SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

Guidelines for Cyber Risk Management in Autonomous Shipping

1st Edition Volume 2

Published 18th Jan 2024

TERMS OF USE

The guidelines are solely intended for use as a reference or guide at the user's own risk. The authors and contributors are not responsible for the accuracy and efficacy of any information or recommendations provided or omitted in this document or for any issues or failures caused, directly or indirectly, as a result of the use of the guidelines.

Executive Summary

The emergence of autonomous ships represents a significant advancement in maritime technology, promising enhanced efficiency, reduced operating costs and reducing or even completely removing crews from hazardous environments. However, the progress is accompanied by a burgeoning concern on the cyber security of these autonomous ships due to their exposure to the connected world.

The four key systems investigated in the guidelines are: 1) Shore Control Centre (SCC)[1]; 2) Communication System; 3) Autonomous Ship Controller (ASC), comprising the Autonomous Engine Monitoring and Control System (AEMCS), Anchoring and Mooring System (AMS), Stability and Integrity System (SIS) and Cargo Handling System (CHS); and 4) Autonomous Navigation System (ANS), comprising the Navigation and Situation Awareness System (NSAS), Route and speed Optimisation Planning System (RSOPS), Collision Avoidance System (CAS) and Weather Monitoring and Interpretation System (WMIS). SCC enables monitoring and control but also introduces remote hacking pathways into ships. ANS fuses sensor data to guide ships independently but also could be blinded or fed misinformation by attackers. Communication links connecting a ship to the shore and between ships are vulnerable to attacks such as jamming, spoofing and interception. Centralised ASC functions are akin to a virtual captain and play a pivotal role in assisting SCC, which can have adverse impacts if compromised.

The interconnectivity of systems within autonomous ships forms a complex web where various components collaborate seamlessly. However, the crux of their vulnerability lies not in this interconnectedness itself, but in their exposure to the broader connected world. When a component or system is compromised, the repercussions cascade through the intricate network, leading to multifaceted effects. On the other hand, a disruption in one area could potentially impact navigation, communication and other systems interacting with it. To counteract this vulnerability, it is imperative that stringent cybersecurity measures are integrated into the design of ship systems and robust contingency plans are implemented (and revisited) to bolster the ship's cyber hygiene and resilience.

The guidelines presented in this document aim to provide an effective protection guide for stakeholders (shipowners, maritime authorities etc.) to bolster their cybersecurity posture by highlighting specific operational technology (OT) risks associated with MASS (Maritime Autonomous Surface Ship). For completeness, the guidelines include cyber risks and impacts associated with sub-systems of these major OT systems. A comprehensive cyber risk assessment methodology based on the MITRE framework is employed to evaluate the severity of risks. Recommended mitigations include defence-in-depth cybersecurity protections for all systems, security-by-design approaches, personnel training and redundancy in certain critical systems. Finally, a checklist is also included to assist operators in regular hygiene assessments.

[1] An alternative term that emphasises remote operations is "Remote Control Centre" (RCC). In this document, SCC may be considered better than RCC as it offers a clear indication that the centre is managing maritime operations based on or near the shore. This term is often more commonly used and recognised in maritime contexts. However, the choice between two terms depends on the specific needs of the industry.

Table of Contents

LIST OF ABBREVIATIONS

AMS	Anchoring and Mooring System
ANS	Autonomous Navigation System
ASC	Autonomous Ship Controller
AAWA	Advanced Autonomous Waterborne Applications
ABS	American Bureau of Shipping
AIS	Automatic Identification System
BV	Bureau Veritas
C2	Command and Control
CAS	Collision Avoidance System
CCS	China Classification Society
CHS	Cargo Handling System
CIA	Confidentiality, Integrity and Availability
COLREGs	Convention on the international Regulations for Preventing Collisions at Sea, 1972
CPA	Closest Point of Approach
DNV	Det Norske Veritas
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IMO	International Maritime Organization
IT	Information Technology
KR	Korean Register
LAN	Local Area Networks
LiDAR	Light Detection and Ranging
LR	Lloyd's Register
MARS	Mayflower Autonomous Research Ship
MASS	Maritime Autonomous Surface Ship
MitM	Man-in-the-Middle Attack
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
NAVTEX	NAVigational TEleX
NTNU	Norwegian University of Science and Technology
OS	Operating System
OT	Operational Technology
RADAR	*RAdio Detection And Ranging*
RSOPS	*Route and Speed Optimisation Planning System*

SAS	*Samsung Autonomous Ship*
SCC	Shore Control Center
SIEM	Security Information and Event Management
SIS	Stability and Integrity System
SMAV	Smart Maritime Autonomous Vessel
UHF	Ultra-High Frequency
USB	Universal Serial Bus
VDR	Voyage Data Recorder
VHF	Very High Frequency
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WMIS	Weather Monitoring and Interpretation System

1: INTRODUCTION

A significant transformation in terms of advancements in technology, shifts in customer behaviours and changes in the competitive landscape is in underway with the emergence of autonomous ships [1]. The International Maritime Organisation (IMO) defines MASS as "a ship which, to a varying degree, can operate independent of human interaction." Four degrees of automation are listed by IMO [2]:

"Degree one: 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."

"Degree two: 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."

"Degree three: Remotely controlled ship without seafarers on board. The ship is controlled and operated from another location. There are no seafarers on board."

"Degree four: Fully autonomous ship. The OS of the ship is able to make decisions and determine actions by itself."

This study focuses on Degree 3 MASS because it strikes a balance between automation and human involvement. The prevailing academic literature and established guidelines within the autonomous shipping domain prioritize the notion of 'remotely controlled' over 'completely autonomous'. Human operators will continue to be essential for ensuring the safety, security, and widespread acceptance of autonomous ships in the foreseeable future [3, 4]. We favour Degree 3 autonomy due to its potential for unmanned or minimally manned operations. A Degree 3 autonomous ship possesses the ability to perceive its surroundings, chart optimal collision-free routes in compliance with maritime regulations, and regulate propulsion systems to adhere to planned trajectories while avoiding potential hazards. It solicits human input solely when faced with unprecedented circumstances beyond its operational scope, activating alerts in case of anomalies. The envisaged autonomous and automation systems are designed to function robustly and securely for extended durations with minimal onshore supervision. However, the extensive reliance on the interconnected network connecting the ship to the SCC amplifies the vulnerability to cyber-attacks [5]. Notably, a critical limitation of Degree 3 systems lies in their incapacity to dynamically evaluate their competency and revert control to human operators when autonomy falters. Instead, they depend on operators to actively monitor for any arising issues. This constraint implies that autonomous ships at sea will likely necessitate ongoing vigilance from onshore personnel. Onboard systems are exposed to risks such as malware infections, and some AI-based models integrated into these systems are susceptible to adversarial attacks [6, 7]. Furthermore, given that seamless connectivity between ship and shore infrastructures forms the cornerstone of autonomous and remotely controlled technologies, cybersecurity assumes a paramount role in ensuring the operational efficacy of these ships.

One of the objectives of this research is to precisely define the intended scope of autonomous ships, as cyber-attack surfaces are contingent upon the degree of autonomy [8]. The focus of this

investigation is to mitigate the cyber threats by recommending appropriate cybersecurity measures to protect the ship's operation and data. Numerous other directives, as put forth by organisations such as the Lloyd's Register (LR), Det Norske Veritas (DNV), Bureau Veritas (BV), Maritime UK, China Classification Society (CCS), Russian Maritime Register of Shipping (RS), ClassNK, American Bureau of Shipping (ABS), and Korean Register (KR), primarily emphasise offering counsel concerning secure design and functional prerequisites in autonomous systems, encompassing certain facets of cybersecurity precautions. These guidelines duly recognise that autonomous ships necessitate an all-encompassing strategy consisting of risk assessment, technical dependability, operational safety, human factors, and cybersecurity throughout the complete lifecycle of the system. Nevertheless, we find that there is a gap in the understanding - and conversely the identification - of cyber threats, and viable mitigation strategies that can be promptly implemented by engineers, IT specialists, and vessel inspectors. Hence, this research aspires to bridge this gap and provide a comprehensive and easy-to-use guidelines for MASS stakeholders.

The structure of this document is organised as follows: Firstly, it lists down shipboard Operational Technology (OT) systems and their respective sub-systems found in a typical or anticipated MASS of autonomy Degree 3. Secondly, it lists the cyber threats linked to these OT systems by examining how they can be attacked and the possible scenarios. Thirdly, it presents a set of risk control measures designed to mitigate the identified cyber risks. Fourthly, a cyber risk assessment methodology, developed in conjunction with a scholar from NTNU, is illustrated. Putting these findings together, this document presents a checklist for assessing, monitoring and enhancing the security posture of MASS. It also aspires to serve as a pragmatic guide for those tasked with ensuring the cybersecurity of MASS. Figure 1 depicts the roadmap undertaken in developing the guidelines.

The key distinction between IT and OT lies in the fact that an attack on IT typically doesn't pose a threat to life or the safe operation of systems. Conversely, an attack on a ship's OT system introduces a significant risk to the safety of both the crew and passengers. According to Naval Dome's report, there was a 900% increase in OT attacks over three years, rising from 50 in 2017 to 120 in 2018 and further escalating to 310 in 2019. As such, OT systems are the focus of this study.

