Autonomous Ships: A Thematic Review

Ruhaimatu Abudu and Raj Bridgelall *

Transportation, Logistics & Finance, College of Business, North Dakota State University, P.O. Box 6050, Fargo, ND 58108-6050, USA; ruhaimatu.abudu@ndsu.edu

* Correspondence: raj@bridgelall.com or raj.bridgelall@ndsu.edu

Abstract: Ships connect the global economy through maritime transport. However, their susceptibility to increasing geopolitical conflicts has heightened concerns about the risks to crew safety and navigation security. This systematic literature review (SLR), utilizing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, rigorously examines the safety and security of autonomous ships in maritime transport. The methodology employs a comprehensive search across major databases including Scopus, Google Scholar, and Science Direct, based on explicit inclusion criteria focusing on recent advancements from 2014 to 2023. By methodically analyzing 58 relevant publications screened from an initial pool of 1407, this paper highlights critical trends and gaps in the application of advanced sensor technologies, cybersecurity measures, and autonomous navigation systems. The findings provide insights into the operational challenges and technological developments shaping the future of maritime safety and security, offering valuable guidance for policymakers and industry stakeholders. This research contributes to scholarly discourse in this industry by mapping the trajectory of technological integration and its implications for maritime operations in a global context.

Keywords: autonomous ships; maritime safety and security; cybersecurity in maritime operations; autonomous navigation technologies; risk assessment in maritime operations; maritime regulatory frameworks

1. Introduction

Maritime transport, responsible for more than 80% of international trade, is set to witness significant transformations with the advent of sensors and digitalization [1]. Such developments have introduced new paradigms in maritime operations, notably the rise of maritime autonomous ships [2]. The concept of autonomous ships, central to recent maritime research, aims to address prevailing challenges in cost, safety, and security within the industry [3]. The recent bridge collapse in Baltimore, USA, caused by a strike from a large container ship has further raised concerns about maritime navigation safety and the potential for automation to thwart such incidents [4].

The world’s first crewless ship was launched in 2021 between two Norwegian ports, marking a pivotal moment in maritime history [5], with the industry expecting advanced technologies and artificial intelligence to enhance operational efficiency, reduce costs, and minimize environmental impact [6]. Equipped with an array of sensors and navigational aids, such as GPS, radar, and cameras, evolving ship technology promises safer and more efficient navigation by enabling ships to continuous monitoring their surroundings and adjusting their course and speed as needed [7]. These sensors provide the necessary data for real-time environmental awareness, obstacle detection, and collision avoidance, serving as the eyes and ears of autonomous ships. The integration of these technologies ensures that autonomous ships can accurately perceive their surroundings, even in challenging weather conditions or congested maritime traffic zones. Communication technologies play a crucial role in the remote monitoring and intervention if needed to assure the safe operation of these ships. High-speed satellite communications ensure continuous data
exchange between the ship and shore-based control centers, allowing for remote oversight of ship operations and intervention when necessary.

Despite the potential benefits, autonomous ships face significant threats that challenge their operation and security. Current solutions, primarily benefiting law enforcement and naval applications, might be insufficient for the commercial maritime sector, necessitating novel approaches to ensure the safety and security of these ships [8,9].

The goal of this study is to highlight research trends and voids that will offer insights, through a comprehensive literature review, to inform policy, industry practices, and technological advancements. This work focuses on a critical gap in published research on cybersecurity, regulatory framework, and emergency response management pertinent to the safety and security of autonomous ships. Utilizing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, this systematic literature review (SLR) formulated the following research questions on key safety and security dimensions of autonomous ships:

1. Threat Evaluation: How does the maritime industry approach the evaluation of threats that affect the safety and security of autonomous ships?
2. Operational Challenges: What are the principal operational challenges to enable autonomous maritime ships?
3. Technological Assistance: What are the technologies employed to mitigate threats to autonomous ship operations?

The authors developed these research questions to guide the SLR, ensuring a focused exploration of the most pertinent issues that the maritime industry currently faces. A preliminary analysis of recent studies on maritime safety and security, particularly in the context of autonomy, aided the development of these research questions. Each question aims to explore different dimensions of autonomous maritime operations, guiding the selection and analysis of literature to ensure comprehensive coverage of each topic.

The subsequent parts of this paper have the following structure: Section 2 explains the SLR methodology utilized; Section 3 provides an analytical review of the existing literature, categorizing the main themes that address the research questions; Section 4 expands the discourse on safety and security concerns in autonomous ship operations; Section 5 concludes the study, highlighting the research gaps and limitations.

