorizes and articulates the interdependencies among various components, including human factors, technological systems, and regulatory considerations, within the context of different LoA. By systematically organizing these elements, the taxonomy enhances the understanding of potential vulnerabilities and facilitates targeted risk assessment and management strategies.

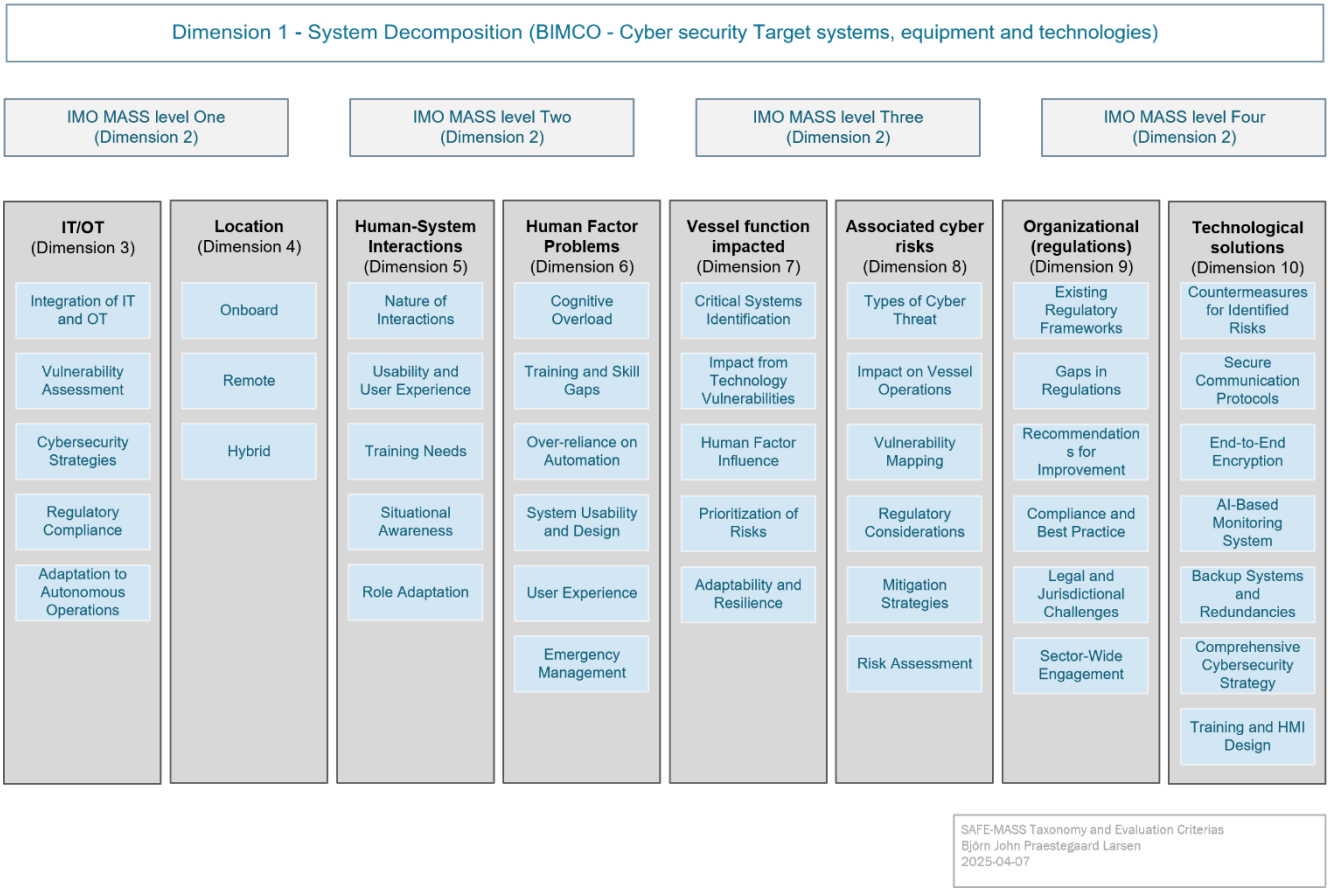

Figure 1. SAFE-MASS Taxonomy and Evaluation Criterias

3.2.1 *Dimension 1 - System decomposition*

To provide actionable insights for vessel operators, this study uses the BIMCO (2020) as an industry standard for identifying IT/OT vulnerabilities, forming the basis for analyzing HMI and human factor issues across MASS LoA. Emphasis is placed on maintaining Confidentiality, Integrity, and Availability (CIA). Each BIMCO-listed vulnerability was evaluated across the IMO (2021) LoA levels, relevant IT/OT functions, and operational domains, recognizing that some vulnerabilities shift or vanish as autonomy evolves. System decomposition is key in this context, breaking down complex ship systems to assess vulnerabilities and interdependencies among components like navigation, communication, and automation. This enables targeted cybersecurity assessments and highlights how human interactions affect system exposure.

3.2.2 *Dimension 2 - LoA and consideration of MASS as an evolving system overtime*

The transition to MASS involves a step-by-step approach through the various LoA, allowing for adaptations in technology, regulations, and HMI (da Conceição et al., 2017; Liu et al., 2022). Each level of autonomy presents unique challenges and opportunities (Burmeister et al., 2014). Addressing critical aspects such as cybersecurity (Tam and Jones, 2018a), remote operation capabilities (Ramos et al., 2020b), and the evolving role of human operators (Mallam et al., 2020). MASS represent a future objective for the maritime industry, following a technological roadmap that incorporates various LoA (Rødseth et al., 2022). This transition to MASS is not an immediate shift but requires the maritime domain to implement and adapt to different LoAs progressively (Poornikoo and Øvergård, 2022).

There are numerous different standards for how to define different LoA's, Sheridan (1992) established a standard based on ten levels of robotic autonomy, the Bureau

Veritas establishes in the guidance note NI64DTRO1E "Guidelines for Autonomous Shipping", describing the transition from manual to automatic, named A0 to A4 (Veritas, 2019). Hoem et al. (2018) defines five distinct LoA. The conference paper titled "Marine autonomous surface ship - Control system configuration" by Zubowicz et al. (2019) proposes a hierarchical LoA for MASS. Another conference paper titled "Characterization of Autonomy in Merchant Ships" by Jan Rødseth et al. (2018) a detailed outline over six levels is presented. There are indeed many standards available, SINTEF Ocean Institute and Rødseth et al. (2022) published an article namned "Levels of autonomy for ships" which lists seven LoAs for MASS and there has been versions of Sheridan (1992) definitions made that even incorporated half levels. The role of human operators in MASS evolves with each Level of Autonomy (LoA) (da Conceição et al., 2017; Grech et al., 2008; Lyons et al., 2021). At lower LoAs, they are actively involved in navigation and decision-making, with human-automation teaming as a design goal (Vianello et al., 2023), requiring deep operational understanding and quick decision-making skills (Lundberg and Johansson, 2021; Tolone, 2014).

As autonomy increases, operators shift to supervisory roles, intervening only when necessary (Barosz et al., 2020; Lundberg and Johansson, 2021), which enhances human-robot team performance (Chinchilla-Rodriguez et al., 2018; Conner et al., 2018; Deoker et al., 2015). This transition demands updated competencies (Fergusson, 2022). Industry 4.0 technologies (e.g., IoT, Big Data, Cloud Computing) enable high automation but also challenge workforce development (Ibidapo, 2022; Nardelli, 2022; Raja Santhi and Muthuswamy, 2023; Yang and Gu, 2021). As production systems evolve, so must organizational structures and skillsets (Emad and Ghosh, 2023; Saniuk et al., 2023; Vermeulen et al., 2018).

Table 1. IMO MASS levels as specified within the document MSC.1/Circ.1638 IMO (2021).

MASS LoA / Characteristics on task control sharing			
Degree one	Degree two	Degree three	Degree four
Ship with automated processes and decision support. Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.	Remotely controlled ship with seafarers on board. The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.	Remotely controlled ship without seafarers on board. The ship is controlled and operated from another location. There are no seafarers on board.	Fully autonomous ship. The operating system of the ship is able to make decisions and determine actions by itself

The MSC.1/Circ.1638 document (IMO, 2021), based on the IMO's Regulatory Scoping Exercise, defines four LoA categories and serves as the internationally recognized benchmark for MASS. Adopting this standard ensures regulatory alignment. Figure 2 outlines core IMO considerations, including the cybersecurity implications of rising autonomy. While SOLAS addresses physical safety, it lacks specific cybersecurity guidance, especially for remote or autonomous operations. As LoAs advance, HMI design must evolve accordingly, reflecting deeper shifts in human-machine responsibility (Goerlandt, 2020; Poornikoo and Øverg˚ard, 2022).

As autonomy increases, HMI must evolve to maintain situational awareness and ensure operational continuity (da Concei¸c˜ao et al., 2017).

- LoA 1–2 (Onboard Presence): At these stages, HMI systems are designed to complement human activities onboard, providing intuitive alerts and visual feedback that enhance rather than overwhelm the crew. According to insights from the SAFE-MASS framework, avoiding issues such as information overload or interface-induced miscommunication is crucial.
- LoA 3 (Remote Control): The HMI must support remote monitoring by delivering enhanced visualizations, real-time system status updates, and contextual feedback. These features help remote operators maintain an accurate mental model of the ship's operational context despite being physically distant.
- LoA 4 (Full Autonomy): At this stage, the HMI should prioritize clarity, summarization of key situational data, and streamlined alerts that allow human intervention from the Shore Control Center (SCC) when necessary. Ensuring that overrides are intuitive and actionable becomes essential for preserving safety under autonomous operations.

Cybersecurity management must evolve with each LoA. At LoA 2, challenges involve supporting active onboard operators, while at LoA 4, autonomous systems must handle critical decisions independently. This progression underscores the need for scalable, adaptive HMI systems that align with advancing technologies and regulatory demands (Endsley, 2017; Veitch and Andreas Alsos, 2022).

3.2.3 *Dimension 3 - IT/OT*

Cybersecurity risks onboard ships are commonly framed through the division of Information Technology (IT) and Operational Technology (OT) systems (Larsen and Lund, 2021). IT governs information systems, while OT controls physical devices (IMO, 2022). Though OT is traditionally tied to cyber safety, its integration with IT places both under broader cybersecurity concerns (Androjna et al., 2020). These systems are often remotely managed and monitored by third parties, adding layers of complexity (Kala and Balakrishnan, 2019). Figure 2 visualizes this IT/OT interface, highlighting the exchange of knowledge and data. Autonomous vessels, in this context, function as massive floating robots reliant on tightly coupled IT/OT systems (Ramos et al., 2020b).

Figure 2. The IT/OT intangible area (Praestegaard Larsen, 2022).

In maritime cybersecurity, the interplay between Human Factors (HFs) and HumanMachine Interfaces (HMI) becomes increasingly complex across LoA in MASS (Broek et al., 2020; Pollini et al., 2022; Poornikoo and Øverg˚ard, 2022; Simões-Marques et al., 2021; Ye et al., 2023). At lower LoAs, where human input is prominent, HMIs must support rapid, informed decisions through intuitive design and clear cybersecurity alerts (Martíınez et al., 2024; Ramos et al., 2020a,b; Ren et al., 2023). As autonomy grows, operators shift to supervisory roles, raising concerns about maintaining situational awareness and cybersecurity responsiveness with reduced direct control (Akter et al., 2022; Martínez et al., 2024; Tam and Jones, 2019c). At the highest LoAs, the key challenge is ensuring effective remote monitoring and timely human intervention (Androjna et al., 2021; Reggiannini et al., 2019). MASS across different LoAs demand secure communication systems to enable timely operator response to threats (Xu et al., 2020). Striking a balance between automation and human input is essential for effective cybersecurity and safe operations (Androjna et al., 2020; Chan et al., 2022; Martínez et al., 2024; Poornikoo and Øvergård, 2022). The IT/OT convergence, especially in HMI design,

introduces distinct cybersecurity challenges at each autonomy level (see Table 2). As autonomy increases, human roles shift toward oversight, requiring continuous training to manage complex, integrated systems (Hollnagel and Woods, 2005).