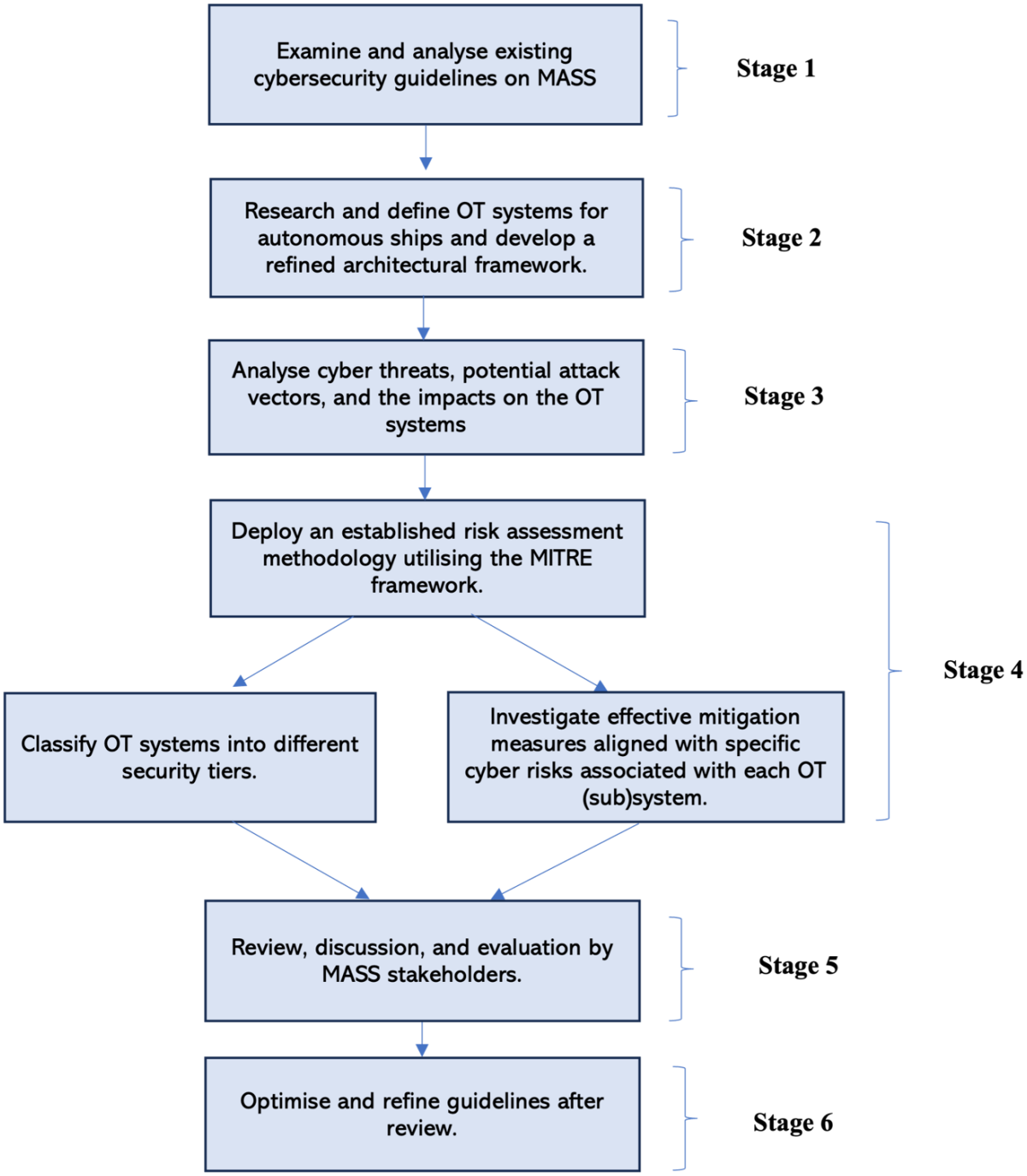

Figure 1 Roadmap for Producing the New Guidelines

Stage 1

Initially, a comprehensive examination of existing cybersecurity guidelines pertaining to MASS is carried out. This involves analysing guidelines from various institutions and major maritime organizations. The aim is to identify widely accepted and implemented cybersecurity principles, frameworks, and best practices within the domain. A gap analysis is ensured to determine areas where the existing guidelines may need enhancements or adaptations to suit the autonomous nature of MASS.

Stage 2
An in-depth examination was conducted on MASS OT systems and their respective sub-systems. The foundational architectural framework is based on a paper published by Aalto University entitled "An initial hierarchical systems structure for systemic hazard analysis of autonomous ships" and subsequently refined [9].

Stage 3
The impacts specific to each associated system were individually addressed. In our analysis of cyber risks and corresponding mitigation strategies, we also drew insights from a variety of sources. Understanding cyber threats and attack vectors helped in developing effective cybersecurity strategies.

Stage 4
This stage encompasses the integration of study conducted by a SUTD Master student, focusing on a related subject matter [10]. Moreover, we sought and incorporated valuable feedback from esteemed researchers and instructors in this domain, including researchers from the University of Plymouth, the Norwegian University of Science and Technology, and Aalto University, who provided enlightening recommendations. Additionally, we initiated a more profound collaboration with NTNU scholar to deploy a robust cyber risk assessment methodology [11]. It assesses cyber risk in cyber-physical systems using the MITRE ATT&CK framework.

Stage 5
Furthermore, advice is also sought from industry partners to enhance its practicality. These are individuals or entities with an interest or involvement in MASS. During this stage, the team enhances the guidelines' content based on feedback received from a variety of stakeholders. The iterative process ensures that the guidelines are optimised to meet the needs and expectations of all involved parties. Any valuable insights or suggestions provided by stakeholders are carefully considered and integrated to enhance the overall quality of the document.

Stage 6
The guidelines are finalised.

2: BACKGROUND

MASS marks a paradigm shift in maritime technology, where navigational decision making is partially or entirely influenced by advanced algorithms, optimisation, machine learning and a combination of old and new technologies onboard. However, this transition to crewless ships present significant challenges, as sensor technologies, real-time data processing and effective communication are paramount in the absence of crew. The challenges notwithstanding, there are several notable MASS projects (Table 1) that have contributed to technological advancements and shaping of and preparing for the future of autonomous shipping.

Table 1 List of Notable Autonomous Ship Projects

Country	Name of MASS Project	Brief Description	Duration of Project
European countries	Maritime Unmanned Navigation through Intelligence in Networks (MUNIN)	MUNIN represented a significant research venture generously funded by the European Commission. The primary aim of this initiative was to conceptualize, develop, and validate the potential of an autonomous dry bulk carrier. The project made substantial strides by creating prototypes for pivotal systems, including ANS and ASC and so on, subsystems including situational awareness, etc [12].	2012 - 2015
	ReVolt	ReVolt constitutes a collaborative project within Norway with a primary objective centred around the advancement of maritime transportation through the development of fully electric and autonomous vessels. The fundamental aim of ReVolt is to facilitate regional shipping that is not only zero-emission but also prioritises safety and cost-efficiency. The ambition is to demonstrate the viability and potential of autonomous electric ferries for both short-distance transportation and loner routes, promoting a greener future for the maritime sector [13].	2013 - 2018
	Advanced Autonomous Waterborne Applications (AAWA)	AAWA was a significant initiative focused on the development and implementation of autonomous ship technology, and it is a collaborative effort involving various stakeholders from both academia and industry. The principal aim of AAWA was to conceive and showcase modular	2015 – 2017* *Short runs by 2020. Ocean going by 2025.

		autonomy solutions tailored for maritime vessels, with the ultimate objective of fostering the adoption of autonomous shipping across Europe [14].	
	Mayflower Autonomous Ship (MAS)	The Mayflower Autonomous Ship (MAS) represents a notable achievement in autonomous maritime technology, constructed through a collaborative effort between ProMare, a marine non-profit research organization, and IBM. Equipped with hybrid electric propulsion supported by solar panels, this unmanned vessel possesses the capacity for extended operation. A significant milestone was achieved in June 2022 when MAS accomplished the inaugural fully autonomous transatlantic voyage, covering a distance from Plymouth, UK to Plymouth, Massachusetts [15].	2015 - 2020
	Yara Birkeland	Yara Birkeland, an autonomous electric container ship, developed through a partnership between Yara and Kongsberg. This cutting-edge vessel integrates a sophisticated autonomous navigation system encompassing a variety of sensors such as RADARs, cameras, and Automatic Identification System (AIS). These sensors collectively geared towards ensuring precise and safe navigation for the ship. Prominent attributes of the Yara Birkland encompass an electric propulsion mechanism reliant on batteries and an automated mooring system [16].	2017 - 2022
Singapore	Smart Maritime Autonomous Vessel (SMAV)	ST Engineering, situated in Singapore, has effectively concluded the preliminary sea trials within Singaporean waters for the pioneering Smart Maritime Autonomous Vessel project. The autonomous tug initiative necessitated the collision avoidance algorithm to adhere meticulously to the Convention on the international Regulations for Preventing Collisions at Sea, 1972 (COLREGS) rules, specifically concerning safe overtaking,	2019 - 2020