2. Methodology

The SLR employed is a rigorous and methodical approach designed to systematically identify and analyze the existing body of literature in a specific field. This process helps in identifying research gaps and offering insights for theoretical development and future studies [10]. The methodology of an SLR ensures a comprehensive, transparent, and replicable review process, vital for maintaining the integrity and validity of the findings [11]. This review utilized the 2020 update of PRISMA, which is particularly suitable for mixed-method reviews encompassing both quantitative and qualitative studies. The framework comprises 27 items across seven sections [11]. Figure 1 illustrates the SLR framework employed in this study. The next three subsections further describe the framework in detail.

2.1. Publication Selection

The selection process involved a thorough Internet search using various keywords related to unmanned maritime vehicles, encapsulating the concept of autonomous ship and their safety and security aspects. This initial phase included formulating research questions and appropriate keyword combinations to produce potentially relevant publications. The screening evaluated publications based on criteria such as publication titles, abstracts, keywords, publication date, and language—with a preference for publications in English. The selection emphasized peer-reviewed publications (journal articles, conference papers, official industry reports) that directly addressed the research questions formulated to guide the SLR. These criteria aim to filter the literature to those studies that have undergone rigorous peer review and are widely accessible to the international research community.
2.1. Publication Selection

The selection process involved a thorough Internet search using various keywords related to unmanned maritime vehicles, encapsulating the concept of autonomous ship and their safety and security aspects. This initial phase included formulating research questions and appropriate keyword combinations to produce potentially relevant publications. The screening evaluated publications based on criteria such as publication titles, abstracts, keywords, publication date, and language—with a preference for publications in English. The selection emphasized peer-reviewed publications (journal articles, conference papers, official industry reports) that directly addressed the research questions formulated to guide the SLR. These criteria aim to filter the literature to those studies that have undergone rigorous peer review and are widely accessible to the international research community.

2.2. Systematic Review

The following structured phases guided the selection of publications for further scrutiny and topic classification:

1. Database Search: The authors selected three databases for the literature search: Google Scholar, Scopus, and Science Direct. This choice was strategic, aimed at capturing a broad spectrum of interdisciplinary research spanning the technological, regulatory, and operational dimensions of autonomous ships. Scholars recognize these databases for their extensive coverage of both theoretical and applied research, providing a comprehensive view of the current state of knowledge in the field.

2. Search Criteria: The search focused on publications appearing between January 2014 and December 2023, related to maritime safety, security, and autonomous ship operations. This time frame and thematic focus aimed to capture the most recent and relevant advancements in the field, aligning with the period of rapid development in autonomous maritime technologies and the corresponding regulatory discussions. The search used Boolean combinations of phrases such as “maritime safety and security”, “nautical safety and security”, and variations of “autonomous”, “unmanned”, “maritime autonomous surface ship (MASS)” along with “vessel”, “ship”, or “craft”, with further details provided in Section 3. The use of Boolean combinations allowed for a refined search strategy, targeting the intersection of safety, security, and autonomy in maritime operations.

Figure 1. The SLR framework utilized in this study.
3. Snowball: This technique examines the references from the selected literature to include additional relevant articles not discovered during the initial search.

4. Relevance Screening: Setting inclusion and exclusion criteria aimed to distill the vast body of literature to those contributions that directly inform the safety, security, and operational challenges of autonomous ship:
   a. Inclusion criteria: Peer-reviewed journal articles, conference papers, and reports published within the specified date range, written in English and focusing on safety and security operations of autonomous ships.
   b. Exclusion criteria: Non-peer-reviewed articles, publications before 2014, articles not in English, and those not aligned with the research questions. The excluded articles categorized as “grey literatures” were works not peer-reviewed such as newsletters, marketing studies, and reports from institutions.

Table 1 summarizes the criteria used to include relevant publications.

<table>
<thead>
<tr>
<th>Category</th>
<th>Inclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source type</td>
<td>Peer-reviewed journal articles, conference papers, and reports</td>
</tr>
<tr>
<td>Publication date</td>
<td>Articles published between January 2014 and December 2023</td>
</tr>
<tr>
<td>Access to text</td>
<td>Availability of full-text copies of selected articles</td>
</tr>
<tr>
<td>Language</td>
<td>Published in English language</td>
</tr>
<tr>
<td>Databases</td>
<td>Articles published in Google Scholar, Scopus, and Science Direct</td>
</tr>
<tr>
<td>Content focus</td>
<td>Articles focusing on the safety and security of autonomous ships</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>Non-duplicate articles from the selected databases</td>
</tr>
<tr>
<td>Search phrases</td>
<td>Based on specific search phrases</td>
</tr>
</tbody>
</table>

2.3. Literature Classification

This final phase of the review process involved a detailed assessment of the selected literature, focusing on its relevance to the research questions. This included a comprehensive analysis, guided by the Critical Appraisal Skills Program [12], and categorized into themes addressing the three research questions as follows:

1. Threat Evaluation: Performance standards, vulnerability assessments, operational safety metrics, environmental impacts, and security technologies;
2. Operational Challenges: Human interference and technological challenges;