Table 2. IT/OT Acceleration of complexity for increasing autonomy within MASS.

MASS LoA / Cybersecurity challenge			
Degree one	Degree two	Degree three	Degree four
IT/OT focuses on enhancing efficiency and safety through automation with human oversight.	IT/OT becomes critical to prevent unauthorized access or manipulation of ship controls.	IT/OT amplified for all operational aspects, demanding higher cybersecurity protection.	IT/OT demands unparalleled cybersecurity defenses to protect against complex threats

Integration of IT and OT The framework emphasizes the importance of understanding how IT systems (which manage information and data) and OT systems (which control physical processes and equipment) interact. As vessels become more autonomous, the integration of these two systems becomes critical for ensuring operational safety and cybersecurity (Bolbot et al., 2020).

Vulnerability Assessment Evaluating IT/OT focuses on identifying specific vulnerabilities that arise when these systems are interconnected. For instance, cyber threats such as data spoofing, tampering, or unauthorized access can affect both IT and OT environments, leading to safety risks and operational failures (Karamperidis et al., 2021). The framework outlines potential flaws that may emerge when these systems overlap.

Cybersecurity Strategies The SAFE-MASS framework outlines cybersecurity strategies for securing IT and OT integration, emphasizing encrypted data exchange and secure communication protocols. These measures become increasingly critical as autonomy levels rise, helping to prevent cyberattacks and ensure system integrity (Sarker, 2024a).

Regulatory Compliance Ensuring that both IT and OT systems adhere to regulatory standards is crucial. The framework highlights the need for compliance with international regulations, such as those set by the IMO, which helps standardize the safety and security measures across both domains as technology progresses (IMO, 2022).

Adaptation to Autonomous Operations As vessels transition through different levels of autonomy, the roles and functionalities of both IT and OT systems must be evaluated and adapted accordingly (Haugli-Sandvik et al., 2024). This includes considering how operator interactions with these systems change as processes become more automated, maintaining operational integrity and safety (Endsley, 2017). Through addressing these aspects, the SAFE-MASS framework provides a structured approach to understanding and managing the risks associated with the convergence of IT and OT.

3.2.4 *Dimension 4 - Location*

Location provides information about where systems and vulnerabilities are situated, specifying whether they are onboard the vessel, remote, or a hybrid combination. This categorization provides understanding where risks and problems can manifest, which helps in designing effective mitigation strategies and safety measures for MASS (Tam and Jones, 2019b). The evaluation of location involves identifying and categorizing technological components and vulnerabilities based on their physical or operational presence, it is assessed through the following locations.

Onboard the Vessel This involves evaluating systems and components that are physically located on the ship itself.

Remote This pertains to systems that are managed and operated from a location away from the vessel, such as remote control centers.

Hybrid This includes scenarios where systems involve a mix of both onboard and remote components, which can introduce different vulnerabilities and challenges.

By categorizing location in this way, the SAFE-MASS framework aims to provide a thorough understanding of where potential risks and problems can occur, which is crucial for designing effective mitigation strategies and safety measures for MASS

3.2.5 *Dimension 5 - Human-System Interactions*

This dimension focuses on the interaction between human operators and automated systems, examining HMI usability, efficiency, and user experience. It assesses whether system design effectively supports decision-making and operational control (Gauthier et al., 2019; Liu et al., 2022; Veitch and Andreas Alsos, 2022). Human-system interactions are evaluated through several key considerations, which assess how operators engage with automated systems on maritime vessels. Here are the main aspects of human-system interactions.

Nature of Interactions This captures how operators interact with HMI and automated systems. Measuring the efficiency and effectiveness of these interactions, focusing on how well the systems support human decision-making and operational control helps in decisions within risk assessment (Parhizkar et al., 2022b).

Usability and User Experience Evaluating the usability of the systems involves looking at the complexity of the interfaces and how they affect the operator's ability to manage tasks and respond to emergencies. This includes identifying potential issues that could arise from poor design, such as cognitive overload or unnecessary complexity.

Training Needs Understanding the interactions also involves recognizing the training requirements for operators to handle automated systems effectively. Determining if operators are adequately trained to interact with and monitor the system, particularly under different levels of autonomy helps identify potential risks (Emad and Ghosh, 2023).

Situational Awareness The interaction evaluation focuses on ensuring that operators maintain situational awareness. Something that is of outmost importance and means that they have a clear understanding of the system's status and operational context, especially in

automated or partially automated environments (Sharma et al., 2019).

Role Adaptation As autonomy levels change, the roles of human operators also change, from direct control to supervisory roles (Lynch et al., 2024). This requires an assessment of the skills and competencies needed for operators to adjust to these evolving responsibilities. By examining these aspects of human-system interactions, the SAFE-MASS framework aims to ensure that operators can interact effectively with both autonomous and automated systems, thus enhancing safety and operational efficiency.

3.2.6 *Dimension 6 - Human Factor Problems*

This section identifies specific issues that human operators might face while interacting with automated systems, such as cognitive overload, improper training, or over-reliance on automation (Monsaingeon et al., 2021). These problems are often linked to system design and user interface complexity, which can impact situational awareness and the ability to manage emergencies (Hollnagel and Woods, 2005). The SAFE-MASS framework focuses on identifying specific issues that human operators might face while interacting with automatic systems in MASS.

Cognitive Overload This aspect assesses whether operators are subjected to excessive information or task demands, which could impair their decision-making abilities. Human factors research suggests that too much information or rapidly changing conditions can overwhelm operators, leading to potential mistakes or delays in response (Parhizkar et al., 2022a).

Training and Skill Gaps The framework examines whether operators receive adequate training to handle the complexities of automated and semi-autonomous systems. Issues may arise due to insufficient understanding of system functionalities, operational protocols, or how to manage unexpected scenarios, which can directly impact safety and operational efficiency (Pseftelis and Chondrokoukis, 2021).

Over-reliance on Automation As systems become more automated, there is a risk that operators may become overly dependent on these technologies, leading to skill degradation (Ramos et al., 2018). The evaluation identifies concerns related to operators losing situational awareness and the ability to intervene effectively when necessary.

System Usability and Design This evaluates how well the design of human machine interfaces (HMIs) supports user interactions. Poorly designed HMIs can lead to misunderstandings or errors in operation, emphasizing the need for intuitive designs that enhance usability and reduce the potential for error (Hoem et al., 2022).

User Experience The overall user experience is assessed through feedback on the interactions operators have with both automated systems and HMIs. This includes understanding their satisfaction, comfort level, and perceptions of safety while operating these systems.

Emergency Management The framework looks at how well operators are prepared to handle emergencies, particularly under automated conditions. Training and system design should support effective responses to unexpected incidents, ensuring operators can manage crises efficiently and maintain safety (Liu et al., 2022). By evaluating these human factor problems, the SAFE-MASS framework identifies necessary improvements in training, system design, and operational protocols, ensuring that human operators can perform effectively and safely as the maritime industry increasingly adopts autonomous technologies.

3.2.7 *Dimension 7 - Vessel Function Impacted*

The SAFE-MASS framework identifies how technological and human factors impact key vessel functions, such as navigation, collision avoidance, and propulsion, enabling targeted risk assessments and prioritization of critical systems for mitigation (Li et al., 2012; Ronca et al., 2023).

Critical Systems Identification The framework identifies which essential functions of the vessel are influenced by both OT and HF. This includes key systems such as navigational controls, collision avoidance mechanisms, propulsion systems, and environmental controls (Gauthier et al., 2019).

Impact from Technology Vulnerabilities It examines how vulnerabilities within IT and OT systems can negatively impact vessel functions. For instance, if cybersecurity threats compromise the navigation system, this could lead to incorrect positioning or routing decisions, potentially resulting in hazardous situations like collisions or grounding (Hareide et al., 2018; Rajaram et al., 2022).

Human Factor Influence The assessment also looks at how human factors, such as operator error, miscommunication, or cognitive overload, can disrupt the functionality of vessel systems. Understanding these influences can highlight vulnerabilities in human-technology interactions that may affect overall operational safety (Zhang et al., 2020).

Prioritization of Risks By identifying which vessel functions are impacted by technology and human factors, the framework allows organizations to prioritize risk assessments. This ensures that critical systems receive the necessary attention in terms of security measures, training, and operational protocols to mitigate potential disruptions (Li et al., 2024).

Adaptability and Resilience The impact evaluation emphasizes the need for systems to be designed with adaptability in mind. It aims to ensure that as vessel functions become more automated, they remain resilient, allowing for smooth transitions and minimizing risks during operational changes or unexpected incidents (Kim et al., 2020; Rødseth et al., 2023).

By systematically assessing the vessel functions impacted by both technology and human factors, the SAFE-MASS framework aids in enhancing the design, security, and operation of maritime autonomous systems, ensuring that operational reliability and safety are maintained as autonomy levels increase.

3.2.8 *Dimension 8 - Associated Cyber Risks*

This dimension focuses on potential cyber threats related to the identified technologies and human interactions. It includes risks such as unauthorized

access, data breaches, GPS spoofing, jamming, and malware attacks. Understanding these risks is essential for developing a comprehensive cybersecurity strategy that ensures the secure operation of both IT and OT systems (Karamperidis et al., 2021).

Types of Cyber Threats The framework outlines various cyber threats that vessels face, including unauthorized access to systems, data breaches, GPS spoofing, jamming, and malware attacks. Recognizing these threats is essential for developing a comprehensive cybersecurity strategy that protects both IT and OT systems (Androjna and Perkovič, 2021).

Impact on Vessel Operations Each identified cyber risk is analyzed in terms of how it might disrupt vessel operations. For example, GPS spoofing could lead to misnavigation, while malware attacks on navigation systems could compromise operational integrity, posing significant safety risks (Bielawski and Lazarowska, 2021).

Vulnerability Mapping The framework emphasizes the importance of mapping out vulnerabilities associated with specific technologies and human interactions. This includes analyzing potential weak points in IT and OT integrations that cyber threats could exploit to gain control over or disrupt critical vessel functions (Kim et al., 2020).

Regulatory Considerations The framework also highlights the need to adhere to regulatory guidelines that address cybersecurity in maritime operations. This includes compliance with international standards set by the IMO to ensure that vessels are equipped to mitigate potential cyber risks effectively (Androjna et al., 2020).

Mitigation Strategies For each associated cyber risk, the SAFE-MASS framework suggests relevant technological solutions and best practices. This may include implementing redundancy systems, such as backup communication pathways, end-to-end encryption, and AI-based monitoring systems to enhance resilience and ensure the secure operation of vessel systems (Tam and Jones, 2018b).

Risk Assessment The framework advocates for ongoing risk assessments that evaluate how emerging cyber threats could impact autonomous shipping. By continuously updating risk profiles and response strategies, maritime organizations can better prepare for and defend against potential cyber incidents (Tam and Jones, 2019b).