		head-on encounters, and vessel crossings [17].	
Japan	MEGURI2040	A Nippon Foundation-led initiative is underway to create a fully autonomous ship capable of operating without a crew or onboard support systems. This ambitious, long-term project is set to span the next two decades, with the primary objective of revolutionizing the shipping industry and mitigating its environmental footprint. Propelled by renewable energy sources, the autonomous ship serves as an eco-friendly alternative to conventional shipping methods [18].	2020-ongoing
China	Zhi Fei	Zhi Fei, translating to 'flying wisdom' in Chinese, represents a notable venture actualized by the Qingdao Shipyard. The commencement of its regular voyage on 22nd April marked a significant milestone. This state-of-the-art containership is engineered to seamlessly transition between various operational modes, encompassing manned driving, remote driving, and unmanned driving. Initiated in April 2021, the vessel underwent a meticulous process of sea trials and comprehensive system testing, diligently evaluating its technical capabilities. This scrutiny culminated in a thorough technical evaluation in March 2022 [19].	2021 - 2022
Korea	Samsung Autonomous Ship (SAS)	Samsung Heavy Industries has signed a Memorandum of Understanding (MOU) to develop an autonomous ready ship design to support maritime digitalisation and then brought in Kongsberg Maritime to work on the ongoing autonomous ship technology program. The Samsung Autonomous Ship (SAS) system for remote autonomous navigation processed data from the tug's integrated navigation and communication apparatus, encompassing RAdio Detection And Ranging (RADAR), Global Positioning	2022-ongoing

		System (GPS), and AIS, in order to promptly identify nearby vessels and potential obstructions. Subsequently, the onboard computer system analysed this data to assess collision risks within the ship's operational parameters, devising optimal navigational decisions to avert any impending hazards [20].	

MUNIN's work provides early insights into the potential for autonomous merchant vessels to offer benefits like lower operating costs and safer navigation. The project's concepts, findings and prototyping serve as an important foundation for subsequent advances in maritime automation. While fully autonomous ships at large scale have still not been realised, MUNIN represented an influential pioneering initiative in autonomous shipping R&D [12].

ReVolt aims to revolutionise the ferry industry by introducing vessels that are not only autonomous but also run on clean energy sources, mitigating environmental footprint. Extensive research is conducted within the project to advance critical aspects like battery safety, grid integration, and elevated situational awareness [13].

The objective of AAWA is to expedite research and development, address regulatory impediments, and define benchmarks, thereby facilitating the progressive development of fully autonomous vessels for diverse applications such as inland waterway transport, coastal shipping, and ocean-going vessels [21]. The project plays a pivotal role in advancing fundamental components and blueprint structures crucial for the construction of autonomous ships.

The Mayflower project demonstrates the potential for AI and automation to chart new possibilities in oceanic data gathering, maritime research, and seafloor mapping. The collaborative partners envision broadening the scope of testing to encompass more intricate scenarios and embarking on further research expeditions to demonstrate the extensive capabilities of this autonomous maritime vessel [15].

Yara Birkeland represents a push towards more sustainable logistics. As a pioneering autonomous vessel project moving towards full unmanned operations, it provides key insights into technology development, regulatory approvals, and commercial adoption challenges for autonomous shipping [22].

The SMAV project represents a pivotal contribution within a range of cutting-edge industry initiatives aimed at guiding the formulation of the recently released ABS Guide for Autonomous and Remote Control Functions [23].

On January 11, 2022, a compact autonomous tourist boat achieved a milestone by autonomously navigating the waters near Sarushima, an island situated off the coast of Yokusuka City in Kanagawa Prefecture. This marked the world's inaugural successful demonstration of entirely autonomous navigation, encompassing automated guidance from departure to docking, for a small tourist boat [24].

Zhi Fei is actively engaged in operations, navigating the route between Qingdao Port situated in Shandong Province and Dongjiakou. These operations are adeptly managed by the esteemed shipping entity, Navigation Brilliance (BRINAV). Zhi Fei has been identified as a demonstrative vessel intended to yield substantial insights and knowledge crucial for the forthcoming advancements in this technology [19].

It is evident from these MASS projects that the ships are jam-packed with technologies that facilitate varying degrees of automation and with them, cybersecurity challenges. Recognising the uncertainties around the operation of MASS, Lloyd's Register (LR), Det Norske Veritas (DNV), Bureau Veritas (BV), Maritime UK, China Classification Society (CCS), Russian Maritime Register of Shipping (RS), Nippon Kaiji Kyokai (ClassNK), American Bureau of Shipping (ABS), IRCLASS – Indian Register of Shipping and Korean Register (KR) have published guidelines around the safe design, construction and operation – cyber or otherwise – of MASS (Table 2).

All the guidelines for cyber risk management on conventional ships are excluded as it was done in previous work. In the initial edition (Volume 1), a framework was introduced to manage cyber risks within the maritime sector. It specifically addressed the OT systems of conventional ships.

Table 2 List of Existing Guidelines

Name of the Publisher	Name of the Document	Year of Publication
KR	Guidance for Autonomous Ships	2022
Maritime UK	Maritime Autonomous Surface Ships (MASS) UK Industry Conduct Principles and Code of Practice 2022 (V6)	2022
ABS	Guide for Autonomous and Remote-Control Functions	2021
IRCLASS	Guidelines on Remotely Operated Vessels and Autonomous Surface Vessels	2021
ClassNK	Guidelines for Automated/Autonomous Operation on ships (Ver.1.0)	2020
RS	Regulations for Classification of Maritime Autonomous And Remotely Controlled Surface Ships (MASS)	2020
BV	Guidelines for Autonomous Shipping	2019
CCS	Guidelines for Autonomous Cargo Ships	2018
DNV	Remote-Controlled and Autonomous Ships	2018
LR	Cyber-enabled ships: ShipRight procedure – autonomous ships (First edition)	2016

The recommended *Guide for Autonomous Ships* by KR presents a comprehensive 5-level cyber autonomy model, spanning from fundamental cyber access to complete autonomy devoid of any onboard presence. Detailed system configuration and ship characteristics are set for each autonomy level. Additionally, a risk-centric approval framework for remote-controlled and autonomous ship systems is outlined within this guide [25].

In 2022, Maritime UK unveiled the third iteration of the *Maritime Autonomous Surface Ships UK Industry Conduct Principles and Code of Practice (V6),* a voluntary code. According to the Industry Code of Practice established by Maritime UK, this code aims to establish standards and best practice for those who design, build, manufacture, own, operate and control MASS of those under 24 meters in length. The central objective was to formulate policies aligning with the anticipated technological, commercial, and regulatory advancements for deployment of autonomous vessels in UK waters [26].

The ABS introduced *Guide for Autonomous and Remote Control Functions* providing guidance for applying risk-based approval process to autonomous and remote control features on marine vessels. It introduced notable aspects such as the AUTONOMOUS and REMOTE-CON notation and a distinct acknowledgment of remote-control functions. The guide delineates a goal-oriented

framework to facilitate the integration of these technologies within vessels and offshore units [27].

The primary objective of the current elevated *Guidelines on Remotely Operated and Autonomous Surface Vessels* published by IRCLASS centres on vessels showcasing diverse levels of autonomy. The main purpose of its manuscript is to furnish a comprehensive framework, drawing from industry best practices, for stakeholders engaged in the design, construction, and testing phases of such vessels [28].

Guidelines for Automated/Autonomous Operation on ships (Ver.1.0) published by ClassNK presents a comprehensive approval scheme covering technical, operational, human factors and documentation prerequisites. The guidelines referenced also provides frameworks for vessels with remote control capabilities. This framework serves to evaluate safety elements for remotely controlled and autonomous ship systems [29].

The RS-published *Regulations for the Classification of Maritime Autonomous and Remotely Controlled Surface Ships (MASS)* encompass specifications for the electrical, automation, radio, and navigational equipment employed in autonomous ships. Additionally, it outlines a risk-oriented procedure aimed at maintaining a safety standard during the operation of MASS.

Both CCS's *Guidelines for Autonomous Cargo Ships* and BV's *Guidelines for Autonomous Shipping* strongly focus on the functional requirements of autonomous systems. They provide a safety and functionality-oriented scheme to support autonomous shipping adoption. To ensure system reliability, safety goals are determined from quantitively risk assessment [30, 31].

DNV's *Remote-Controlled and Autonomous Ships* elaborates on the regulatory landscape and the compliance verification process that autonomous ships must undergo to meet international and industry standards. It also emphasizes the safety assurance management to ensure protection against cyber threats [32].

Lloyd's Register's guidelines with title *Cyber-enabled Ships: ShipRight Procedure – Autonomous Ships (First Edition)* present a specialized framework concentrating on cybersecurity, pivotal for the seamless functioning of autonomous ships that heavily depend on integrated digital systems. The guidelines maintain a continuous focus on cybersecurity aspects, integrating them comprehensively into the development and lifecycle of autonomous systems [33].

While the guidelines exhibit differences in their use of terminology and focus areas as shown in Figure 2, they provide useful background information and a strong foundation upon which we can build our own technical guidelines on the cybersecurity risks in MASS. We use symbols – empty, semi and filled circles - as visual indicators to represent different levels of completion and depth (Figure 2), and define them as follows:

1) Empty Circle: An empty circle is used to indicate that a specific aspect or content element in the table is completely missing or not addressed at all. It represents a "lack of content" in that category.