The authors meticulously extracted and analyzed the primary themes from each article, focusing particularly on the technological approaches employed to enhance vessel safety. The authors then systematically classified the themes according to how they address each research question. For the first question on threat evaluation, the classification focused on articles that discuss methodologies and technologies for assessing risks such as cyber threats and physical vulnerabilities. For the second question regarding operational challenges, the authors analyzed studies that detail the complexities of integrating automation with human oversight. Lastly, for the third question on technological assistance, the review concentrated on innovations in technologies that enhance the safety and security of ship operations, such as collision avoidance systems and cybersecurity measures. This classification strategy was instrumental in organizing the literature into coherent themes that directly correspond to the core research questions of this study. By systematically categorizing the literature, the review process facilitated a focused analysis of the key areas of interest, enabling a targeted synthesis of findings that can inform policy, practice, and future research directions in autonomous maritime operations. The next section presents the results of the SLR.
3. Results

Table 2 lists the search phrases and formats used for each database, including the results, which totaled 1351 publications. Applying the snowball technique of forward referencing added 56 publications for a total of 1407 publications. Relevance screening eliminated 1349 of these publications, leaving 58 publications for classification. There were no relevant publications in 2014. Table 3 lists the publications within the thematic categories addressing the research questions. Figure 2a shows the distribution of publications by theme category, split by publication year, and Figure 2b shows the transverse view. Figure 3a shows the distribution of publications by year, split by country of authorship, and Figure 3b shows the transverse view. The next three subsections evaluate the findings that address the research questions guiding the SLR.

Table 2. Search results from selected databases.

<table>
<thead>
<tr>
<th>Database</th>
<th>Search Phrase and Format</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Scholar</td>
<td>(“maritime safety and security”) OR (“nautical safety and security”) AND (“autonomous” OR “unmanned” OR “MASS”) AND (“vessel” OR “ship” OR “craft”)</td>
<td>1220</td>
</tr>
<tr>
<td>Scopus</td>
<td>ALL (“maritime safety and security”) OR (“nautical safety and security”) AND (“autonomous” OR “unmanned” OR “MASS”) AND (“vessel” OR “ship” OR “craft”) AND PUBYEAR &gt; 2014 AND (LIMIT-TO [LANGUAGE, “English”])</td>
<td>33</td>
</tr>
<tr>
<td>ScienceDirect</td>
<td>(“maritime safety and security”) OR (“nautical safety and security”) AND (“autonomous” OR “unmanned” OR “MASS”) AND (“vessel” OR “ship” OR “craft”)</td>
<td>98</td>
</tr>
</tbody>
</table>

Table 3. Literature categorization.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Publications Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collision Avoidance</td>
<td>Chen, et al. (2020) [13], Hu et al. (2020) [14], Jalonen et al. (2017) [15], Johansen et al. (2016) [16], Lyu et al. (2019) [17], Rudan et al. (2020) [18], Thombe et al. (2022) [19], Valdez et al. (2019) [20], Zhang et al. (2022) [21], Eriksen et al. (2020) [22], Zaccone (2021) [23]</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Cho et al. (2022) [24], Le Tixerant et al. (2018) [25]</td>
</tr>
<tr>
<td>Emergency Response</td>
<td>Azam et al. (2022) [26], Dalpe et al. (2021) [27], Douglas et al. (2020) [28], Michailidis et al. (2020) [29], Michelen et al. (2023) [30], Santoso et al. (2018) [31]</td>
</tr>
<tr>
<td>Environmental Impacts</td>
<td>Browne et al. (2020) [32], Lee et al. (2021) [33], Wröbel et al. (2018) [8]</td>
</tr>
<tr>
<td>Human Interference</td>
<td>Chae et al. (2020) [34], Kavallieratos et al. (2020) [35], Yang et al. (2023) [36]</td>
</tr>
<tr>
<td>Operational Safety</td>
<td>Gu et al. (2021) [37], Norton et al. (2017) [38], Rokseth et al. (2019) [39]</td>
</tr>
<tr>
<td>Performance Standards</td>
<td>Fan et al. (2020) [40], Mukhoti et al. (2018) [41], Porathe et al. (2019) [42], Rødseth et al. (2017) [43], Vosooghi et al. (2019) [44]</td>
</tr>
<tr>
<td>Technological Assistance</td>
<td>Ali et al. (2021) [45], Amro et al. (2021) [46], Chang et al. (2021) [47], Gülcan et al. (2023) [48], Karim et al. (2022) [49], Kavallieratos et al. (2019) [35], Kim et al. (2020) [50], Laurinen (2016) [51], Nzengu et al. (2021) [52], Paker (2022) [53], Pedersen et al. (2022) [54], Perera (2018) [35], Petrig et al. (2020) [56], Prins et al. (2017) [57], Ramos et al. (2018) [58], Ringbom et al. (2019) [59], Salvemini et al. (2015) [60], Sogancilar (2021) [61], Tam et al. (2018) [62], Tarkowski et al. (2021) [63], Zolich et al. (2019) [64]</td>
</tr>
<tr>
<td>Technological Challenges</td>
<td>Thiem et al. (2018) [65]</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Bolbot et al. (2019) [66], Condiffe (2017) [67], He et al. (2017) [14]</td>
</tr>
</tbody>
</table>
Table 4 summarizes the various methodologies used in the maritime industry to evaluate threats that affect the safety and security of autonomous ship operation. From this table, it becomes evident that the maritime industry faces a multifaceted array of risks associated with autonomous ships, which this work categorized broadly into technological, operational, and environmental risks. Technological risks often stem from malfunctions or failures in autonomous systems, requiring robust design, redundancy, and advanced diagnostics as potential solutions. Operational risks, such as collisions or navigation errors, necessitate enhanced algorithms for real-time decision making and comprehensive simulation-based training for intervention missions. Environmental risks, including oil spills or damage to marine ecosystems, require strict adherence to environmental standards and the development of eco-friendly technologies.
3.1. Threat Evaluation
This section investigates the methodologies and indicators employed to evaluate threats to autonomous ships. These methodologies encompass five key themes: performance standards, vulnerability assessment, safety, environmental impact, and security technologies. These themes collectively offer a comprehensive view highlighting the balance between reduced human intervention and emerging challenges due to advanced technology.