Through this comprehensive examination of associated cyber risks, the SAFE-MASS framework provides a structured approach to enhance the cybersecurity posture of vessels, ensuring that as autonomy levels increase, risks are effectively managed to maintain safety and operational integrity.

3.2.9 *Dimension 9 - Organizational (Regulations)*

The regulatory frameworks applicable to the technology, HFs, and vessel operations. It includes international maritime regulations like those set by the IMO, which ensure that ships comply with safety and cybersecurity standards. This regulatory perspective helps organizations align their operations with global best practices to enhance safety and security (Hopcraft and Martin, 2018).

Existing Regulatory Frameworks The framework identifies relevant international and national regulations that apply to MASS, such as those established by the IMO. These regulations provide guidelines on safety, cybersecurity, and operational standards essential for the safe functioning of autonomous vessels (Parlov, 2023).

Gaps in Regulations The SAFE-MASS framework addresses gaps identified in current regulatory documents regarding the transition to higher levels of autonomy. The evaluation underscores areas where existing regulations may not adequately cover the specific challenges posed by automation or neglect sociotechnical aspects of vessel operations. For instance, the absence of personnel on fully autonomous vessels raises questions about oversight and accountability (Verdiesen et al., 2021).

Recommendations for Improvement Based on the identified gaps, the framework discusses recommendations for amending existing regulatory instruments to better accommodate MASS. This includes proposing changes that take into account human factors, technology integration, and the evolving landscape of maritime operations as they increase in autonomy.

Compliance and Best Practices The framework emphasizes the importance of aligning organizational operations with global best practices outlined in regulatory documents. This alignment helps organizations enhance safety and security while ensuring that their practices reflect current technological advancements and operational complexities (Kanwal et al., 2022).

Legal and Jurisdictional Challenges The SAFE-MASS framework highlights the legal and jurisdictional challenges associated with remote operations and how these impact regulatory compliance. It raises awareness about the need for clarity on the roles of remote operators and the legal implications of operating autonomous vessels across different jurisdictions (IMO, 2023).

Sector-Wide Engagement The framework advocates increased collaboration among stakeholders, regulatory bodies, maritime industry representatives, and technology developers, to ensure that regulations evolve to meet the needs of an increasingly autonomous shipping landscape. Engaging multiple sectors can facilitate the sharing of insights and best practices, leading to more comprehensive and effective regulations (Ventikos et al., 2020). By effectively addressing these organizational and regulatory considerations, the SAFE-MASS framework supports a structured approach to governance in the maritime sector, ensuring that regulations keep pace with technological advancements and contribute to safer and more efficient maritime operations.

3.2.10 *Dimension 10 - Technological Solutions*

Technological solutions are detailed in this dimension as countermeasures for the risks identified earlier. It includes recommendations for redundancy systems, such as backup communication pathways, end-to-end encryption, and AI-based monitoring systems. These solutions are designed to address both technical and cyber risks, ensuring that vessels

maintain operational integrity even in compromised scenarios.

Countermeasures for Identified Risks The framework details various technological solutions designed to counter the cyber risks previously identified. These measures include strategies such as implementing redundancy systems, which ensure that if one system fails or is compromised, alternative systems can maintain vital operations (Olsen, 2024).

Secure Communication Protocols Creating robust communication systems is critical. The framework emphasizes the need for secure communication protocols that prevent unauthorized access and safeguard data integrity during the transmission of information between vessel systems, especially in remote operations (Lee and Lee, 2024; Tran et al., 2021).

End-to-End Encryption To protect sensitive data from interception or unauthorized access, the framework recommends the use of end-to-end encryption. This technology safeguards the information being communicated between onboard systems and external operators, making it difficult for potential attackers to exploit vulnerabilities (Sarker, 2024a; Yaacoub et al., 2022).

AI-Based Monitoring Systems The incorporation of AI for monitoring and responding to cyber threats is highlighted as an essential technological solution (Sarker, 2024b). AI can be used to detect anomalies in system behavior or network traffic, facilitating timely interventions and augmenting human oversight in operational settings.

Backup Systems and Redundancies Implementing backup communication pathways and systems ensures continuity of operation even in adverse conditions or following a cyber attack. The framework stresses the importance of having alternative means of communication and control to enhance resilience (Sarker, 2024b; Tzavara and Vassiliadis, 2024).

Comprehensive Cybersecurity Strategy The framework advocates for developing a comprehensive cybersecurity strategy that encompasses IT and OT systems, ensuring that security measures are integrated throughout the technological landscape of the vessel. This strategic approach helps organizations address the multifaceted nature of cybersecurity risks in a holistic manner (Stoynov and Nikolov, 2021).

Training and HMI Design In addition to technological solutions, research underscores the importance of designing effective HMI that enhance operator situational awareness (Debernard et al., 2016; Parhizkar et al., 2022b). Training programs should be established to ensure that operators are well-prepared to understand and manage the complexities introduced by automated systems (Liu et al., 2022). By incorporating these technological solutions, the SAFE-MASS framework aims to improve the cybersecurity of MASS, ensuring that technological advancements are aligned with safety, operational integrity, and regulatory compliance in the maritime domain.

4 BUILDING OF THE SAFE-MASS FRAMEWORK, AND EXAMPLE OF USE FOR PRACTITIONERS

SAFE-MASS is a sociotechnical framework that integrates human operators, automation, and cybersecurity across MASS autonomy levels. At lower LoAs, it prioritizes intuitive HMI design and real-time alerts to support situational awareness and decision making, while targeted training builds operator trust and competence. By preserving manual control, the framework ensures readiness for both routine and emergency scenarios as autonomy progresses.

4.1 *SAFE-MASS*

The SAFE-MASS framework moves beyond conventional siloed approaches by offering an integrative taxonomy tailored to the evolving cybersecurity demands of MASS. Developed through a structured literature review and cross disciplinary collaboration, SAFE-MASS integrates key perspectives including system architecture, autonomy progression, human factors, risk assessment, and regulatory alignment. It draws from maritime standards, sociotechnical research, and cybersecurity practices to provide a comprehensive foundation for managing risks across all levels of autonomy. As demonstrated in figures 3 and 4, SAFE-MASS serves as a scalable blueprint for industry-wide adoption.

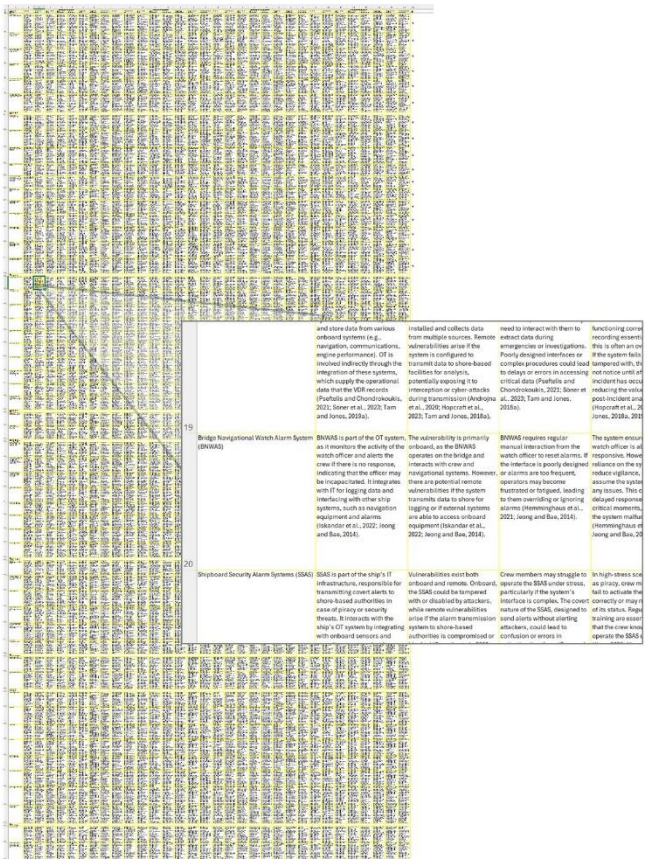

Figure 3. The SAFE-MASS matrix consisting of 1728 movements within LoA for BIMCO cybersecurity target systems, equipment and technologies.

Designed for flexibility, SAFE-MASS can be adapted to diverse maritime contexts, allowing stakeholders to proactively address emerging threats. Beyond immediate mitigation, SAFEMASS fosters a systems-thinking mindset by highlighting the

interdependencies among human, technical, and organizational elements. This holistic perspective is critical for integrating advanced technologies into existing maritime practices. As a practical tool, it supports comprehensive evaluation of vessel functions, operator roles, system reliability, and cybersecurity posture. To maximize its utility, understanding the structure of the framework, especially the organizational dimension, is essential, and the following section provides that detail.

The SAFE-MASS framework is accessible through GitHub. https://github.com/bjornplarsen/SAFE-MASS

4.2 *Example*

To illustrate the practical application of the SAFE-MASS framework, we will explore how it can be applied to Integrated Navigation Systems (INS) as a vessel transitions from LoA 1 to LoA 4. This detailed walkthrough highlights the evolving cybersecurity risks, human-system interactions, and technological adaptations at each stage of autonomy, providing a comprehensive view of how SAFE-MASS guides risk assessment.

4.2.1 *LoA 1 - Automated Processes with Human Operators Onboard*

At LoA 1, vessels operate with crews supported by automated systems for navigation, collision avoidance, and situational awareness. The goal is to enhance human decisionmaking while keeping manual control. Cyber threats mainly target data integrity and system availability, including GPS spoofing, data manipulation, and communication breaches. Operators depend on automation but must stay alert to anomalies, with cognitive overload being a major risk due to the need to monitor multiple systems. The SAFE-MASS framework advises redundant critical systems, secure communications, and user-friendly HMIs to reduce overload and improve awareness. Training emphasizes trust in automation, interpreting alerts, and regaining manual control when needed..

4.2.2 *LoA 2 - Semi-Autonomous Operations with Minimal Human Supervision*

At LoA 2, some operations are automated, with crew onboard but less involved in routine navigation. Humans intervene only when needed, shifting to supervisory roles. This increased automation brings risks to system integrity and remote access, as attackers may exploit decision-support systems or manipulate data. Over-reliance on automation can reduce situational awareness. Operators need new skills to monitor systems and respond to alerts. The SAFE-MASS framework recommends intuitive HMIs for quick status understanding and real-time data validation to ensure integrity. Training focuses on supervisory skills, enabling effective monitoring and timely intervention during failures or anomalies.