2) Filled Circle: A filled circle is used to represent full or complete content in each category. It indicates that all relevant information is included, and there are no gaps in that specific aspect.

3) Semi Circle: A half circle (or a semicircle) is used to show partial completeness or depth. It signifies that there is some content present, but it's not exhaustive or complete. This may suggest that additional information is needed to fully address that category.

These symbols are used as part of a legend to provide a quick visual overview of how well each category is addressed in the listed guidelines work.

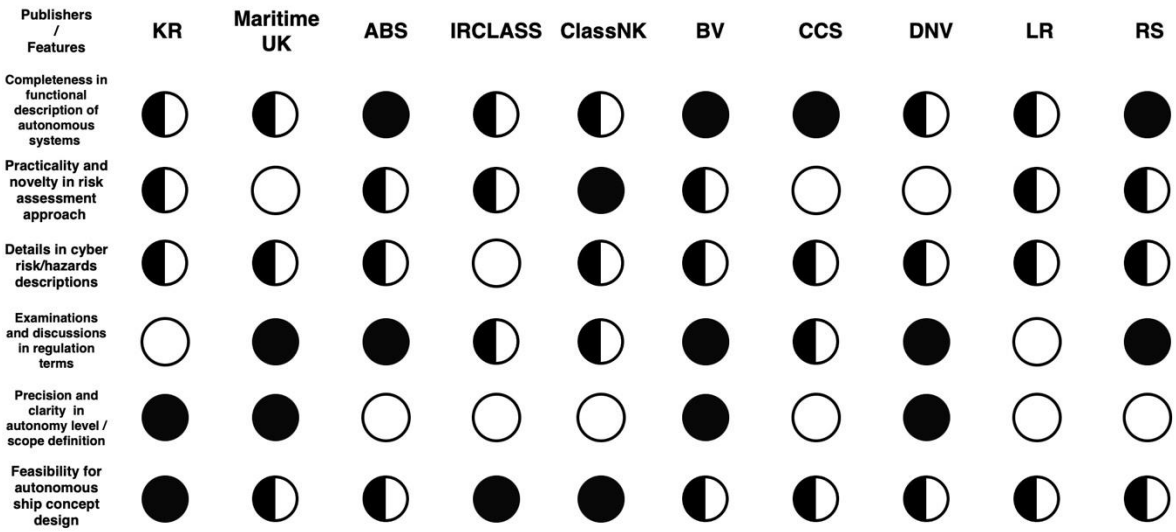

Figure 2 Existing Guidelines Comparison

Specifically, we identified a gap in cybersecurity strategies and cyber risk analysis tailored for individual systems in MASS that we aspire to fill. We also wish to add depth and granularity to risk analyses, including the human factor (or lack thereof), so that readers can better understand where they stand vis-à-vis the cybersecurity measures, they have already implemented. As an evolving field, we are cognizant that these guidelines must remain organic and respond to new developments and challenges, to continuously offer updated and relevant mitigation strategies.

3: SHIPBOARD AUTONOMOUS OT SYSTEMS

We define the OT systems in MASS to include pivotal components that play a crucial role in enabling autonomous operations, namely the Shore Control Centre (SCC), the Communication System, the Autonomous Ship Controller (ASC), and the Autonomous Navigation System (ANS), as illustrated in the Figure 3. This list is built upon the analysis of research projects and literature on autonomous ship systems. We then break down the primary OT systems deployed on autonomous ships into their subsystems. By doing so, it allows us to understand the diverse systems and their individual components, as well as the complex interactions and interconnections between and among them, which collectively contribute to enable the ship's autonomy.

There is a lack of consensus among researchers regarding the systems that a typical autonomous ship should include. During the exploration stage, we endeavored to encompass as many systems, sub-systems, and units as possible. However, in the end, we chose to compile a list of the most essential systems. These were selected from various academic papers, journals, and materials. Certain vital systems might not be referenced because of their limited coverage in research materials.

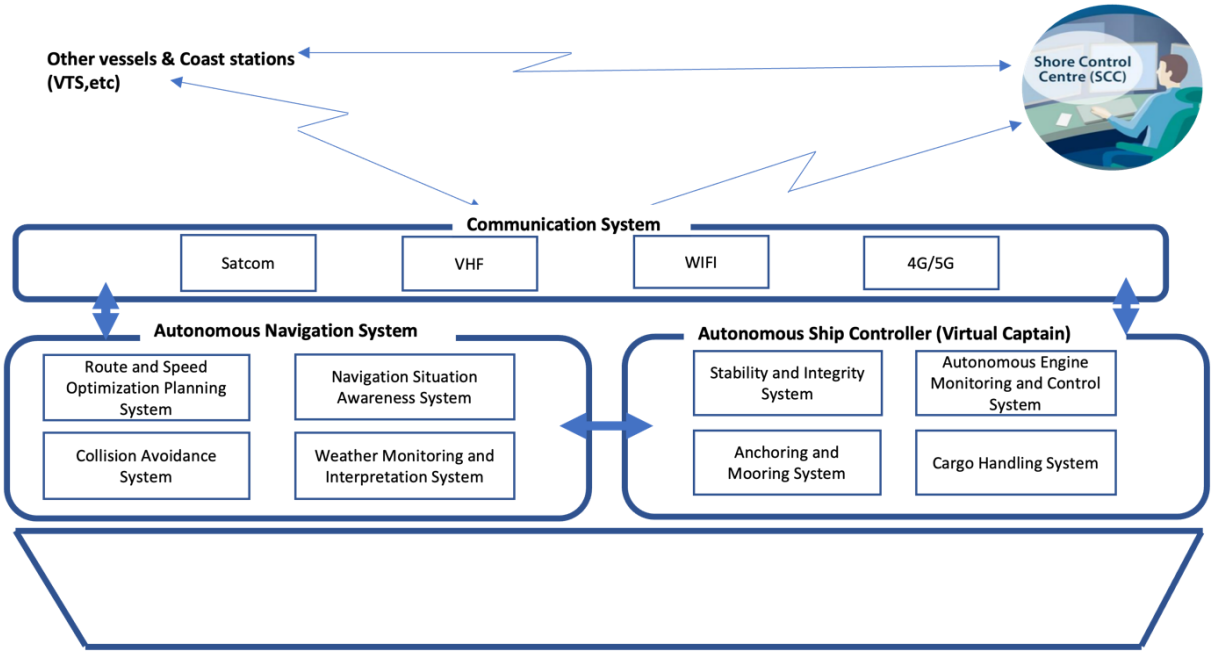

Figure 3 Modified System Overview of an Autonomous Ship [10]

3.1 SHORE CONTROL CENTRE (SCC)

The SCC refers to a land-based station and it is a backbone that enables the remote monitoring and control of autonomous ships from shore, and is considered an essential component in the foreseeable future for autonomous shipping in IMO's Degree Two and Three autonomy. The operators at SCC may initiate remote control for general oversight of the autonomous ship or to switch to the manual mode to handle specific hazardous or emergency situations that are beyond the ship's autonomous capabilities [31, 34, 35]. SCC requires a specific human-machine interface

design and acts as a hub for human operators to supervise unmanned maritime operations through sensor data analysis, communications' links, and active control interventions when required [36]. Equipped with advanced automation and decision support systems, SCC allows qualified personnel off-board instead of onboard, to conduct critical functions such as emergency response coordination, navigation assistance, and regulatory compliance for autonomous vessels. As such, humans at SCC should also be accounted for as part of a remotely controlled ship, given the crucial interactions between the human and automation systems [37]. By providing a link between autonomous ships and expert human monitoring, SCC aims to enable safer, more efficient and reliable maritime autonomous operations at a broad level.

3.2 COMMUNICATION SYSTEM

The communication system on autonomous ships enables connectivity for monitoring, control, and coordination between the ship, other ships, and shoreside centres. For ship-to-ship communication, AIS and VHF radio allow autonomous ship to enhance situational awareness and exchange vital information with other ships at sea. Within the ship, networks and industrial protocols can be used to connect various onboard systems and components. It allows subsystems such as navigation and engine monitoring to communicate effectively to synchronize ship operations. Lastly, the communication system establish a reliable link between the autonomous ship and the SCC for the transmission of critical operational data. Communication between ships and the shore facilitates remote control and monitoring by onshore operators, fosters data exchange for informed decision-making, and effectively manages emergency situations [31, 38]. Long range satellite links enable consistent global coverage for monitoring and emergency situations with the shoreside operators. Higher bandwidth options like 4G and 5G cellular provide supplementary connectivity near coasts. In scenarios with high traffic, such as port areas, IP-based protocols, high-data-rate networks utilising advanced cellular networks like 5G and beyond, and Wi-Fi systems are pivotal for efficient data exchange and remote control [10].