3.1.1. Performance Standards
The literature consistently addressed performance standards within the autonomous shipping industry, focusing on the varying levels of autonomy as classified by the International Maritime Organization [68]. Table 5 summarizes the IMO standards recognizing the emergence of autonomous ships promises to mitigate some traditional risks, such as human error in navigation, thereby enhancing safety and efficiency. However, it also introduces new risks, particularly in cybersecurity, where ships may become targets for hacking or software manipulation. Addressing these new challenges necessitates a multi-disciplinary research approach, combining maritime studies with cyber-physical system security, and fostering collaborations between industry, academia, and regulatory bodies. Future research directions could include the development of standardized protocols for autonomous ship operation, the integration of advanced cybersecurity measures, and the exploration of the socio-economic impacts of transitioning towards autonomous shipping. This discussion sets the stage for a deeper exploration of risk management strategies in the subsequent sections of the results.

![Figure 3. Publications by (a) year split by country and (b) country split by year.](image-url)
### Table 4. Approaches relevant to the research questions about autonomous ship operations.

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Categories</th>
<th>Approaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Evaluation</td>
<td>Safety</td>
<td>Performance standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operational indicators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System performance</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Cyber-risk assessment</td>
<td>Safety performance</td>
</tr>
<tr>
<td>assessment</td>
<td></td>
<td>Safety-related cyber-attacks identification</td>
</tr>
<tr>
<td></td>
<td>Risk</td>
<td>assessment</td>
</tr>
<tr>
<td>Threat Evaluation</td>
<td>Safety</td>
<td>Safety evaluation metrics: system-theoretic process analysis (STPA)</td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
<td>Human–robot interaction safety</td>
</tr>
<tr>
<td>impacts</td>
<td></td>
<td>Leading safety indicators</td>
</tr>
<tr>
<td>Security Technologies</td>
<td></td>
<td>Cybersecurity risk management metrics</td>
</tr>
<tr>
<td>Human Interference</td>
<td>Human</td>
<td>Communication and networks survey</td>
</tr>
<tr>
<td></td>
<td>–machine</td>
<td>Blockchain security implementation</td>
</tr>
<tr>
<td>Operational</td>
<td>Human–machine interface quality (HMI)</td>
<td>Operational Challenges</td>
</tr>
<tr>
<td>Challenges</td>
<td>Regulatory</td>
<td>Evaluating of lean product development stages</td>
</tr>
<tr>
<td>Technological</td>
<td>Deep learning for autonomous ship navigation</td>
<td>Changes</td>
</tr>
<tr>
<td>Changes</td>
<td></td>
<td>Incorporation of human factors engineering</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Comprehensive risk assessment</td>
<td>Technological Assistance</td>
</tr>
<tr>
<td>Emergency response</td>
<td>Performance evaluation and review framework of robotic missions (PERFORM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fault-detection system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STRIDE and LINDDUN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stakeholder framework for autonomous behaviors</td>
<td></td>
</tr>
<tr>
<td>Collision avoidance</td>
<td>Collision risk index</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hybrid collision avoidance system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optimal path planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real time path planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Predictive hazard assessment</td>
<td></td>
</tr>
</tbody>
</table>

#### 3.1. Threat Evaluation

This section investigates the methodologies and indicators employed to evaluate threats to autonomous ships. These methodologies encompass five key themes: performance standards, vulnerability assessment, safety, environmental impact, and security technologies. These themes collectively offer a comprehensive view highlighting the balance between reduced human intervention and emerging challenges due to advanced technology.