BIMCO - Cyber security Target systems, equipment and technologies

1. Communication Systems

Integrated communication systems

DEGREE ONE

IT/OT	Location	Human-System Interactions	Human Factor problems	Vessel function impacted	Associated cyber risks	Organizational (regulations)	Technological Solutions
Integrated communication systems impact both IT (information exchange, cybersecurity) and OT (operational control systems for shipboard functions) as they bridge information flow between systems critical for safe navigation and operations (Munim and Haralambides, 2022; Progoulakis et al., 2021).	The vulnerability is mainly onboard, as seafarers rely on integrated systems to communicate with shore-based entities, but there is also a remote aspect due to satellite or radio communication links (Ko and Song, 2021; McGillivary,2018; Oruc, 2022).	Human-computer interaction issues such as over-reliance on automated com munication systems may lead to complacency. Misunderstanding or misuse of the interfaces can exacerbate these issues during high-stress situations or when managing high volumes of data (Johansson et al., 2023; Melo et al., 2023; Veitch and Andreas Alsos, 2022).	Operators may experience decreased situational awareness as they over-rely on automated decision support. A lack of training on system failures could delay the ability to regain manual control during emergencies (Johansson et al., 2023; Lynch et al., 2024).	Integrated communication systems are critical to navigation and collision avoidance. If these systems are compromised, it can hinder effective co ordination between ship and shore or other vessels, affecting safe navigation (Ko and Song, 2021; Munim and Haralambides, 2022; Zhang et al., 2021).	Potential cyber risks include unauthorized access, jamming, or denial-of-service attacks targeting weak encryption or unpatched software vulnerabilities, com promising communications or allowing adversaries to intercept sensitive infor mation (van de Poel, 2020; Sarker, 2024).	IMO regulations, such as those outlined in the SOLAS Convention and the IMO guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3), require robust communication protocols and cybersecurity measures to safeguard integrated systems from unauthorized access or attacks (IMO, 2022; Johansson et al., 2023; McGillivary, 2018).	End-to-end encryption of communication channels, regular patching of soft ware, and implementation of anomaly detection systems are essential. Fur ther, redundant communication pathways and continuous cybersecurity train ing for crew members should be adopted to mitigate these risks (van de Poel, 2020; Sarker, 2024b; Tam and Jones, 2018; Tran et al., 2021).

DEGREE TWO

IT/OT	Location	Human-System Interactions	Human Factor problems	Vessel function impacted	Associated cyber risks	Organizational (regulations)	Technological Solutions
The vulnerability affects both IT and OT, but remote control elements heighten the importance of IT systems for secure and stable communication between the ship and remote control centers (Androjna et al., 2020; Guo et al., 2022; Utne et al., 2020).	Vulnerabilities exist in both onboard and remote systems due to the hybrid nature of control. Remote access introduces additional security challenges such as protecting satellite or radio communication links (Caprolu et al., 2020; IMO, 2023).	Remote operators may face challenges due to communication delays or inac curacies in the transmitted data, impacting decision-making in critical scenar ios. Additionally, ambiguity about control distribution between onboard crew and remote operators can create confusion during emergencies (Goerlandt, 2020).	Seafarers onboard might struggle with reduced authority or decision-making power when relying on remote operators. In a situation where communication fails, seafarers might not be sufficiently trained to assume control quickly, especially if they are unfamiliar with manual operations (Utne et al., 2020; Vakil, 2022).	Loss of communication could disrupt the command and control structure between the remote operator and the ship, leading to failures in navigation, emergency response, or safe handling of the vessel (Ramos et al., 2020; Zhou et al., 2021).	With the additional attack surface created by remote operations, vulnerabilities such as man-in-the-middle attacks or spoofing are more pronounced. If an attacker intercepts communication, they could manipulate or disrupt vessel operations, posing serious safety risks (Bolbot et al., 2020; Caprolu et al., 2020).	In this degree, compliance with IMO cyber risk management guidelines (MSC FAL.1/Circ.3) is vital to secure remote communication links. Organizations must implement redundancy in communication channels and strict access control to safeguard remote operations (IMO, 2022; Johansson et al., 2023; Kim et al., 2020; McGillivary, 2018).	Implementing multi-layered security protocols including firewalls, encryption, and intrusion detection systems (IDS) is essential. Continuous monitoring of remote systems and regular cybersecurity training for both remote operators and onboard crew are critical to maintaining secure communication (McGillivary, 2018; van de Poel, 2020).

DEGREE THREE

IT/OT	Location	Human-System Interactions	Human Factor problems	Vessel function impacted	Associated cyber risks	Organizational (regulations)	Technological Solutions
This vulnerability impacts both IT and OT, with a heavier emphasis on IT. The absence of seafarers onboard means that all control and monitoring are done remotely, increasing reliance on communication networks and cybersecurity of IT systems (Barrera et al., 2021; Goerlandt, 2020).	The vulnerability is primarily remote since no crew is onboard. The integrity of satellite, radio, and other remote communication channels is critical to maintaining operational control from a remote control center (Guo et al., 2022; IMO, 2021; Utne et al., 2020).	Operators rely solely on remote data for decision-making, and latency or poor data transmission can lead to incomplete situational awareness. The inability to directly obseve and control the vessel may increase cognitive workload, requiring operators to process and interpret data from various systems in real time (Ramos et al., 2020a; Utne et al., 2020).	Without physical presence on the vessel, remote operators must respond to alarms or anomalies from a distance, which may delay real-time actions in case of emergencies like cyber-attacks or system malfunctions. This dependency on automated alerts reduces human flexibility in reacting to unforeseen issues (Ramos et al., 2020a; Utne et al., 2020).	The core functions impacted include navigation, propulsion control, and safety management. Loss of communication or control due to a cyber-attack could completely disable the vessel's operations. Since there is no crew onboard, all recovery must happen through remote channels, which can be difficult if attackers disrupt IT or OT functions simultaneously (IMO, 2021; Ko and Song, 2021).	This level introduces significant risks such as man-in-the-middle attacks, signal jamming, or control system takeovers. The lack of human presence onboard makes physical intervention impossible, leaving the vessel highly vulnerable to cyber-attacks, remote hijacking, or spoofing of communication channels (Goerlandt, 2020; Munim and Haralambides, 2022).	Adherence to the IMO's Maritime Cyber Risk Management guidelines (MSC-FAL.1/Circ.3) is critical. Additionally, redundancy in communication systems and robust encryption protocols must be enforced to prevent unauthorized access. Regulatory frameworks must also consider incident response plans for remotely operated ships, including shore-based cybersecurity measures (Johansson et al., 2023; Kanwal et al., 2022; Stoynov and Nikolov, 2021).	A multi-layered defense approach is essential, including encrypted communication channels, real-time anomaly detection, and network segmentation to isolate operational and information systems. AI-driven security monitoring and enhanced redundancy are also necessary to detect and respond to any cyber incidents in real-time (Humayun et al., 2020; Longo et al., 2022; Munim and Haralambides, 2022).

DEGREE FOUR

IT/OT	Location	Human-System Interactions	Human Factor problems	Vessel function impacted	Associated cyber risks	Organizational (regulations)	Technological Solutions
In fully autonomous ships, the vulnerability primarily affects OT, as the ship's systems independently manage navigation, propulsion, and communication. However, IT is also critical because autonomous decision-making systems rely on algorithms, sensors, and data from external sources (Akpan et al., 2022; Ramos et al., 2020b; Zhou et al., 2021).	The vulnerability is both onboard and remote. Onboard systems must autonomously detect, process, and respond to operational changes, while remote monitoring systems must verify and audit decisions made by the autonomous system. Weaknesses in either can be exploited by cyber attackers (Munim and Haralambides, 2022; Refsdal et al., 2015).	With full autonomy, human operators only intervene during system audits or rare crisis scenarios. This minimizes direct human-system interaction, but it introduces problems related to trust in the automation, lack of transparency in decision-making processes, and challenges in maintaining situational awareness from afar (Parhizkar et al., 2022; Ramos et al., 2020b)	Human involvement in fully autonomous systems typically comes into play during remote monitoring or override scenarios. The lack of continuous human oversight can lead to issues when the system encounters unforeseen problems, such as novel cyber threats or environmental conditions not accounted for by the algorithms (Lynch et al., 2024).	Navigation, propulsion, collision avoidance, and environmental monitoring are completely dependent on the autonomous systems. A failure in the system's decision-making capability due to a cyber-attack or sensor spoofing could lead to collisions, grounding, or environmental incidents (Kanwal et al., 2022; Kim et al., 2022; Munim and Haralambides, 2022).	Autonomous vessels are highly susceptible to sophisticated attacks such as data manipulation, sensor spoofing, and AI-based attacks where adversaries manipulate input data to mislead the decision-making algorithms. Additionally, malware or ransomware attacks on the vessel's IT/OT systems could lead to total loss of control (Ben Farah et al., 2022; Sarker, 2024b; Tam and Jones, 2018)	The regulatory frameworks for fully autonomous vessels must include rigorous testing and validation of autonomous algorithms. Compliance with cyber risk management guidelines must be upheld, and there should be international coordination to handle incidents affecting autonomous vessels. Organizations must also implement regulations around liability in the event of cyber-related incidents (Kanwal et al., 2022; Lynch et al., 2023; World Maritime University, 2019).	Strong AI-driven cybersecurity mechanisms, such as machine learning-based intrusion detection, are essential. Autonomous systems should also include self-healing capabilities to restore operations after an attack. End-to-end encryption of all data traffic and highly sophisticated backup communication channels must be implemented to maintain control integrity (Sarker, 2024b).

Figure 4. An example of how the SAFE-MASS evolves Intergrated Communication Systems from LoA1 to LoA4

4.2.3 *LoA 3 - Remotely Controlled Operations with No Crew Onboard*

At LoA 3, vessels are remotely operated from a Shore Control Center (SCC) with no crew onboard, making communication and system integrity vital. Key risks include communication loss, signal interception, and remote manipulation. Attacks on communication channels can cause control loss or misread navigational data. Operators must maintain situational awareness from a distance, supported by HMIs that provide clear, comprehensive data. The SAFE-MASS framework recommends encrypted communication, real-time monitoring, and AI-based anomaly detection. Training focuses on remote operation skills, including managing data latency, communication delays, and complex remote interactions.

4.2.4 *LoA 4 - Fully Autonomous Operations with Minimal Human Intervention*

At LoA 4, in fully autonomous operations, the vessel navigates and manages itself without onboard crew, with minimal human oversight through remote intervention. This autonomy introduces sophisticated threats like AI manipulation, sensor spoofing, and system-wide cyberattacks targeting decision-making. Systems must be resilient and self-sufficient. Human involvement centers on monitoring system health and responding to critical alerts. HMIs must provide clear summaries and escalate issues effectively. The SAFE-MASS framework recommends AI-driven cybersecurity (e.g., self-healing, AI-based threat detection), strong system redundancy, and integrated anomaly detection. Training focuses on emergency interventions, understanding autonomy limits, and remote cyber incident response.

4.2.5 *Conclusion of the Example*

The SAFE-MASS framework offers a structured pathway for addressing the diverse challenges faced by INS as vessels transition through different LoA. By systematically identifying cybersecurity threats, human factors, and technological solutions, SAFE-MASS ensures that risks are mitigated at each stage of automation. The framework provides guidance on the design and implementation of secure systems, training programs, and operational protocols, ultimately facilitating the safe integration of autonomous technologies in the maritime sector.

4.3 *Usage*

The SAFE-MASS framework offers a comprehensive, multidimensional approach to addressing the sociotechnical challenges of MASS, enhancing cybersecurity, safety, and operational efficiency. It supports the progression from LoA 1 (automated with crew) to LoA 4 (fully autonomous) by guiding the development of HMI, HF practices, and regulatory compliance. As operations become more remote, SAFE-MASS emphasizes secure communication, real-time situational awareness, and operator training to manage challenges such as data latency and cognitive workload.

At full autonomy, the framework highlights the need for AI-driven cybersecurity, resilient systems, and continued human oversight from Remote Operations Center (ROC). It promotes redundancy, encryption, and effective alert mechanisms to counter threats like GPS spoofing and data manipulation. SAFE-MASS also adapts to the four operational modes: Onboard (crew-operated), Hybrid (remotely controlled with onboard crew), Remote (fully controlled from an ROC), and Auto (fully autonomous with no human input). Each mode presents unique vulnerabilities that shift with increasing autonomy, requiring tailored mitigation strategies.