3.2.1 Satellite Communication System (SATCOM)

SATCOM is a pivotal and indispensable technology in autonomous ship operations, as it ensures consistent, efficient, and reliable communications by leveraging on satellites to establish robust communication channels [10]. The benefits that SATCOM brings to MASS are:

a) Real-time connections with shore control centres, thus enabling effective and reliable command and control of their operations [39].
b) Facilitates seamless data exchange between ship and shore-based systems, enabling continuous monitoring, diagnostics, and remote troubleshooting of onboard systems [40].
c) Establishes reliable communication channels during emergencies for distress signals and coordination with rescue authorities. Additionally, it grants access to up-to-date weather forecasts and environmental information, thereby facilitating optimal route planning and aiding in the avoidance of hazardous weather conditions [41].

3.2.2 Terrestrial Communications – VHF, Broadband, Internet

Under SATCOM, terrestrial communications utilise land-based communication infrastructure and technologies to establish essential communication links between autonomous ships and external entities like control centres, maritime authorities, and other ships, especially in coastal areas or near port operations [10]. A reliable and efficient terrestrial communication infrastructure is

crucial in enhancing safety, situational awareness, and operational efficiency. In MASS, terrestrial communication encompasses a range of technologies:

a) Cellular Networks: Autonomous ships can make effective use of existing cellular networks, such as 4G and 5G, to facilitate wireless data transfer, voice communication, and internet connectivity. The shore-based control centre can leverage cellular networks to provide extensive coverage and high-speed data connectivity, enabling real-time information exchange with the autonomous ship. This empowers personnel at the shore-based control centre to exercise real-time control over the autonomous ship and monitor its operations [42].
b) Wi-Fi and Local Area Networks (LAN): Autonomous ships can establish Wi-Fi networks or LAN onboard to facilitate internal data exchange, sensor connectivity, and integrated control and coordination among various systems and devices such as propulsion, navigation, and power management. Additionally, these networks enable crew access to onboard resources and services [43].
c) Very High Frequency (VHF) and Ultra High Frequency (UHF) Radios: Widely employed in maritime communications, these communication technologies serve diverse functions, including ship-to-ship and ship-to-shore communication. Moreover, they play a critical role in complying with legal obligations, such as AIS transmissions [44].

3.3 AUTONOMOUS SHIP CONTROLLER (ASC)

The ASC assumes the role of a virtual captain, overseeing the autonomous operations of crewless ships. Serving as the central decision-making authority, it harnesses an integrated artificial intelligence model to perceive its surroundings, strategically plan routes, adhere to navigational protocols, and execute vessel manoeuvres akin to a human captain's capabilities [7]. By processing comprehensive sensor data from all subsystems within the autonomous navigation framework, the controller upholds situational awareness, averts potential hazards, and commands route adjustments, all while dynamically adapting to ever-changing sea conditions. Predominantly, the ASC autonomously manages navigation and directs the operation of propulsion and steering systems through an in-depth analysis of sensor data. However, it retains the capability to seamlessly transition control to remote human operators when unforeseen circumstances arise. The ASC's overarching objective is to replicate and enhance human navigational expertise via machine learning methodologies, thereby ensuring a harmonious collaboration between automation and human supervision in maritime operations.

3.3.1 Autonomous Engine Monitoring and Control System (AEMCS)

The AEMCS is a key subsystem within the autonomous ship controller that is responsible for robust automation and control. It could integrate additional subsystems such as autonomous navigation system (ANS), to ensure dependable propulsion power and provide feedback on the running condition [31]. Significant disparities in the power systems of conventional ships versus autonomous ships revolve around several key factors, including levels of automation and control, redundancy and safety measures, energy efficiency, and the integration of advanced sensor technologies [45]. Within this context, the AEMCS of an autonomous ship can be finely tuned for optimal fuel efficiency and improved producibility, leveraging advanced routing algorithms that consider variables such as weather conditions and traffic congestion through sensor systems. Furthermore, the AEMCS must facilitate autonomous ships in maintaining uninterrupted propulsion and power supply, especially when adhering to voyage plans and executing collision

avoidance manoeuvres [45]. The AEMCS presents substantial potential for enhancing operational efficiency and cost reduction.

3.3.2 Anchoring and Mooring System (AMS)

The anchoring and mooring system is a specialised sub-module within the autonomous ship controller. The goal is to guarantee the ship's safe arrival and departure at the dock, or anchoring and weighing anchor at designated anchorages, with effective securing at the predetermined position [31]. Both the anchoring and mooring operations align with the signals and data detected and received on a real-time basis. AMS conducts continuous real-time assessments of the ship's positioning and conditions to determine the suitability of anchoring and mooring manoeuvres [31]. It also relies on sensor data, environmental factors and navigational inputs to assist in making decisions. In the event of an emergency collision caused by the dragging of the ship's anchor, wherein the AMS loses the ability to maintain control over the vessel, it should be imperative for the system to establish communication with SCC to promptly alert operators.

3.3.3 Stability and Integrity System (SIS)

Since 2012, the emphasis on stability has remained steadfast in light of the heightened level of automation and collisions, groundings, and the subsequent water ingress leading to capsizing or sinking have consistently emerged as significant risk factors for ships [46]. The SIS, as a specialized subsystem within the autonomous ship controller responsible for providing ships' officers with clear and concise information regarding the ship's watertight subdivision together with the integrity of related equipment, is pivotal in proactively averting catastrophic accidents [47]. In this capacity, the SIS can provide regular structural health reports and issue timely degradation alerts to SCC operators supervising autonomous vessels. The implementation of a SIS presents an effective approach to systematically address both prevention and mitigation measures, thereby diminishing risks and fostering a culture of continuous improvement.

3.3.4 Cargo Handling System (CHS)

The cargo handling system is an integral module within the autonomous ship controller. It is envisioned to task with overseeing essential cargo parameters such as temperature, and the cargo shifting by means of sensors, and adeptly manage the loading and unloading sequences to ensure smooth operations [30]. It may involve interface with the ship's communication system to replay cargo status and updates to the SCC as it provides visibility to shoreside operators. CHS operates seamlessly within the ASC, interacting with other subsystems like navigation, stability, and power management to ensure cargo operations align with overall ship control and decision-making.

3.4 AUTONOMOUS NAVIGATION SYSTEM (ANS)

An ANS refers to the integrated hardware and software responsible for operating a ship without constant human control or supervision. It utilises various sensors, processors, algorithms and actuation capabilities to sense the environment, analyse navigational complexities, plot collision-free routes, and manoeuvre the vessel accordingly. Major specialised components and functions include Navigational Situation Awareness, Collision Avoidance, Route and Speed Optimisation Planning, Weather Monitoring and Interpretation Systems, and interacting with other ships and shore-based entities per maritime regulations. A more detailed hierarchical architecture of an autonomous cargo ship may include additional systems such as Positioning, Navigation and

Timing System, Lights System and Dynamic Positioning System [48]. However, this study aims at a concise system structure and focuses mainly on the most relevant functionalities. AI has also been widely integrated as a core technology in ANS [7]. The system operates within a defined mission envelope and hands over control to human operators in shore control centres when encountering situations exceeding its capabilities. Through machine perception, planning, learning and control technologies, autonomous navigation aims to replicate and exceed human navigational abilities for unmanned maritime operations. Nevertheless, maintaining robustness, security and safety-critical reliability is a challenging task for the following respective sub-systems.

3.4.1 Navigation and Situational Awareness System (NSAS)

The NSAS is a specialised subsystem within the broader ANS responsible for localisation and comprehensive understanding of the operating environment. It integrates fusing data from navigational sensors such as RADARs, cameras, AIS receivers, GNSS (Global Navigation Satellite System) receivers and LiDARs to construct a robust internal representation of the contextual factors surrounding the autonomous vessel [30, 31, 49]. Through sensor fusion and analytics, it detects, identifies, tracks and predicts the behaviour of maritime entities and anomalies even in degraded visibility or adverse weather [50]. The NSAS facilitates real-time analysis of navigational intricacies, risks, and constraints [30]. It serves as a critical input to other planning and decision-making subsystems, including collision avoidance, route optimisation, and SCC. Advanced situation awareness capabilities are indispensable for ensuring safe autonomous operation without constant human oversight. Maintaining accurate and reliable situation awareness stands as a critical imperative for resilient autonomous maritime operations.

3.4.2 Route and Speed Optimisation and Planning System (RSOPS)

The RSOPS, as a sub-system, refers to the algorithms and software responsible for charting the optimal navigational path and speed profile for an autonomous vessel to safely, adaptively and efficiently reach its destination. It processes inputs like the voyage plan, real-time environmental data, maritime traffic density, and control actions from the controller to generate multi-dimensional trajectory optimisation objectives such as lowest fuel consumption, maximum operational efficiency and safety, and shortest arrival time [51]. The RSOPS continuously updates the active optimal trajectory based on new sensor data or operator inputs. The path planning module is tasked with calculating an unobstructed course by utilizing the provided data. This course is continuously revised at a regular interval with the most current obstacle information, prompting the motion planning module to revaluate the optimal path on each update [52]. In order to guarantee collision avoidance and adherence to COLREG regulations, the path planning algorithm anticipates the prospective movement of mobile obstacles [52]. Periodic re-planning ensures that obstacle data is refreshed to accommodate unforeseen alterations. It executes the trajectory in conjunction with other autonomous navigation subsystems, such as the collision avoidance system, to assess collision risks and securely guide the vessel [48]. Sophisticated optimisation solvers balance these complex trade-offs accounting for factors like wind, waves, ocean currents and collision avoidance constraints [50, 53]. As a key driver of autonomy, the RSOPS contributes to safe and efficient trajectories for the autonomous ship.