#### 3.1.1. Performance Standards

The literature consistently addressed performance standards within the autonomous shipping industry, focusing on the varying levels of autonomy as classified by the International Maritime Organization [68]. Table 5 summarizes the IMO standards recognizing the different levels of autonomy. These standards revolve around the operational aspects of a ship’s operations and autonomy, emphasizing the replacement of human roles with so-
phisticated sensors and algorithms. The performance standards, as examined by [40,42,43], include safety protocols, risk assessments, communication systems, and human–machine interfaces (HMIIs). Considerations attend to ensuring diverse and robust communication systems [50] and the integration of advanced maritime technology to enable autonomy [55].

Table 5. Degrees of ship autonomy by IMO.

<table>
<thead>
<tr>
<th>Degree</th>
<th>Description</th>
<th>Autonomy Level</th>
<th>Human Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Seafarers operate and control ship’s systems; some operations are automated.</td>
<td>Conventional</td>
<td>Operating and monitoring ship.</td>
</tr>
<tr>
<td>2</td>
<td>Remote-controlled ships with seafarers on board.</td>
<td>Conventional</td>
<td>Supervising ship operations.</td>
</tr>
<tr>
<td>3</td>
<td>Remotely controlled ship without crew on board.</td>
<td>Semi-autonomous</td>
<td>Remote operation; no humans on board.</td>
</tr>
<tr>
<td>4</td>
<td>Fully autonomous ship making decisions independently.</td>
<td>Fully autonomous</td>
<td>There is no human intervention. The ship’s operating system makes decisions.</td>
</tr>
</tbody>
</table>

3.1.2. Vulnerability Assessment

Vulnerability assessment in this context is a comprehensive process to identify potential threats affecting autonomous ship operations. This category covers the vulnerability to threats like piracy and cyberattacks. Studies indicate that these vulnerabilities span the maritime supply chain, including ports and offshore platforms [40,67]. Studies highlight the physical security risks, such as collision avoidance [69], and the complexities of autonomy leading to increased system vulnerability [66]. The International Regulations for Preventing Collisions at Sea 1972 (COLREGs), for instance, addresses ship collision risks.

3.1.3. Operational Safety

This subcategory encapsulated the safety of autonomous ships in terms of collision avoidance management, cybersecurity, and operational concerns [37]. Rokseth et al. (2019) emphasized that the inherent safety of autonomous ships is a fundamental prerequisite for their deployment [39]. Hence, the focus is on design verification standards, ensuring functional system performance over time.

3.1.4. Environmental Impacts

In evaluating the environmental impact of autonomous ships, it is essential to consider the broader implications on sustainability. Studies by authors like Gu et al. (2021) [37] and Lee et al. (2021) [33] emphasize the importance of including environmental considerations in evaluating autonomous ships. Wróbel et al. (2018) proposed a system-centric safety evaluation model for incorporating environmental factors into safety assessments [8]. Recent advancements in battery technologies and alternative fuels, as discussed by Koumentakos (2019), suggest significant potential for reducing the environmental impact of maritime operations [70]. Moreover, the application of machine learning algorithms for energy-efficient route optimization, as detailed in the work of Huang et al. (2022), provides promising avenues for enhancing the sustainability of autonomous ships [71]. These studies highlight the progressive steps towards minimizing the ecological impact of maritime transport, thereby supporting a transition to greener maritime technologies.

3.1.5. Security Technologies

The security of autonomous ships is paramount, requiring advanced technologies to mitigate risks from cyber threats. The integration of blockchain technology, as explored by Liu et al. (2021), offers a robust solution for enhancing the security of navigational and operational data through decentralized and tamper-resistant digital ledgers [72]. Additionally, recent innovations in intrusion detection systems tailored for maritime environments, as reported by Tabish and Chaur-Luh (2024), provide essential capabilities for identifying and responding to cybersecurity threats in real-time [73]. Other reviewed literature
covered aspects such as communication networking technologies [64], safety technology development [54], and the integration of cybersecurity and artificial intelligence (AI) for navigation [35].

3.2. Operational Challenges

This section investigates the operational challenges encountered in autonomous ship operations, focusing on human interference and technological complexities. This analysis seeks to uncover and address potential barriers to deploying autonomous ship technology and its integration into maritime operations.

3.2.1. Human Interference

The integration of autonomous systems in maritime operations introduces new challenges in human–system interaction [74]. These challenges primarily revolve around the influence of human operators on the functionality of autonomous systems, the potential for errors in HMI, and the safety risks associated with human factors. To address these issues, there is a pressing need for the development of advanced technologies aimed at minimizing human interference while simultaneously bolstering the safety of ships.