In early autonomy levels (LoA 1-2), the focus is on reducing fatigue and human error through workload management. At higher levels (LoA 3-4), the framework supports protocols that prevent cognitive overload and guide emergency response through well designed interfaces and automated support systems. Human-centered design, iterative development, and continuous training ensure that operators can intervene effectively across all autonomy levels.

As a practical and adaptable tool, SAFE-MASS enables maritime stakeholders to assess and manage cybersecurity risks while aligning human and technological capabilities. Its flexible structure allows customization for various operational needs, making it a valuable resource for improving resilience and ensuring safe adoption of autonomous technologies across the maritime industry.

4.3.1 *System Providers*

System providers can utilize the SAFE-MASS matrix as a blueprint for designing and developing security features in autonomous systems. By understanding the different Levels of Autonomy (LoA) defined in the framework, providers can assess which vulnerabilities are pertinent to their technologies and address these in the design phase. The framework emphasizes the importance of human factors and operational contexts, enabling providers to create user interfaces that enhance operator decision-making and situational awareness, thus reducing the likelihood of human error. System providers can also use the SAFE-MASS framework to ensure that their products comply with industry regulations and standards. This proactive approach can streamline the certification process and position the provider as a leader in cybersecurity solutions in the maritime sector.

4.3.2 *Vessel Managers*

Vessel managers can implement the SAFE-MASS framework to conduct thorough risk assessments that integrate both technological systems and human factors. By applying the framework, they can identify specific vulnerabilities associated with their vessels' autonomous systems and develop tailored mitigation strategies. The SAFEMASS framework underscores the significance of training programs that enhance crew proficiency in handling both automated and manual operations. Vessel managers can use the framework to design training initiatives that prepare their staff for emergencies, ensuring smooth operations even during high-pressure situations. The framework provides guidance on developing operational protocols that account for varying levels of autonomy. This ensures that vessel managers can create clear procedures for

transitioning between automated and manual control, thereby enhancing safety and compliance.

4.3.3 *Ship Classification Auditors*

Ship classification auditors can utilize the SAFE-MASS framework as a comprehensive assessment tool to evaluate vessels against cybersecurity and safety standards. The modular structure allows auditors to examine each component of the vessel's systems and operations, thereby ensuring compliance with international and national regulatory guidelines. By referencing the matrix and the associated best practices outlined in the SAFE-MASS framework, auditors can provide actionable recommendations to ship operators. This can help highlight areas for improvement, enhance overall cybersecurity measures, and ensure a holistic approach to maritime safety. The framework encourages a cycle of continuous feedback and improvement, allowing auditors to assist organizations in adapting to emerging technologies and evolving cyber threats as MASS capabilities advance.

5 DISCUSSION

This research fills a critical gap by introducing a comprehensive sociotechnical framework, the SAFE-MASS, tailored to the cybersecurity challenges of MASS. Traditional maritime risk management has largely focused on technical measures such as encryption and redundancy, often overlooking HFs and HMI design. SAFE-MASS addresses this imbalance by integrating these elements into the core of cybersecurity strategies, ensuring human oversight remains central even as autonomy increases. The framework identifies specific vulnerabilities and risks associated with each LoA, offering a roadmap for implementing targeted countermeasures. This approach bridges the gap between technology-centric solutions and human-centered resilience, promoting not only technical security but also operational safety. Its sociotechnical orientation ensures that transitions across LoA's are systematic, building on a foundation that enhances situational awareness, system integrity, and trust in automation.

Beyond the core framework, several additional considerations are critical. Autonomous navigation depends entirely on sensor and GPS data, making it vulnerable to spoofing or tampering, which could lead to misinterpretation or unsafe maneuvers. Ensuring the authenticity and integrity of this data is therefore vital. As autonomy increases, particularly at LoA 4 where no crew are onboard, cybersecurity risks intensify. Remote control systems must be secured against threats such as signal interception, data manipulation, and unauthorized access. The integration of OT and IT systems introduces further complexity. OT systems, once isolated, are now networked for remote monitoring and maintenance, requiring robust cybersecurity measures to maintain operational safety. Additionally, human operators, whether onboard or remote, must receive updated cybersecurity training, including threat recognition and incident response.

Effective HMI design is also essential. As human roles shift from direct control to supervisory oversight, interfaces must support situational awareness and enable rapid response to incidents. Research is needed to optimize these interfaces and strengthen human-machine collaboration as autonomy advances. Remote controlled and autonomous vessels are especially exposed to risks like signal disruption or spoofing. This underscores the importance of fault-tolerant communication systems and secure control protocols to prevent operational failure. Regulatory standards must evolve to address these challenges across all autonomy levels, as current frameworks remain insufficiently prepared for the full scope of MASS operations.

Looking forward, the SAFE-MASS framework can serve as a foundation for establishing industry-wide cybersecurity benchmarks. Its integration into regulatory guidelines and design standards can help the maritime sector adopt a comprehensive and forward-looking approach to secure, resilient, and scalable autonomous operations.

5.1 *Positioning the SAFE-MASS Framework*

The SAFE-MASS risk assessment framework presents a comprehensive approach to addressing the cybersecurity challenges faced by MASS. Unlike existing frameworks, such as the BIMCO guidelines and the IMO Maritime Safety Committee recommendations, SAFE-MASS not only emphasizes technical and regulatory components but also integrates sociotechnical aspects crucial for managing the complexities of increasing autonomy in maritime operations.

While the BIMCO guidelines (BIMCO, 2020) offer practical guidance for implementing cybersecurity measures, they primarily focus on risk assessments and mitigation strategies without adequately addressing the interplay between human oversight, remote operations, and automated decision-making. The limitations highlighted in this document underscore the shortfalls of current frameworks, which tend to overlook the evolving nature of human-machine interactions and the cognitive workload of operators in autonomous environments. By explicitly incorporating human factors into its risk assessment methodology, SAFE-MASS aims to bridge this gap and provide a more holistic evaluation of vulnerabilities.

Moreover, the existing literature reflects a tendency to focus on compliance and general safety principles, often neglecting the dynamic risk landscape posed by the progressive automation of maritime systems. While frameworks like MaCRA (Tam and Jones, 2019b) and CERP (Erstad et al., 2023) contribute to risk assessment methodologies, they may be outdated or primarily applicable to manned operations, limiting their relevance to the rapidly evolving field of MASS. Fenton and Chapsos (2023) primarily focuses on compliance, technical safeguards, and cybersecurity protocols without fully incorporating the complex interplay between human factors, operational context, and evolving legal definitions.

SAFE-MASS also surpasses the Emad and Ghosh (2023) MET framework by offering a more comprehensive sociotechnical approach that explicitly

integrates human factors, regulatory alignment, and evolving maritime autonomy levels. While MET primarily focuses on technical risk assessment, SAFE-MASS addresses the dynamic interplay between operators, automation, and cybersecurity threats across all LoA.

This positions SAFE-MASS not merely as an academic construct but as an operational enabler for maritime stakeholders who must navigate increasingly complex cyber-risk environments.

5.2 *Limitations and Perspectives of the Research*

Despite its comprehensive nature, the SAFE-MASS framework is not without limitations. One primary limitation is the reliance on existing data and literature, which may not fully capture the emergent risks associated with novel technologies and operational paradigms in autonomous shipping. Therefore, continuous updates and real-world case studies will be crucial to ensuring the adaptability and relevance of the framework.

While SAFE-MASS offers a structured approach to risk assessment, its implementation in diverse maritime contexts may face challenges due to varying regulatory environments and operational practices across different regions. The framework's adaptability to unique maritime operations will require collaborative efforts among stakeholders, including regulatory bodies, industry operators, and researchers. Looking forward, the SAFE-MASS framework presents several research opportunities and perspectives. Future studies could focus on validating and refining the framework through empirical research and case analyses of specific MASS implementations. Additionally, exploring the integration of emerging technologies such as AI and machine learning in the framework could enhance its predictive capabilities and responsiveness to evolving cyber threats.

In conclusion, the SAFE-MASS risk assessment framework seeks to advance the discourse in maritime cybersecurity by addressing limitations found in existing literature and offering a dynamic, integrated approach that emphasizes the critical interaction between technological systems and human operators. Through continuous iteration and stakeholder engagement, the framework intends to adapt and evolve with the needs of the maritime industry, fostering a more secure and resilient operational environment for autonomous vessels.

6 ETHICAL CONSIDERATIONS

Ethical principles provide a foundational framework for assessing the acceptability of research practices, particularly in the context of Maritime Autonomous Surface Ships (MASS) research. These principles are shaped by individual moral beliefs, regulatory frameworks, and sociocultural norms (Hamburg and Grosch, 2017). As the research landscape evolves, especially within cybersecurity and maritime autonomy, the necessity for stringent ethical guidelines becomes more pronounced (Navalta et al., 2019). This is particularly crucial given the integration of IT and OT within MASS, where ethical challenges intersect with technological advancements (Praestegaard Larsen, 2024).

The authors confirm that there are no known disputes regarding intellectual property rights associated with this research. Additionally, all data and findings presented in this work adhere to established best practices for citation, acknowledgment, and ethical dissemination of research outcomes.

REFERENCES

Abilio Ramos, M., Utne, I.B., Mosleh, A., 2019. Collision Avoidance on Maritime Autonomous Surface Ships: Operators' Tasks and Human Failure Events. Safety Science 116, 33-44, doi: https://www.doi.org/10.1016/j.ssci.2019.02.038

Ahvenjärvi, S., 2016. The Human Element and Autonomous Ships. TransNav : International Journal on Marine Navigation and Safety of Sea Transportation , 517–521. doi: https://www.doi.org/10.12716/1001.10.03.18

Akter, S., Uddin, M.R., Sajib, S., Lee, W.J.T., Michael, K., Hossain, M.A., 2022. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research, doi: https://www.doi.org/10.1007/s10479-022-04844-8.

Alcaide, J.I., Llave, R.G., 2020. Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia 45, 547–554, doi: https://www.doi.org/10.1016/j.trpro.2020.03.058.

Androjna, A., Brcko, T., Pavic, I., Greidanus, H., 2020. Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering 8, 776, number: 10 Publisher: Multidisciplinary Digital Publishing Institute, doi: https://www.doi.org/10.3390/jmse8100776

Androjna, A., Perkovič, M., 2021. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. Transactions on Maritime Science 10, 361–373, publisher: Sveučilište u Splitu, Pomorski fakultet, doi: https://www.doi.org/10.7225/toms.v10.n02.w08

Androjna, A., Perkovič, M., Pavic, I., Mišković, J., 2021. AIS Data Vulnerability Indicated by a Spoofing Case-Study. Applied Sciences 11, 5015, number: 11 Publisher: Multidisciplinary Digital Publishing Institute, doi: https://www.doi.org/10.3390/app11115015

Awan, M.S.K., Al Ghamdi, M.A., 2019. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). Journal of Marine Science and Engineering 7, 350, publisher: MDPI.

Balduzzi, M., Pasta, A., Wilhoit, K., 2014. A security evaluation of AIS automated identification system, in: Proceedings of the 30th Annual Computer Security Applications Conference, Association for Computing Machinery, New York, NY, USA. pp. 436–445. URL: https://dl.acm.org/doi/10.1145/2664243.2664257.

Barosz, P., Gol da, G., Kampa, A., 2020. Efficiency Analysis of Manufacturing Line with Industrial Robots and Human Operators. Applied Sciences 10, 2862. URL: https://www.mdpi.com/2076-3417/10/8/2862, number: 8 Publisher: Multidisciplinary Digital Publishing Institute.