3.4.3 Collision Avoidance System (CAS)

The CAS is a critical subsystem in the ANS that is responsible for detecting obstacles and planning collision-free manoeuvres in dynamic maritime environments. CAS operates within the framework of predefined Closest Point of Approach (CPA) and Time to Closest Point of Approach (TCPA)

limits, adhering to the principles of COLREGs to determine the most appropriate avoidance strategy [30, 48]. CAS algorithm relies on processing data from navigational sensors, LiDAR and RADAR to identify and track surrounding vessels and objects, then predicts potential encounters [54]. In situations where potential collision risks arise, the CAS activates necessary measures, which may involve altering the vessel's course or adjusting its speed to proactively prevent accidents. It is also subject to human supervision from a SCC when it lacks a viable solution or operators within SCC disagree with the proposed solution [55].

3.4.4 Weather Monitoring and Interpretation System (WMIS)

Weather conditions have significantly impacted sea transportation and all maritime affairs, emphasizing the necessity of a WMIS in the context of crewless operation onboard [56]. Its fundamental mission is to monitor and interpret dynamic atmospheric and oceanographic conditions, ensuring the autonomous ship's responsiveness to ever-changing weather phenomena and its potential impact on ship operations. The WMIS aggregates real-time data from onboard sensors and equipment like anemometers and NAVTEX [48]. Weather analytics used to derive actionable insights such as detecting severe storms, are integrated with route planning, situational awareness, and collision avoidance functionalities to initiate appropriate navigational adaptations to avoid hazards or dangerous conditions. Continuously monitoring and interpreting environmental forces is critical for ensuring safe autonomous operation.

4: CYBER RISKS IN AUTONOMOUS SHIPBOARD OT SYSTEMS

Shipboard OT systems rely heavily on interconnected sensors, networks, and remote monitoring infrastructure. While this integrated systems-of-systems facilitate unmanned operations aboard autonomous ships, it significantly amplifies the vulnerability to cyber threats compared to conventional ships. The proliferation of cyber access points, coupled with low cyber hygiene and/or awareness, render essential OT systems susceptible to potential exploitation by malicious actors. The numerous entry points provide adversaries with avenues to infiltrate critical operational systems essential for ensuring safe navigation, thereby potentially causing threats to the ship and her crew. This section provides an in-depth exploration of the cyber threats associated with individual OT systems and their respective subsystems, as described in Section 3.

The list below includes different things like threat scenarios, threat vectors, vulnerabilities, and more. This mix is on purpose because the names of these attacks come from different places. Some are derived from the STRIDE framework, some are abbreviated from threat scenarios, and others are named based on how the attacks happen.

4.1 CYBER RISKS IN SHORE CONTROL CENTRE (SCC)

UNAUTHORISED ACCESS AND INTRUSIONS

It refers to both physical and software-based access, each representing distinct security risks. Intruders such as pirates, criminals, or hostile actors could potentially board ships and gain physical access to onboard system and hardware, causing damage - tampering with the system, or stealing physical assets from the perspective of industrial espionage [8]. The likelihood of unauthorised physical access also exists for the control room with close proximity to shore. Intruders may easily locate the control stations and attempt to gain physical access to shore control room facilities and workstations [57]. Unauthorised software-based access involves adversaries gaining entry to the SCC's digital systems without proper authorization. This could occur by exploiting vulnerabilities in software systems and communication network [57, 58]. Cybercriminals may use a combination of physical intrusion and software-based breach to further aid in launching sophisticated attacks. What's more, unauthorised physical access can enable an attacker to bypass or disable physical security measures that are intended to protect against software-based attacks. As an example, if intruders gain access to the ship and control station, they could disable alarm related mechanisms, making it simpler for them to cause further damage.

INSIDER THREATS

Insider threats are also manifested through both physical access and software-based access. Individuals with legitimate access badges may abuse their privileges to gain unauthorised access to sensitive areas. Insiders could misuse their software-based access to manipulate data, delete critical records or share confidential information with unauthorised entities. Regardless of entry to SCC through either physical access or software-based access, insiders with malicious intent could lead to data breaches, system manipulation and unauthorised actions that disrupt autonomous ship operations [59].

Tampering and Modification

SCC receives and analyses voyage data from Electronic Chart Display and Information System (ECDIS), RADAR, AIS and a series of sensors such as LiDAR and cameras [60]. There are a number of ways to tamper with sensors and equipment onboard. Hackers may tamper with the crucial navigation information. An example is to replace the live camera or microphone feed with a recorded video or audio clip to launch a replay attack [60]. The transmission of false information could cause faulty intelligence and mislead the operators into making erroneous decisions. The related data transmitted to the SCC must be protected against tampering and modification.

Network and Communication Vulnerabilities

Autonomous ships rely on robust network infrastructure for communication capabilities to enable C2 (Command and Control) links with SCCs [8]. Insufficient network segmentation creates avenues for exploitation as adversaries may manipulate infiltrated nodes and transmit unauthorised commands to autonomous ships or mount a DOS attack to disrupt communication links between the shore control centre and ships [8, 60]. This could disrupt control and monitoring capabilities, hindering the SCC's ability to manage and coordinate autonomous ship operations effectively. A resilient, hybrid communication architecture is essential to match the command, control, and telemetry requirements of autonomous maritime missions.

Supply Chain Attacks

Any of the hardware or software components proposed within the system architecture of autonomous ships can be infiltrated in advance by adversaries. The way to carry out supply chain attacks can include compromising software updates, tampering with system and hardware during manufacturing, or infiltrating third-party suppliers [8]. Most importantly, these can be stealthy and challenging to detect once operational. The attack towards SCC is not limited to specific software or infrastructure installed on its own as supply chain attacks occur throughout the entire lifecycle of both IT and OT hardware and software components. This can result in unauthorised access, data breaches, system malfunctions, and disruptions to critical operations. Taking an example of the compromised components on CAS, it may fail to detect a collision course and warn remote operators, while the humans were monitoring large fleets of vessels simultaneously. However, SCC would be sensitive and not immune to those effects as humans flounder about being back in the loop promptly [61]. It is the SCC that ultimately bears the brunt of these consequences and risks ending up in a fiasco. An attack targeting any component within the supply chain can potentially exert both direct and indirect consequences on the SCC as a result of heightened interconnectivity and deep integration.

Code Injection & Malware infection

SCC may be influenced by the lateral motion resulting from compromised components on the ship. Adversaries can introduce security vulnerabilities into SCC's system by relatively straightforward means like malware, ransomware, spyware, and viruses which can infiltrate critical systems. This infiltration can transpire through various means, such as the utilization of infected removable media like USB, the introduction of a compromised device or sensor, or through the distribution of malicious firmware updates [60]. For example, VDR has been found to be susceptible to flawed firmware updates [62]. Due to the evolution of autonomous ships, the risk of malware injection by human-machine interface or control station through USB ports is still extant, even though the possibility of physically injecting malware to the system or hardware

through crew on board is diminishing. The collision avoidance system and situational awareness system are also vulnerable to malware installation [6]. After successfully infiltrating a system with viruses, intruders can exploit the rapid propagation nature in a highly-connected network and swiftly infect other critical systems. Since SCC perceives its surroundings and formulates decisions based on the feedback from different systems, it potentially results in delays to vital navigation instructions and additional latent responses, thereby posing a significant safety risk to vessels, particularly in emergency situations. Other examples like ransomware, the operators at SCC have to undergo financial loss in exchange for restored access and control for OS of an autonomous ship.

Social Engineering

Social engineering based attacks can be used to compromise people if unaware and untrained [59]. Social engineering involves manipulating individuals or exploiting human vulnerabilities to trick SCC personnel into revealing sensitive information or credentials. The most frequently used scenario is phishing, in which attackers may send deceptive emails impersonating trusted sources or maritime authorities. These emails could contain malicious attachments or links, tricking SCC employees into revealing login credentials or downloading malware. Other scenarios include vishing, pretexting and tailgating. In summary, these tactics aim to deceive, persuade, or manipulate SCC personnel to divulge confidential information and compromise SCC's security measures.

4.2 CYBER RISKS IN COMMUNICATION SYSTEM

4.2.1 Satellite Communication System (SATCOM)

Data Modification and Corruption

It pertains to the manipulation of communication data or unauthorised modifications to the integrity of data being transmitted. If an autonomous ship's commands are corrupted or if false information is introduced, it could lead to incorrect actions being take [63]. Adversaries might tamper with data originating from various systems to influence the decision-making process or alter data/commands sent from the SCC to deceive autonomous systems. Further details will be expounded upon in their respective subsystem sections.

Jamming

RF waves enable bidirectional communication with satellites. Satellite communication serves as a means to establish a connection between the SCC and autonomous ships, especially over extended distances. Jamming is the act of transmitting RF signals within the same frequency band as the satellite signals and creating interference, in order to disrupt the genuine signals by the autonomous ship's communication systems. Jamming satellite signals becomes notably feasible when the transmitter is within the satellite's antenna coverage [8]. Other approaches to jamming can be realised by exploiting vulnerabilities in software [63]. Jamming occurrences severely disrupt the seamless flow of communication between the autonomous ship and SCC, leading to an impasse in critical data transmission and instructions. During critical situations, jamming can impede distress signals and risk effective responses.