Central to mitigating these challenges is the design of the HMI, which serves as the crucial link between human operators and autonomous systems. The main characteristic of effective HMI design is intuitiveness, offering operators access to straightforward controls and clear, concise information. Developers achieve this through the user-friendly presentation of sensor data, system status indicators, and predictive analytics, enabling operators to swiftly comprehend and react to operational situations. Notably, advancements such as early warning systems based on multi-sensor fusion have demonstrated significant potential in reducing human errors and enhancing safety [36]. Furthermore, the incorporation of feedback mechanisms within HMI supports a dynamic interaction between operators and the system, facilitating timely adjustments and interventions as needed. Emphasizing ergonomics and the management of cognitive load in HMI design is critical for minimizing errors and improving the safety of maritime operations.

As ships become autonomous, it becomes increasingly important for ship operators to undergo specialized training. Such training should equip personnel with the necessary competencies to effectively manage autonomous systems, encompassing a thorough understanding of AI decision-making processes, emergency protocols, and system troubleshooting techniques. Utilizing simulation-based training tools, such as virtual and augmented reality, offers operators valuable hands-on experience within a controlled setting, thereby preparing them for the complexities of real-world scenarios. Concurrently, the maritime industry should revise the certification process for autonomous ship operators to better reflect the distinct requirements of operating within an autonomous framework. This revision should introduce competency standards that highlight proficiency in new technology, decision making under uncertainty, and the ability to communicate effectively with remote monitoring centers. Establishing stringent training and certification standards is imperative for ensuring that human operators are adequately prepared to synergize with and augment the capabilities of autonomous ships.

Overall, to effectively balance autonomous technologies with human factors, the industry could adopt a multi-disciplinary approach that combines ergonomic design, user-interface optimization, and advanced training programs. This methodology involves the iterative testing of HMI to ensure intuitive user experiences and minimize cognitive load. Furthermore, the integration of decision support systems that provide real-time feedback and situational awareness aids operators in maintaining control and oversight, thereby enhancing safety mechanisms. Regarding cybersecurity measures, the balancing approach incorporates both technology-driven solutions, such as encryption and intrusion detection systems, and human-centered strategies, including continuous training and simulation-based drills, to equip maritime personnel with the skills necessary to identify and respond to cyber threats effectively.
3.2.2. Technological Challenges

Publication within this subcategory reveals that the challenges in autonomous ship operations are multifaceted, including regulatory and technological aspects. That is, the complexities of advanced technology also introduce new challenges that affect autonomous ship operation. This includes increased risks of cyberattacks and other potential threats. Understanding and addressing these challenges is vital for the smooth operation of uncrewed ships. A primary approach involves identifying inherent obstacles and devising effective solutions to enhance safety and security. Studies like [64] have focused on developing robust communication and network systems for autonomous ships. Similarly, Thieme et al. (2018) emphasized the importance of assessing risks, including technical reliability, software performance, and human–machine interactions [65]. Addressing technological challenges necessitates the development and implementation of robust systems and networks to provide cyber-enabled solutions, thereby offering potential mitigation strategies for operational risks.

3.3. Technological Assistance

This section identifies the technologies used to enhance the safety and security of autonomous ship operations, particularly focusing on cybersecurity, emergency response capabilities, and collision avoidance.

3.3.1. Cybersecurity

Publications in this category reveal methodological approaches to enhancing cybersecurity, emphasizing the need for comprehensive risk assessments and proactive planning. For example, Le Tixerant et al. (2018) discuss the use of data from automatic identification systems (AIS) to improve maritime spatial strategies and reduce cyber threats [25]. This approach emphasizes the significance of data utilization for risk assessment and enhancing maritime security. Blockchain technology can enhance the cybersecurity of autonomous ships by providing a secure, decentralized method for data exchange and communication. By encrypting data and distributing them across a network, blockchain makes it significantly more difficult for unauthorized parties to compromise the system's integrity. This technology not only secures communication channels but also ensures the authenticity and reliability of navigational data, crucial for safe autonomous operations. There is, however, a notable gap in the discourse on using AI to enhance cybersecurity practices and to predict threats.

3.3.2. Emergency Response

Addressing emergency response capabilities in autonomous ship operations is crucial. The literature in this subcategory emphasized the adaptation of models and technologies from other autonomous systems, like autonomous cars, to maritime contexts. Azam et al. (2022) highlight the use of STRIDE and LINDDUN models to scrutinize data threats and enhance emergency response [26]. Some publications also explored the use of remote diagnostics and integrated automation systems as means to improve emergency response in autonomous ships [29,31].