Barrera, C., Padron, I., Luis, \.F., Llinas, O., 2021. Trends and Challenges in Unmanned Surface Vehicles (Usv): From Survey to Shipping. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 15.

Baumler, R., Arce, M.C., Pazaver, A., 2021. Quantification of Influence and Interest at IMO in Maritime Safety and Human Element Matters. Marine Policy 133, 104746. publisher: Elsevier.

Bielawski, A., Lazarowska, A., 2021. Discussing cybersecurity in maritime transportation. Maritime Technology and Research 4, 252151. Publisher: Faculty of International Maritime Studies.

BIMCO, B.a.I.M.C., 2020. The Guidelines on Cyber Security Onboard Ships URL: https: //www.bimco.org.
Bolbot, V., Theotokatos, G., Boulougouris, E., Vassalos, D., 2020. A novel cyber-risk assessment method for ship systems. Safety Science 131, 104908. URL: https://www.sciencedirect.com/science/article/pii/S0925753520303052.
Bolbot, V., Theotokatos, G., Bujorianu, L.M., Boulougouris, E., Vassalos, D., 2019. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. Reliability Engineering & System Safety 182, 179–193. URL: https://www.sciencedirect.com/science/article/pii/S0951832018302709,.
Boyes, H., Isbell, R., 2017. Code of Practice: Cyber Security for Ships. URL: https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/ code-of-practice-cyber-security-for-ships/.
Broek, J.H.v.d., Griffioen, J.R.J., Drift, M.M.v.d., 2020. Meaningful Human Control in Autonomous Shipping: An Overview. IOP Conference Series. Materials Science and Engineering 929. place: Bristol, United Kingdom Publisher: IOP Publishing.
Bui, V.D., Nguyen, H.P., 2021. A Comprehensive Review on Big Data-Based Potential Applications in Marine Shipping Management. International Journal on Advanced Science, Engineering and Information Technology 11, 1067–1077.
Burmeister, H.C., Bruhn, W., Rødseth, J., Porathe, T., 2014. Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: The MUNIN Perspective. International Journal of e-Navigation and Maritime Economy 1, 1–13. URL: https://www.sciencedirect.com/science/article/pii/S2405535214000035,
Chan, J.P., Norman, R., Pazouki, K., Golightly, D., 2022. Autonomous maritime operations and the influence of situational awareness within maritime navigation. WMU Journal of Maritime Affairs 21, 121–140. URL: https://doi.org/10.1007/s13437-022-00264-4.
Chang, C.H., Kontovas, C., Yu, Q., Yang, Z., 2021. Risk Assessment of the Operations of Maritime Autonomous Surface Ships. Reliability Engineering & System Safety 207, 107324.
Chinchilla-Rodriguez, Z., Miguel, S., Perianes-Rodriguez, A., Sugimoto, C.R., 2018. Dependencies and autonomy in research performance: examining nanoscience and nanotechnology in emerging countries. Scientometrics 115, 1485–1504. URL: https://doi.org/10.1007/ s11192-018-2652-7,
Christiansen, M., Hellsten, E., Pisinger, D., Sacramento, D., Vilhelmsen, C., 2020. Liner Shipping Network Design. European Journal of Operational Research 286, 1–20. publisher: Elsevier.
da Conceição, V.P., Dahlman, J., Navarro, A., 2017. What is maritime navigation? Unfolding the complexity of a Sociotechnical System. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 61, 267–271. URL: https://doi.org/10.1177/ 1541931213601549, publisher: SAGE Publications Inc.
Conner, D.C., Kohlbrecher, S., Schillinger, P., Romay, A., Stumpf, A., Maniatopoulos, S., Kress-Gazit, H., von Stryk, O., 2018. Collaborative Autonomy Between High-Level Behaviors and Human Operators for Control of Complex Tasks with Different Humanoid Robots, in: Spenko, M., Buerger, S., Iagnemma, K. (Eds.), The DARPA Robotics Challenge Finals: Humanoid Robots To The Rescue. Springer International Publishing, Cham. Springer Tracts in Advanced Robotics, pp. 429–494.
Constanta Maritime University, Zagan, R., Raicu, G., Constanta Maritime University, Sabau, A., Constanta Maritime University, 2022. Studies And Research Regarding Vulnerabilities Of Marine Autonomous Surface Systems (Mass) And Remotely Operated Vessels (Rovs)
From Point Of View Of Cybersecurity. International Journal of Modern Manufacturing
Technologies 14, 310–318. URL: https://ijmmt.ro/vol14no32022/46_Remus_Zgan.pdf,
Debernard, S., Chauvin, C., Pokam, R., Langlois, S., 2016. Designing Human-Machine Interface for Autonomous Vehicles. IFAC-PapersOnLine 49, 609–614. URL: https://www.sciencedirect.com/science/article/pii/S2405896316322418,
Deling, W., Dongkui, W., Changhai, H., Changyue, W., 2020. Marine autonomous surface Ship–a great challenge to maritime education and training. American Journal of Water Science and Engineering 6, 10–16.
Deoker, A.V., Meservy, T.O., Helquist, J., 2015. Creating and Sustaining Collaborative Efforts for Scientific Idea Exchange through Autonomy, Competence, and Relatedness, in: 2015 48th Hawaii International Conference on System Sciences, pp. 591–599. URL: https:// ieeexplore.ieee.org/document/7069726, iSSN: 1530-1605.
Emad, G.R., Ghosh, S., 2023. Identifying essential skills and competencies towards building a training framework for future operators of autonomous ships: a qualitative study. WMU Journal of Maritime Affairs 22, 427–445. URL: https://doi.org/10.1007/ s13437-023-00310-9,
Endsley, M.R., 2017. From Here to Autonomy: Lessons Learned From Human–Automation
Research. Human Factors 59, 5–27. URL: https://doi.org/10.1177/0018720816681350, publisher: SAGE Publications Inc.
Erstad, E., Hopcraft, R., Palbar, J.D., Tam, K., 2023. CERP: A Maritime Cyber Risk Decision
Making Tool. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 17. URL: https://pearl.plymouth.ac.uk/secam-research/796,
Felski, A., Zwolak, K., 2020. The Ocean-Going Autonomous Ship—Challenges and Threats. Journal of Marine Science and Engineering 8, 41. publisher: MDPI.
Fenton, A.J., Chapsos, I., 2023. Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS). Frontiers in Computer Science 5. URL: https://www.frontiersin.org/articles/10.3389/fcomp.2023.1151188/full, publisher: Frontiers Media S.A.
Fergusson, L., 2022. Learning by... Knowledge and skills acquisition through work-based learning and research. Journal of Work-Applied Management 14, 184–199. URL: https: //doi.org/10.1108/JWAM-12-2021-0065, publisher: Emerald Publishing Limited.
Fonseca, T., Lagdami, K., Schröder-Hinrichs, J.U., 2021. Assessing Innovation in Transport: An Application of the Technology Adoption (TechAdo) Model to Maritime Autonomous Surface Ships (MASS). Transport Policy 114, 182–195.
Gauthier, M., Kruithof, G., Narlis, C., Jolliffe, W.A.M., 2019. Control and automation systems onboard the vessel: Lessons in human-centered design learned from 20 years of marine occurrences in Canada. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 63, 1000–1004. URL: https://doi.org/10.1177/1071181319631066, publisher: SAGE Publications Inc.
Goerlandt, F., 2020. Maritime Autonomous Surface Ships from a risk governance perspective: Interpretation and implications. Safety Science 128, 104758. URL: https://www.sciencedirect.com/science/article/pii/S0925753520301557,
Grech, M., Horberry, T., Koester, T., 2008. Human Factors in the Maritime Domain. CRC Press, Boca Raton.
Hamad, M., Steinhorst, S., 2023. Security Challenges in Autonomous Systems Design. URL: http://arxiv.org/abs/2312.00018, arXiv:2312.00018 [cs].
Hamburg, I., Grosch, K.R., 2017. Ethical Aspects in Cyber Security. Archives of Business Research 5, 199–206. URL: https://doi.org/10.14738/abr.510.3818.
Hareide, O.S., Jøsok, , Lund, M.S., Ostnes, R., Helkala, K., 2018. Enhancing Navigator Competence by