Outdated VSAT Software Vulnerabilities

Vulnerabilities stemming from outdated Very Small Aperture Terminal (VSAT) software present a potential risk that adversaries can exploit. Updated satellite communication protocols or changes in network configurations may not be supported by outdated VSAT software due to incompatibility issues. Such vulnerabilities could be exploited for launching attacks like remote code execution, privilege escalation, or gaining control of the VSAT terminal [10]. Attackers may leverage these weaknesses to gain unauthorised access, execute malicious code, or exploit the system in diverse ways, thereby potentially compromising the confidentiality, integrity, and availability of the communication systems and the connected systems [10].

Eavesdropping

Data transmitted through RF signals may occasionally lack encryption or employ weak encryption methods, making it susceptible to decryption and retrieval of the unencrypted information [63]. Eavesdropping involves the unauthorised interception or monitoring of communication traffic through specialised equipment to capture and decipher transmitted data. Confidential operational details obtained through eavesdropping may enable adversaries to manipulate ship's operations and cause reputational harm to the organisation.

HIJACKING

Numerous cases exist where satellites have been hijacked and repurposed for different functions. This can involve modifying genuine signals or completely altering their intended use. An example of communication hijacking is broadcast signal intrusion. The hijacking can occur by overpowering the original signal at the same frequency or by directly breaching the transmitter and substituting the signal [63]. Hijacking can jeopardise the safety of the ship by allowing malicious actors to interfere with navigation, emergency response and safety protocols.

SPOOFING

Spoofing involves the transmission of fabricated signals or data that appears to be legitimate sources. In the context of autonomous ships, it encompasses creating false navigational data and misleading position information [63]. Spoofing can compromise the integrity and safety of ship operations by influencing decisions based on falsified data. One of the most famous example of satellite spoofing is GPS spoofing. Manipulated navigational information can result in severe navigational errors such as collisions, grounding, or unsafe routes.

DENIAL OF SERVICE (DOS) ATTACKS

The accessibility of satellite communication can also be interrupted using attackers, such as engaging in a network-based DoS attack [64]. A DoS attack involves flooding the communication channels with a massive volume of traffic, exhausting the available bandwidth and making the system unresponsive to legitimate communication attempts. The disruption may interfere with autonomous ship's ability to receive navigational data and updates on weather conditions.

4.2.2 Terrestrial Communications – VHF, Broadband, Internet

EAVESDROPPING

VHF radio communication utilises radio waves for communication and is limited to line-of-sight propagation. It is generally terrestrial and has a shorter range. However, it often lacks encryption, making conversations over VHF susceptible to eavesdropping [65]. Eavesdropping allows unauthorised individuals to listen on conversations, breaching the privacy of the ship operations and sharing information that should remain confidential.

JAMMING

In the case of VHF radio, attackers can intentionally overwhelm the legitimate VHF communication signals [66]. When a jamming signal is transmitted, it competes with the legitimate VHF communication signals, making it difficult for autonomous ships to send or receive messages effectively. A loss of availability of VHF communication may also hinder critical operations and impact the overall efficiency of autonomous ships.

DENIAL OF SERVICE (DOS) ATTACKS

Adversaries may inundate the ship's communication network that relies on VHF radio or cellular networks with an overwhelming number of requests. The flood of requests could exceed the network's capacity and overload the network's computational resources [10]. The attacker aims to disrupt cellular communication services crucial for the autonomous ship operations.

4.3 CYBER RISKS IN AUTONOMOUS SHIP CONTROLLER (ASC)

4.3.1 Autonomous Engine Monitoring and Control System (AEMCS)

DENIAL OF SERVICE (DOS) ATTACKS

AEMCS can be vulnerable to DoS attacks from various angles such as network vulnerabilities, protocol exhaustion and hardware limitations. Considering that the AEMCS is the primary control hub for the engines, vessel velocity, and speed generation, any downtime could lead to critical operational challenges [67]. During a DoS attack, attackers may render it unable to respond to legitimate commands, affecting engine control and monitoring capabilities.

UNAUTHORISED ACCESS AND INTRUSIONS

Insufficient authentication protocols or vulnerable access control mechanisms could grant unauthorised individuals access to the AEMCS. What sets AEMCS apart is the potential for significantly greater impact; unauthorised access could empower attackers to influence the vessel's trajectory [68]. These unauthorised users might tamper with engine controls, manipulate operational configurations, or disrupt vital monitoring processes.

OUTDATED SOFTWARE

The AEMCS is regarded as one of the less vulnerable systems in traditional maritime vessels, given its functional similarities to propulsion control systems [69]. Nonetheless, it is important to recognise that the software responsible for managing AEMCS may still exhibit susceptibility to certain vulnerabilities. These vulnerabilities can manifest in the form of outdated software components or unpatched security flaws [70]. In the event that such vulnerabilities exist, malicious actors could potentially capitalise on these weaknesses to compromise the integrity and security of the system, underscoring the importance of regular software maintenance and security updates to mitigate these risks effectively.

4.3.2 Anchoring and Mooring System (AMS)

MALWARE INFECTIONS

Programmable Logic Controller (PLC) is relevant to the AMS due to its role in controlling and automating various functions within these critical maritime operations [71]. Infiltration of malware into the PLC that oversee mooring machinery could result in unpredictable activation or deactivation of the equipment. Illicit entry into the PLC logic might permit the alteration of sequencing, posing a potential risk to the machinery or infrastructure. Unauthorised changes to PLC logic controlling anchoring procedure sequencing could damage equipment. PLCs assume a pivotal role in the AMS, and any cyber risks targeting PLCs may impact the functioning and security of AMS.

COMMUNICATION DISRUPTION

AMS often depends on communication networks for instructions and vital updates, such as mooring status. Potential attackers might focus on these communication channels, causing

disruptions in the transmission of instructions between the SCC and the ship. Consequently, this interference could result in a loss of control over the anchoring and mooring process [10].

SPOOFED SENSOR DATA

AMS may rely on sensor data such as water currents and depth measurements to assess the environmental conditions where anchoring and mooring will take place. Real-time measurements allow the system to dynamically adjust anchoring and mooring parameters and avoid hazardous situations. False tension sensor data could disguise dangerous mooring situations and compromise safety at berth [10].

4.3.3 Stability and Integrity System (SIS)

DATA TAMPERING

The system for stability and integrity monitoring oversees critical parameters such as metacentric height, hull stresses, and compartment flooding to uphold the seaworthiness of autonomous ships. Tampering with sensor data could generate deceptive readings, concealing evolving instability or leaks. An example could be tampering with weather data used by the SIS, the autonomous ships would be more likely to suffer from loss of stability in a heavy weather conditions [72]. As such, inaccurate stability assessments can cause the system to make incorrect adjustments, potentially destabilising the ship.

4.3.4 Cargo Handling System (CHS)

UNAUTHORISED ACCESS

Within the sphere of maritime infrastructure, the susceptibility of a vessel's cargo handling system to cyber threats emerges as a matter of significant concern, underscored by a notable incident that unfolded at the port of Antwerp in Belgium [73]. In this particular case, malevolent actors successfully breached the port's terminal OS, thereby enabling illicit activities associated with drug trafficking. The core objective of these cyber intruders was to orchestrate the redirection of shipping containers, effectively pilfering valuable cargo [74]. It is conceivable that these hackers could forge alliances with criminal organizations already entrenched within the realm of drug smuggling operations, thereby leveraging their unauthorised access to the computerised cargo tracking system for financial gains.

INSIDER THREATS

Theft of cargo can become a reality if a cyber attacker possesses insider information about the unloading procedures, allowing them to exploit vulnerabilities and perpetrate theft. In such cases, these activities may go undetected, particularly when dealing with high-value cargo such as weaponry. These compromises also present the unsettling possibility of enabling unchecked drug and human trafficking, ultimately fostering an environment in which illicit operations can thrive with minimal interference or oversight [68].

4.4 CYBER RISKS IN AUTONOMOUS NAVIGATION SYSTEM (ANS)

4.4.1 Navigation and Situational Awareness System (NSAS)

GNSS

The integration of the GNSS sensor in NSAS guarantees precise absolute positioning and time information. The design of maritime-oriented GNSS receivers enables their use in harsh weather conditions [49]. However, the principle of signal processing and transmission is the most exposed target to cyber-attacks. For example, GNSS Jamming is the intentional emission of signals across frequencies employed by GNSS with the aim of obstructing legitimate GNSS signal reception. This form of disruption demands minimal technical expertise, as it primarily involves overwhelming authentic signals with indiscriminate or disruptive noise [75]. On the other hand, GNSS Spoofing entails the transmission of fabricated, misleading GNSS satellite ephemeris and timing data. This deceptive information coerces the targeted receiver into computing erroneous positioning and, on occasion, inaccurate timing data, potentially leading to significant navigational discrepancies [75]. Advancing to the next level, GNSS has also demonstrated susceptibility to a range of security threats on unmanned vehicles, including DoS attacks, instances of malware injection, and unauthorised modifications of firmware [76]. It is still possible to apply these three categories to the GNSS of autonomous ships.