3.3.3. Collision Avoidance

Effective collision avoidance management is vital for the safety of autonomous ships. Publications in this subcategory suggest various methodical approaches for developing and implementing collision avoidance technologies. Hu et al. (2020) provide insights into practical avoidance technologies, suggesting that the implementation of the COLREGs is an innovative solution for managing collision risks [14]. Leveraging artificial intelligence (AI) and machine learning, autonomous ships can utilize predictive analytics to enhance their collision avoidance capabilities. By analyzing vast amounts of data from past incidents, weather patterns, and real-time sensor input, AI algorithms can predict potential hazards and optimize navigational decisions. This approach not only improves safety but also
enhances the efficiency of maritime operations by enabling more precise and adaptive route planning.

4. Discussion

This section further interprets the findings from the results, offering practical insights relevant to the research questions. Figure 3a suggests that there has been a growing interest since 2015 in understanding the potential of autonomous ship operations and their implications to society. The decline in relevant publications after 2021 does not necessarily indicate a waning interest, but potentially a lack of studies in this realm due to the attention paid to problems in maritime logistics during the COVID-19 era. The dominance of topics related to technological assistance (Figure 2b) aligns with the maturation of enabling technologies such as GPS, navigational sensors, high-speed broadband communications, cloud computing, artificial intelligence, and advancements in cybersecurity, including blockchains. The dominance of authorship from Norway, the United Kingdom, China, and Finland (Figure 3b) aligns with historic dominance of ship building industries in these countries.

An essential aspect of advancing autonomous ship operations lies in understanding and navigating the evolving regulatory landscape. The shift towards autonomous shipping is not merely a technological leap but also a regulatory challenge, requiring a re-evaluation of existing maritime laws and conventions. This discussion acknowledges the significant strides made in technology and performance standards but also highlights the urgent need for comprehensive regulatory frameworks that specifically address the unique aspects of autonomy in maritime operations. The subsections that follow focus on various risks under the three research questions focusing on their causes and consequences.

4.1. Threat Evaluation

Exploring the various methodologies and categories is essential to understanding the risks associated with autonomous ship operations. The foundational framework provided by the IMO for assessing ship autonomy is pivotal in identifying potential threats. These threats, encompassing collision risks, operational complexities, cybersecurity vulnerabilities, and safety compliance concerns, form the core of the evaluative process for autonomous ships. A critical aspect of this evaluation is the recognition of the dual nature of technological advancements in autonomous ships: they both mitigate and introduce risks. For instance, while autonomy reduces human error, leading to fewer collisions and operational mistakes, it simultaneously increases reliance on technology, which could lead to new forms of cyber threats and safety compliance issues. This dual nature illuminates the importance of a sophisticated approach to threat evaluation, which must encompass a broad spectrum of risk factors including technological vulnerabilities, operational challenges, and regulatory compliance. These considerations must seamlessly integrate into the broader context of autonomous ship operation. There must be ongoing regulatory development and clarification based on the continuous interaction between technological advancements and regulatory frameworks. Furthermore, comprehensive threat assessments must consider both the benefits and challenges of autonomy in the maritime industry. This assures that the evaluation of threats remains aligned with the evolving landscape of autonomous ship operations to address both current and future risks.

4.2. Performance Standards

The SLR provided an in-depth analysis of the performance standards of autonomous ships, primarily in terms of safety and security compliance. Although the IMO has begun to lay down the foundational framework concerning the guidelines of autonomous ships, there is a critical need for further development and clarification in these regulations. The reviewed literature revealed a need for a comprehensive understanding of both traditional and autonomous ship operations. Studies such as those by Petrig (2020) [56] and Nzengu et al. (2021) [52] emphasize the importance of integrating advanced sensor technologies,
autonomous navigation systems, and adherence to international maritime regulations. The integration of advanced sensor technologies and navigation systems in autonomous ships highlights a significant departure from traditional practices, where manual oversight and conventional navigation methods prevail.

Recent advancements in sensor technology and autonomous navigation systems are crucial in enhancing the performance standards of autonomous ships. High-resolution optical and thermal imaging sensors now enable precise object detection and classification even under adverse weather conditions [75]. Additionally, the integration of LiDAR and radar technologies facilitates detailed 3D mapping of the ship’s surroundings, enhancing navigational accuracy [76]. Sophisticated autonomous navigation systems complement these technologies by incorporating machine learning algorithms to optimize route planning and collision avoidance strategies [77]. These systems not only improve operational efficiency but also significantly enhance maritime safety by reducing human error and response times.

Other key aspects include regulatory frameworks, safety protocols, risk assessments, and the integration of HMI s. A critical finding is the significance of advanced algorithms and technologies in improving performance standards and mitigating regulatory challenges, such as those associated with the implementation of COLREGs in autonomous ship navigation. However, challenges like HMI errors and the development of effective risk management strategies remain areas that need further attention [78].