Demonstrating Maritime Cyber Security. The Journal of Navigation 71, 1025–1039.
URL: https://www.cambridge.org/core/journals/journal-of-navigation/article/ enhancing-navigator-competence-by-demonstrating-maritime-cyber-security/ AF9FD35689C5B5F879B2446722B5CA1B,
Haugli-Sandvik, M., Lund, M.S., Bjørneseth, F.B., 2024. Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems. International
Journal of Information Security URL: https://doi.org/10.1007/s10207-023-00810-y,
Hoem, , Porathe, T., Rødseth, , Johnsen, S., 2018. At Least as Safe as Manned Shipping? Autonomous Shipping, Safety and "Human Error".
Hoem, S., Veitch, E., Vasstein, K., 2022. Human-centred risk assessment for a land-based control interface for an autonomous vessel. WMU Journal of Maritime Affairs 21, 179–211.
URL: https://doi.org/10.1007/s13437-022-00278-y,
Hogg, T., Ghosh, S., 2016. Autonomous merchant vessels: examination of factors that impact the effective implementation of unmanned ships. Australian Journal of Maritime & Ocean
Affairs 8, 206–222. URL: https://doi.org/10.1080/18366503.2016.1229244, publisher: Routledge eprint: https://doi.org/10.1080/18366503.2016.1229244.
Hollnagel, E., Woods, D.D., 2005. Joint Cognitive Systems: Foundations of Cognitive Systems Engineering. CRC Press, Boca Raton.
Hopcraft, R., Martin, K.M., 2018. Effective Maritime Cybersecurity Regulation – the Case for a Cyber Code. Journal of the Indian Ocean Region 14, 354–366. publisher: Routledge.
Horne, R.C., 2021. Autonomous and Remotely Operated Vessels 2021 to 2040. MIAL Future Leaders White Paper. Predictions for the Australian Maritime Industry .
Ibidapo, T.A., 2022. Industry 4.0: A Review, in: Ibidapo, T.A. (Ed.), From Industry 4.0 to Quality 4.0: An Innovative TQM Guide for Sustainable Digital Age Businesses. Springer International Publishing, Cham. Management for Professionals, pp. 537–608.
IMO, 2009. SOLAS -The International Convention for the Safety of Life at Sea. International Maritime Organization, United Kingdom.
IMO, 2021. Outcome of the regulatory scoping exercise for the use of Maritime Autonomous Surface Ships (mass). Technical Report MSC.1/Circ.1638. International Maritime Organization. URL: https://www.imo.org/en/MediaCentre/HotTopics/Pages/ Autonomous-shipping.aspx.
IMO, 2022. Guidelines on Maritime Cyber Risk Managament. URL: https://www.imo.org/ en/OurWork/Security/Pages/Cyber-security.aspx.
IMO, 2023. Development Of A Goal-based Instrument For Maritime Autonomous Surface Ships (Mass). Technical Report. International Maritime Organization. URL: https:// www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx.
Issa, M., Ilinca, A., Ibrahim, H., Rizk, P., 2022. Maritime Autonomous Surface Ships: Problems and Challenges Facing the Regulatory Process. Sustainability 14, 15630. URL: https:
//www.mdpi.com/2071-1050/14/23/15630, number: 23 Publisher: Multidisciplinary Digital Publishing Institute.
Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., Simonin, J., 2018. Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre, in: 2nd Cyber Security in Networking Conference (CSNet), IEEE, Paris, France. pp. 1–8.
Jan Rødseth, , Nordahl, H., Hoem, , 2018. Characterization of Autonomy in Merchant Ships, in: 2018 OCEANS - MTS/IEEE Kobe Techno-Oceans (OTO), pp. 1–7. URL: https:// ieeexplore.ieee.org/document/8559061,
Jiang, B., Li, J., Gong, C., 2018. Maritime Shipping and Export Trade on "Maritime Silk Road". The Asian Journal of Shipping and Logistics 34, 83–90. publisher: Elsevier.
Kala, N., Balakrishnan, M., 2019. Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancement 5, 19–28. URL: https://ijsta.com/ papers/IJSTAV5N2Y19/IJSTAV5N2R1Y19.pdf.
Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.H., 2022. Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management 0, 1–19. URL: https://doi.org/ 10.1080/03088839.2022.2124464,
Karamperidis, S., Kapalidis, C., Watson, T., 2021. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. Journal of Marine Science and Engineering 9, 1323. publisher: Multidisciplinary Digital Publishing Institute.
Kavallieratos, G., Katsikas, S., Gkioulos, V., 2019. Cyber-Attacks Against the Autonomous Ship, in: Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Ant´on, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C. (Eds.), Computer Security, Springer International Publishing, Cham. pp. 20–36.
Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A., Apostolou, P., 2022. Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach. International Journal of Critical Infrastructure Protection 37, 100526.
Keshav, S., 2007. How to read a paper. ACM SIGCOMM Computer Communication Review 37, 83–84. URL: https://doi.org/10.1145/1273445.1273458,
Kim, M., Joung, T.H., Jeong, B., Park, H.S., 2020. Autonomous Shipping and Its Impact on Regulations, Technologies, and Industries. Journal of International Maritime Safety, Environmental Affairs, and Shipping 4, 17–25. publisher: Taylor & Francis.
Komianos, A., 2018. The Autonomous Shipping Era. Operational, Regulatory, and Quality Challenges. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 12.
Kosowska-Stamirowska, Z., Ducruet, C., Rai, N., 2016. Evolving structure of the maritime trade network: Evidence from the Lloyd's Shipping Index (1890–2000). Journal of Shipping and Trade 1, 10. publisher: Springer.
Larsen, M.H., Lund, M.S., 2021. Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. IEEE Access : Practical innovations, Open solutions 9, 144895–144905. publisher: IEEE.
Lee, C., Lee, S., 2023. Evaluating the Vulnerability of YOLOv5 to Adversarial Attacks for Enhanced Cybersecurity in MASS. Journal of Marine Science and Engineering 11, 947.
URL: https://www.mdpi.com/2077-1312/11/5/947, number: 5 Publisher: Multidisciplinary Digital Publishing Institute.
Lee, C., Lee, S., 2024. A Risk Identification Method for Ensuring AI-Integrated System Safety for Remotely Controlled Ships with Onboard Seafarers. Journal of Marine Science and Engineering 12, 1778. URL: https://www.mdpi.com/2077-1312/12/10/1778, number: 10 Publisher: Multidisciplinary Digital Publishing Institute.
Li, M., Zhou, J., Chattopadhyay, S., Goh, M., 2024. Maritime Cybersecurity: A Comprehensive Review. URL: http://arxiv.org/abs/2409.11417, arXiv:2409.11417.
Li, S., Fung, K., 2019. Maritime Autonomous Surface Ships (MASS): Implementation and Legal Issues. Maritime Business Review 4, 330–339. Publisher: Emerald Publishing Limited.
Li, S., Meng, Q., Qu, X., 2012. An Overview of Maritime Waterway Quantitative Risk Assessment Models. Risk Analysis 32, 496–512. URL: https:// onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2011.01697.x, eprint:

https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1539-6924.2011.01697.x.
Lind, M., Ward, R., Jensen, H.H., Chua, C.P., Simha, A., Karlsson, J., Göthberg, L., Penttinen, T., Theodosiou, D.P., 2021. The Future of Shipping: Collaboration Through Digital Data Sharing, in: Lind, M., Michaelides, M., Ward, R., T. Watson, R. (Eds.), Maritime Informatics. Springer International Publishing, Cham, pp. 137–149.
Liu, J., Aydin, M., Akyuz, E., Arslan, O., Uflaz, E., Kurt, R.E., Turan, O., 2022. Prediction of human–machine interface (HMI) operational errors for maritime autonomous surface ships (MASS). Journal of Marine Science and Technology 27, 293–306. URL: https:
//doi.org/10.1007/s00773-021-00834-w,
Longo, G., Martelli, M., Russo, E., Merlo, A., Zaccone, R., 2024. Adversarial waypoint injection attacks on Maritime Autonomous Surface Ships (MASS) collision avoidance systems. Journal of Marine Engineering & Technology 23, 184–195. URL: https:
//doi.org/10.1080/20464177.2023.2298521, publisher: Taylor & Francis eprint: https://doi.org/10.1080/20464177.2023.2298521.
Lundberg, J., Johansson, B.J.E., 2021. A framework for describing interaction between human operators and autonomous, automated, and manual control systems. Cognition, Technology & Work 23, 381–401. URL: https://doi.org/10.1007/s10111-020-00637-w,
Lynch, K.M., Banks, V.A., Roberts, A.P.J., Radcliffe, S., Plant, K.L., 2024. What factors may influence decision-making in the operation of Maritime autonomous surface ships? A systematic review. Theoretical Issues in Ergonomics Science 25, 98–142. URL: https:
//doi.org/10.1080/1463922X.2022.2152900, publisher: Taylor & Francis eprint: https://doi.org/10.1080/1463922X.2022.2152900.
Lyons, J.B., Sycara, K., Lewis, M., Capiola, A., 2021. Human–Autonomy Teaming: Definitions, Debates, and Directions. Frontiers in Psychology 12.
Mallam, S.C., Nazir, S., Sharma, A., 2020. The human element in future Maritime Operations–Perceived impact of autonomous shipping. Ergonomics 63, 334–345. publisher: Taylor & Francis.
Martíınez, F., S`anchez, L.E., Santos-Olmo, A., Rosado, D.G., Fern`andez-Medina, E., 2024. Maritime cybersecurity: protecting digital seas. International Journal of Information Security URL: https://doi.org/10.1007/s10207-023-00800-0,
Mednikarov, B., Tsonev, Y., Lazarov, A., 2020. Analysis of Cybersecurity Issues in the Maritime Industry. Information & Security: An International Journal 47, 27–43. URL: https:
//isij.eu/article/analysis-cybersecurity-issues-maritime-industry,
Monsaingeon, N., Carli, Y., Caroux, L., Langlois, S., Lemercier, C., 2021. Indicating the Limits of Partially Automated Vehicles with Drivers' Peripheral Vision: An Online Study, in: Stanton, N. (Ed.), Advances in Human Aspects of Transportation, Springer International Publishing, Cham. pp. 78–85.
Munim, Z.H., Haralambides, H., 2022. Advances in Maritime Autonomous Surface Ships (MASS) in Merchant Shipping. Maritime Economics & Logistics 24, 181–188.
Murray, G., Johnstone, M.N., Valli, C., 2017. The convergence of IT and OT in critical infrastructure. Australian Information Security Management Conference Publisher: Security Research Institute (SRI), Edith Cowan University.
Nardelli, P.H.J., 2022. Cyber-physical Systems: Theory, Methodology, and Applications. URL: https://ieeexplore.ieee.org/book/9794564.
Navalta, J.W., Stone, W.J., Lyons, T.S., 2019. Ethical Issues Relating to Scientific Discovery in Exercise Science. International journal of exercise science 12, 1. Publisher: Western Kentucky University.
Olsen, A., 2024. Identification of Cyber Vulnerabilities, in: Safety Culture and Leading Indicators for Safety in the Maritime and Offshore Environment. Springer Nature Switzerland, Cham, pp. 599–609. URL: https://doi.org/10.1007/978-3-031-55943-3_43,
Palbar Misas, J.D., Hopcraft, R., Tam, K., Jones, K., 2024. Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness. Journal of Marine Engineering and Technology 23, 224–235. URL: http://www.scopus.com/inward/record.url?scp=85188614796&partnerID=8YFLogxK.
Parhizkar, T., Utne, I.B., Vinnem, J.E., 2022a. Human, Hardware, and Software Interactions in Risk Assessment, in: Parhizkar, T., Utne, I.B., Vinnem, J.E. (Eds.), Online Probabilistic Risk Assessment of Complex Marine Systems: Principles, Modelling and Applications. Springer International Publishing, Cham. Springer Series in Reliability Engineering, pp. 55–74.
Parhizkar, T., Utne, I.B., Vinnem, J.E., 2022b. Online Probabilistic Risk Assessment of Complex Marine Systems: Principles, Modelling and Applications. Springer Series in Reliability Engineering, Springer International Publishing, Cham. URL: https://link.springer. com/10.1007/978-3-030-88098-9,
Parlov, I., 2023. Can the International Regulatory Framework on Ships' Routing, Ship Reporting, and Vessel Traffic Service (VTS) Accommodate Marine Autonomous Surface Ships (MASS)? Ocean Development & International Law 54, 163–180.
Pietrzykowski, Z., Hajduk, J., 2019. Operations of Maritime Autonomous Surface Ships. TransNav, International Journal on Marine Navigation and Safety od Sea Transportation 13.
Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D., 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work 24, 371–390. URL: https://doi.org/10.1007/ s10111-021-00683-y,
Poornikoo, M., Øvergård, K.I., 2022. Levels of automation in maritime autonomous surface ships (MASS): a fuzzy logic approach. Maritime Economics & Logistics 24, 278–301. URL:
https://doi.org/10.1057/s41278-022-00215-z,
Praestegaard Larsen, B., 2022. Maritime Cybersecurity : Shipping Industry Plan. URL: https://www.diva-portal.org/smash/get/diva2:1679057/FULLTEXT01.pdf.
Praestegaard Larsen, B., 2024. A review of Ethical Considerations within Autonomous Maritime Cybersecurity Research. Journal of Maritime Research 21, 97–100. URL: https://www.jmr.unican.es/index.php/jmr/article/view/771. number: 1.
Pseftelis, T., Chondrokoukis, G., 2021. A Study about the Role of the Human Factor in Maritime Cybersecurity. SPOUDAI - Journal of Economics and Business 71, 55–72. URL: https://spoudai.unipi.gr/index.php/spoudai/article/view/2887. number: 1-2.
Raja Santhi, A., Muthuswamy, P., 2023. Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. International Journal on
Interactive Design and Manufacturing (IJIDeM) 17, 947–979. URL: https://doi.org/10. 1007/s12008-023-01217-8,
Rajaram, P., Goh, M., Zhou, J., 2022. Guidelines for cyber risk management in shipboard operational technology systems. Journal of Physics: Conference Series 2311, 012002. URL: https://dx.doi.org/10.1088/1742-6596/2311/1/012002, publisher: IOP Publishing.
Ramos, M.A., Thieme, C.A., Utne, I.B., Mosleh, A., 2020a. A generic approach to analysing failures in human – System interaction in autonomy. Safety Science 129, 104808. URL:
https://www.sciencedirect.com/science/article/pii/S0925753520302058,

Ramos, M.A., Thieme, C.A., Utne, I.B., Mosleh, A., 2020b. Human-system concurrent task analysis for maritime autonomous surface ship operation and safety. Reliability Engineering & System Safety 195, 106697. URL: https://www.sciencedirect.com/science/article/ pii/S0951832018313085,

Ramos, M.A., Utne, \.I., Mosleh, A., 2018. On Factors Affecting Autonomous Ships Operators Performance in a Shore Control Center. Proceedings of the 14th Probabilistic Safety Assessment and Management, Los Angeles, CA, USA , 16–21URL: https: //www.iapsam.org/psam14/proceedings/paper/paper_19 1_1.pdf.