4.3. Vulnerability Assessment

In evaluating the vulnerability of autonomous ships, comparing these risks to those faced by traditional ships highlights the unique challenges of cybersecurity and piracy in the context of ships’ autonomy. Traditional ships, while not immune to cyber threats, rely more heavily on physical security measures and less on cyber protections. This contrast highlights the critical need for robust cybersecurity frameworks tailored to the autonomous maritime environment, where the interplay of advanced technologies presents both opportunities and vulnerabilities. The assessment of maritime vulnerability requires a detailed identification of potential threats and breaches in autonomous ship operations. The current regulatory vacuum in specific cybersecurity standards for ships’ autonomy exacerbates the complexity of securing autonomous ships against cyber threats. The existing regulations governing traditional shipping practices offer a foundation, but they fall short in addressing the sophisticated cyber risks associated with fully autonomous operations.

The discourse on vulnerability assessment for autonomous ships in terms of safety and security compliance falls into several themes, including cybersecurity vulnerabilities, maritime piracy threats, regulatory inadequacies, collision avoidance and security risks, and mitigation strategies. A notable point from the literature is the heightened vulnerability of autonomous ships to cyberattacks due to the complex interactions between systems, components, and humans. This complexity arises from factors like onshore system installation, software usage, and increased connectivity, necessitating robust and comprehensive cybersecurity measures.

4.4. Limitations

One potential limitation is the reliance on specific databases, which may not encompass all relevant publications, especially grey literature or emerging studies not yet indexed. Additionally, the restriction of the language to English could omit significant research published in other languages, thereby narrowing the scope of the review. Future research could mitigate these limitations by expanding the search to include more diverse databases, incorporating grey literature, and considering studies published in multiple languages. This approach would broaden the review’s comprehensiveness and reduce potential biases in the selection of publications.

This study sets the stage for future work to conduct a deeper analysis of the technological landscape in autonomous ships, for instance, by examining the role of AI in
enhancing navigational safety, cybersecurity measures to protect against hacking and data breaches, and the use of sensor fusion for improved situational awareness. Future work should also examine the limitations of technologies such as AI in decision making under uncertain conditions and the challenges in ensuring robust cybersecurity in a maritime context. Additionally, exploring the potential for future technological advancements to overcome current limitations will offer valuable insights into the direction of ongoing research and development in maritime autonomy. Additionally, case studies will validate the theoretical discussions and provide practical lessons for future implementations of autonomous maritime operations.

5. Conclusions

This systematic literature review has critically analyzed the integration of safety and security technologies within autonomous maritime operations, directly addressing the three formulated research questions. First, the findings highlight that the evaluation of threats to autonomous ships increasingly relies on advanced simulation and predictive analytics to assess potential vulnerabilities and compliance with international safety standards. This aligns with the first research question by demonstrating how threat evaluation methodologies have evolved in response to technological advancements. Second, in addressing the second research question on principal operational challenges, this study found that the balance between automation and human oversight is crucial. The literature emphasizes the need for robust human–machine interfaces that enhance decision making in complex navigational scenarios. These findings suggest a growing recognition of the need to integrate ergonomic design principles and cognitive load management into autonomous system operations to mitigate human error and enhance safety. Third, regarding the final question on the employment of technologies to mitigate threats, this review identified a significant trend towards the adoption of AI and machine learning for real-time threat detection and response. This supports the deployment of intelligent systems capable of enhancing the predictive maintenance and operational integrity of autonomous ships.

Overall, this review substantiates that the maritime industry is employing more automation, with clear advancements in safety and security technologies. However, it is imperative that future research continues to explore these dimensions in conjunction with evolving regulatory frameworks and the socio-economic impacts of autonomous ships’ deployment. Such holistic investigations will ensure that the transition towards fully autonomous maritime operations does not compromise safety and security but rather enhances it, benefiting the entire maritime community.

Author Contributions: Conceptualization, R.A. and R.B.; methodology, R.A. and R.B.; software, R.A. and R.B.; validation, R.A. and R.B.; formal analysis, R.A. and R.B.; investigation, R.A. and R.B.; resources, R.B.; data curation, R.A. and R.B.; writing—original draft preparation, R.A. and R.B.; writing—review and editing, R.A. and R.B.; visualization, R.A. and R.B.; supervision, R.B.; project administration, R.B.; funding acquisition, R.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This article includes the data presented in the study.

Conflicts of Interest: The authors declare no conflicts of interest.

References


33. Lee, S.-W.; Jo, J.; Kim, S. Leveraging the 4th Industrial Revolution Technology for Sustainable Development of the Northern Sea Route (NSR)—The Case Study of Autonomous Vessel. Sustainability 2021, 13, 8211. [CrossRef]


70. Koumentakos, A.G. Developments in Electric and Green Marine Ships. *Appl. Syst. Innov.* 2019, 2, 34. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.