Reggiannini, M., Righi, M., Tampucci, M., Bedini, L., Di Paola, C., Martinelli, M., Mercurio, C., Salerno, E., 2019. Remote Sensing for Maritime Monitoring and Vessel Prompt Identification, in: Choro´s, K., Kopel, M., Kukla, E., Siemin´ski, A. (Eds.), Multimedia and Network Information Systems, Springer International Publishing, Cham. pp. 343–352.

Ren, M., Chen, N., Qiu, H., 2023. Human-machine Collaborative Decision-making: An Evolutionary Roadmap Based on Cognitive Intelligence. International Journal of Social Robotics 15, 1101–1114. URL: https://doi.org/10.1007/s12369-023-01020-1,

Ronca, V., Uflaz, E., Turan, O., Bantan, H., MacKinnon, S.N., Lommi, A., Pozzi, S., Kurt, R.E., Arslan, O., Kurt, Y.B., Erdem, P., Akyuz, E., Vozzi, A., Di Flumeri, G., Aric`o, P., Giorgi, A., Capotorto, R., Babiloni, F., Borghini, G., 2023. Neurophysiological Assessment of An Innovative Maritime Safety System in Terms of Ship Operators' Mental Workload, Stress, and Attention in the Full Mission Bridge Simulator. Brain Sciences 13, 1319. URL: https:// www.mdpi.com/2076-3425/13/9/1319, number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

Rødseth, J., Nesheim, D.A., Rialland, A., Holte, E.A., 2023. The Societal Impacts of Autonomous Ships: The Norwegian Perspective, in: Autonomous Vessels in Maritime Affairs: Law and Governance Implications. Springer, pp. 357–376.

Rødseth, J., Wennersberg, L.A.L., Nordahl, H., 2022. Levels of autonomy for ships. Journal of

Physics: Conference Series 2311, 012018. URL: https://dx.doi.org/10.1088/1742-6596/ 2311/1/012018, publisher: IOP Publishing.

Saniuk, S., Caganova, D., Saniuk, A., 2023. Knowledge and Skills of Industrial Employees and Managerial Staff for the Industry 4.0 Implementation. Mobile Networks and Applications 28, 220–230. URL: https://doi.org/10.1007/s11036-021-01788-4,

Sarker, I.H., 2024a. AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. Springer Nature Switzerland, Cham. URL: https://link.springer.com/10.1007/978-3-031-54497-2,

Sarker, I.H., 2024b. AI for Critical Infrastructure Protection and Resilience, in: Sarker, I.H. (Ed.), AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. Springer Nature Switzerland, Cham, pp. 153–172.

URL: https://doi.org/10.1007/978-3-031-54497-2_9,

Sencila, V., 2019. Industry 4.0: Autonomous Shipping and New Challenges for Maritime Education and Training.

Shafqat, N., Masood, A., 2016. Comparative Analysis of Various National Cyber Security Strategies 14. URL: https://sites.google.com/site/ijcsis/.

Sharma, A., Nazir, S., Ernstsen, J., 2019. Situation Awareness Information Requirements for Maritime Navigation: A Goal Directed Task Analysis. Safety Science 120, 745–752. publisher: Elsevier.

Sheridan, T.B., 1992. Telerobotics, Automation, and Human Supervisory Control. MIT Press. Google-Books-ID: eu41 M2Do9oC.

Simões-Marques, M., Frias, A., Agua, P.B., 2021. Human Factors Impact in the Security and´ Safety of the Maritime Domain, in: Nunes, I.L. (Ed.), Advances in Human Factors and System Interactions, Springer International Publishing, Cham. pp. 28–36.

Stannard, S., 2020. COVID-19 in the Maritime Setting: The Challenges, Regulations and the International Response. International Maritime Health 71, 85–90.

Stepien´, B., 2023. Can a Ship Be Its Own Captain? Safe Manning of Autonomous and Uncrewed Vessels. Marine Policy 148, 105451.

Stoynov, S., Nikolov, B., 2021. Approach To Ship's It And Ot Systems Cybersecurity Improvement. Pedagogika-Pedagogy 93, 185–196. URL: https://azbuki.bg/wp-content/ uploads/2021/09/Pedagogy_7s_21_Stoyno-Stoynov-Borislav-Nikolov.pdf,

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y., 2019a. Maritime Cyber Risk Management: An Experimental Ship Assessment. The Journal of Navigation 72, 1108–

1120. URL: https://www.cambridge.org/core/journals/journal-of-navigation/ article/maritime-cyber-risk-management-an-experimental-ship-assessment/ 576B504DA6D2990FFC1B7478E1042609,

Svilicic, B., Rudan, I., Frančić, V., Doričić, M., 2019b. Shipboard ECDIS Cyber Security: Third-Party Component Threats. Pomorstvo 33, 176–180. URL: https://hrcak.srce. hr/229306,

Tabish, N., Chaur-Luh, T., 2024. Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. IEEE Access 12, 17114–

17136. URL: https://ieeexplore.ieee.org/abstract/document/10411879, conference Name: IEEE Access.

Tam, K., Jones, K., 2018a. Cyber-Risk Assessment for Autonomous Ships, in: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8.

Tam, K., Jones, K., 2019a. Factors Affecting Cyber Risk in Maritime, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1–8.

Tam, K., Jones, K., 2019b. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs 18, 129–163. URL: https://doi.org/10.1007/ s13437-019-00162-2,

Tam, K., Jones, K.D., 2018b. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy 3, 147–164. URL: https://doi.org/10.1080/23738871.2018.1513053, publisher: Routledge eprint: https://doi.org/10.1080/23738871.2018.1513053.

Tam, K., Jones, K.D., 2019c. Situational Awareness: Examining Factors that Affect Cyber-

Risks in the Maritime Sector URL: https://pearl.plymouth.ac.uk/handle/10026.1/ 16791, accepted: 2021-01-08T12:41:06Z Publisher: Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC).

Tam, K., Jones, K.D., Papadaki, M., 2012. Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference 1.

Tolone, W.J., 2014. Making Sense of the Operational Environment through Interactive, Exploratory Visual Analysis .

Tran, K., Keene, S., Fretheim, E., Tsikerdekis, M., 2021. Marine Network Protocols and Security Risks. Journal of Cybersecurity and Privacy 1, 239–251. URL: https://www.mdpi. com/2624-800X/1/2/13, number: 2 Publisher: Multidisciplinary Digital Publishing

Institute.

Tzavara, V., Vassiliadis, S., 2024. Tracing the evolution of cyber resilience: a historical and conceptual review.

International Journal of Information Security URL: https://doi.org/ 10.1007/s10207-023-00811-x,

Veitch, E., Andreas Alsos, O., 2022. A systematic review of human-AI interaction in autonomous ship systems. Safety Science 152, 105778. URL: https://www.sciencedirect. com/science/article/pii/S0925753522001175,

Ventikos, N.P., Chmurski, A., Louzis, K., 2020. A systems-based application for autonomous vessels safety: Hazard identification as a function of increasing autonomy levels. Safety Science 131, 104919. URL: https://www.sciencedirect.com/science/article/pii/ S0925753520303167,

Verdiesen, I., Santoni de Sio, F., Dignum, V., 2021. Accountability and Control Over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight. Minds and Machines 31, 137–163. URL: https://doi.org/10.1007/s11023-020-09532-9,

Veritas, B., 2019. NI641 Guidelines for autonomous shipping | Marine & Offshore. URL: https://marine-offshore.bureauveritas.com.

Vermeulen, B., Kesselhut, J., Pyka, A., Saviotti, P.P., 2018. The Impact of Automation on Employment: Just the Usual Structural Change? Sustainability 10, 1661. URL: https:// www.mdpi.com/2071-1050/10/5/1661, number: 5 Publisher: Multidisciplinary Digital Publishing Institute.

Vianello, L., Ivaldi, S., Aubry, A., Peternel, L., 2023. The effects of role transitions and adaptation in human–cobot collaboration. Journal of Intelligent Manufacturing URL: https://doi.org/10.1007/s10845-023-02104-5,

Walter, M.J., Barrett, A., Walker, D.J., Tam, K., 2023. Adversarial AI Testcases for Maritime Autonomous Systems. AI, Computer Science and Robotics Technology URL: https://www. intechopen.com/journals/1/articles/189, publisher: IntechOpen.

World Maritime University, 2019. Transport 2040: Automation, Technology, Employment The Future of Work. Technical Report. World Maritime University. URL: http://dx.doi. org/10.21677/itf.20190104,

Wróbel, K., Montewka, J., Kujala, P., 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability Engineering & System Safety 165, 155–169. URL: https://www.sciencedirect.com/science/article/ pii/S0951832016303337,

Xu, H., Moreira, L., Guedes Soares, C., 2023. Maritime Autonomous Vessels. Journal of Marine Science and Engineering 11, 168. publisher: Multidisciplinary Digital Publishing Institute.

Xu, X., Ngoc Cuong, T., Lee, S.D., You, S.S., 2020. Secure communication system in maritime navigation using state observer with linear matrix inequality. Journal of International Maritime Safety, Environmental Affairs, and Shipping 4, 70–75. URL: https:

//doi.org/10.1080/25725084.2020.1790102, publisher: Taylor & Francis eprint: https://doi.org/10.1080/25725084.2020.1790102.

Yaacoub, J.P.A., Noura, H.N., Salman, O., Chehab, A., 2022. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security 21, 115–158. URL: https://doi.org/10.1007/s10207-021-00545-8,

Yang, F., Gu, S., 2021. Industry 4.0, a revolution that requires technology and national strategies. Complex & Intelligent Systems 7, 1311–1325. URL: https://doi.org/10. 1007/s40747-020-00267-9,

Ye, J., Li, C., Wen, W., Zhou, R., Reppa, V., 2023. Deep Learning in Maritime Autonomous Surface Ships: Current Development and Challenges. Journal of Marine Science and Application 22, 584–601. URL: https://doi.org/10.1007/s11804-023-00367-1,

Yu, H., Meng, Q., Fang, Z., Liu, J., 2023. Literature review on maritime cybersecurity: state-of-the-art. The Journal of Navigation , 1– 14URL: https://www.cambridge.org/core/journals/journal-of-navigation/ article/literature-review-on-maritime-cybersecurity-stateoftheart/90F7A14DEA9148C793819170B2474A89#, publisher: Cambridge University Press.

Zhang, J., Wang, M.M., You, X., 2023. Maritime Autonomous Surface Shipping from a Machine-Type Communication Perspective. IEEE Communications Magazine , 1–7

Zhang, M., Zhang, D., Yao, H., Zhang, K., 2020. A probabilistic model of human error assessment for autonomous cargo ships focusing on human–autonomy collaboration. Safety Science 130, 104838. URL: https://www.sciencedirect.com/science/article/ pii/S0925753520302356,

Zubowicz, T., Armin´ski, K., Witkowska, A., Smierzchalski, R., 2019. Marine Autonomous´ Surface Ship - Control System Configuration. IFAC-PapersOnLine 52, 409–415.