Remote Sensing Equipment

The operational environment of autonomous ships demands continuous and reliable sensor monitoring such as LiDAR, LADAR etc. Among these sensors, LiDAR plays a critical role by relying on reflection signals to provide spatial awareness. However, it is important to acknowledge that LiDAR sensors are susceptible to spoofing when exposed to objects with specific reflective or absorbent properties deliberately placed in their line of sight [77]. Furthermore, recent research has revealed vulnerabilities in LiDAR detectors related to 3D adversarial objects, further underscoring the need for robust security measures [78]. Similarly, the cameras utilised in these systems are not immune to interference and can be easily dazzled or spoofed [77, 79]. The compromise or manipulation of data from these devices introduces the potential for false readings, including the detection of non-existent obstacles or the omission of actual hazards, ultimately leading to misleading situational awareness. Such vulnerabilities emphasize the criticality of safeguarding sensor data integrity in autonomous maritime operations.

Denial-of-Service (DoS) Attacks

Situation awareness (SA) is susceptible to DoS attacks primarily due to its heavy reliance on real-time data collection, which is essential for safe navigation in any maritime environment. SA data, combined with navigation information from systems like AIS and GNSS, forms the foundation for making critical decisions to ensure vessel safety. This data is sourced from multiple sensors, especially when high-resolution sensors are deployed, resulting in substantial data volumes [44]. Consequently, processing this data may necessitate significant computational resources and the continuous flow of data to maintain real-time SA. However, the vulnerability arises from the fact that DoS attacks have the potential to disrupt this continuous flow of real-time data from the sensors. Such interruptions can have severe consequences, significantly impairing the ability to effectively monitor and assess the vessel's surroundings [49]. SA data plays a pivotal role in facilitating timely decision-making processes, including collision avoidance and route planning. A successful DoS attack can introduce delays into these critical decision-making procedures,

increasing the risk of maritime incidents. The susceptibility of SA to DoS attacks is a critical concern, as it undermines the real-time data flow necessary for safe navigation, decision-making, and collision avoidance.

AUTOMATIC IDENTIFICATION SYSTEM (AIS)

Within the realm of situational awareness, AIS serve as invaluable sources of supplementary data, facilitating communication between vessels, the exchange of positional information, and the avoidance of collisions with other ships and floating objects [80]. However, it is imperative to recognize that AIS stands among one of the most susceptible components within a ship's systems [81]. Multiple research efforts have consistently highlighted vulnerabilities associated with AIS, encompassing concerns such as spoofing, replay attacks, and frequency hopping attacks [69]. In any given scenario, there exists a potential risk for the vessel to encounter collisions with obstructions or to inadvertently run aground due to a compromised situational awareness.

4.4.2 Route and Speed Optimisation and Planning System (RSOPS)

ALGORITHM UNDERMINED

The methodology for the local route planning algorithm proposes a comprehensive approach, which incorporates an optimisation model for route decision-making, leverages an A-star heuristic method, and harnesses the capabilities of machine learning models, specifically those based on artificial neural networks (ANN) [53, 82]. This design prioritises efficiency, minimising both computational resources and runtime. However, it is imperative to acknowledge that recent research has revealed vulnerabilities in neural network-based systems, exposing them to potential security breaches. Notably, attacks such as brute forcing, buffer overflow, and malware injection have been identified as sources of insecurity within these systems [83]. One illustrative concern arises from training processes employed by developers, which, if flawed, can introduce vulnerabilities into the algorithms [83]. These vulnerabilities may be exploited by adversaries to compromise the integrity of the AI model and manipulate the optimisation logic. The ramifications of such compromises are far-reaching; once the integrity of the machine-learning-based planning system is compromised, the carefully charted path may be subject to manipulation. In such scenarios, adversaries could divert the vessel toward hazardous areas, undermining the system's ability to ensure collision-free navigation—a critical aspect of maritime safety.

FALSE FEEDBACK

In the context of an autonomous ship, the prerequisites for crafting an optimal route encompass the imperative of anti-collision responsibilities [51]. In this intricate ecosystem, the inputs emanating from collision avoidance systems assume a crucial role in the determination of the meticulously planned route. It is crucial to emphasize that within this multifaceted network, individual systems do not operate in isolation; rather, they operate in concert, each contributing data that reverberates across the entire framework. It is within this interconnected web of systems that adversaries may seek to exploit vulnerabilities. The RSOPS relies on sensitive data, such as weather forecasts, navigational information, real-time situational data and so on. One potential avenue for attack lies in tampering with the collision avoidance system, wherein adversaries could intercept and manipulate this data, introducing false information regarding the presence or location of obstacles. Such an indirect but subversive act could profoundly impact the route planning process, potentially steering it toward unsafe or inefficient trajectories. Furthermore, by disseminating inaccurate or misleading data to the RSOS, adversaries may deceive the control

centre into approving and subsequently endorsing routes that are fraught with risks and inefficiencies.

Denial-of-service (DoS) Attacks

While in-depth research on Denial-of-Service (DoS) attacks directly targeting the RSOS is limited, it's crucial to acknowledge the potential threat posed by such attacks. The inherent interconnectedness of autonomous ship systems, coupled with the critical role of route planning in ensuring safe operations, creates numerous avenues for Denial-of-Service (DoS) impacts. The RSOS heavily depends on connectivity to receive critical data inputs, including weather and situational awareness information. Attackers have the capability to disrupt this system through various means, including jamming, spoofing, and DoS attacks, all of which are known methods for targeting sensor data [7]. These attacks can effectively prevent the system from receiving essential updates required for planning algorithms. By flooding the sensor instead, the adversary could still render the system unresponsive.

Communication Interception

The optimised route and speed profiles are typically disseminated from the route planning system to various ship automation and control systems. Within this interconnected network, a potential vulnerability arises—adversaries may seek to intercept or eavesdrop on the communication channels linking the RSOS with these subsystems. Such unauthorised access can grant them insights into the sensitive information exchanged during the route optimisation process, consequently revealing potential weaknesses that could be exploited elsewhere within the system. Furthermore, it is noteworthy that data from various ship systems is aggregated and fused, with the consolidated information transmitted to remote operators for review [44]. The seamless connectivity between the ship and shore plays a pivotal role in facilitating human inputs and remote operations. However, in the event of an interception or eavesdropping on this communication stream, malicious actors could introduce false data into the RSOS, leading to unintended and potentially detrimental trajectories.

4.4.3 Collision Avoidance System (CAS)

False Data Injection

Collision avoidance systems often rely on sophisticated algorithms to detect potential collisions and make decisions on how to avoid them. These algorithms are designed to analyse data from various sources, such as sensors, RADAR, LiDAR camera and other relevant inputs to assess the risk of a collision and determine appropriate avoidance actions [48, 52]. Attackers can inject false data into a state-of-the-art collision avoidance algorithm, providing fictitious targets as input to force the ship to follow a predetermined and malicious track [52]. This misinformation could mislead the algorithm and lead to incorrect collision risk assessments and avoidance actions.

Sensor Manipulation

Collision avoidance systems work collaboratively with situational awareness and weather data to assess potential risks and implement appropriate actions to maintain a safe course and distance from other vessels and obstacles [55]. RADAR, AIS, LiDAR, cameras and environmental related sensors are fundamental data sources for collision avoidance to determine the presence of other vessels, allow vessels to exchange identification and speed information, detect obstacles and measure distances for them and obtain visual information as well as weather conditions [6, 49].

These sensors work together to provide comprehensive data on the ship's surroundings, enabling the collision avoidance system to assess risks accurately and take appropriate actions to prevent collisions and ensure safe navigation. If any of these critical systems or sensors are attacked or compromised, the effectiveness of the collision avoidance system can be severely impacted as it can create an environment of uncertainty.

DENIAL OF SERVICE (DOS) ATTACKS

Collision avoidance systems in autonomous ships rely on continuous real-time updates and data from various sensors and systems. It processes a vast amount of data to make accurate decisions [7]. A DoS attack can flood the system with spurious or meaningless data, overwhelming the processing capabilities and rendering the system unable to process genuine sensor inputs effectively. The sensor related attacks such as jamming has been repeatedly talked about in the previous sections. Adversaries may also exploit vulnerabilities in the network infrastructure supporting the collision avoidance system, disrupting the data transmission and making it difficult for the system to receive or send alerts.

COMMUNICATION INTERCEPTION

Upon identifying the other vessel as a potential collision candidate, the operator at SCC monitors the ship status and evaluates the need to initiate collision avoidance measures. It may entail establishing communication with external entities, such as the SCC or other vessels, to ascertain the vessel's intentions. Wireless communication used in collision avoidance system, such as AIS and VHF radios, is particularly vulnerable to interception [84]. These systems usually lack strong encryption or authentication mechanisms, making it easier for attackers to intercept and manipulate communication [84]. Intercepted communication can be altered or manipulated to provide false or misleading data to the collision avoidance system. For instance, false information about a ship's speed or direction could lead to incorrect collision risk assessments, potentially causing unsafe situations.

4.4.4 Weather Monitoring and Interpretation System (WMIS)

SENSOR JAMMING AND SPOOFING

The system heavily relies on a variety of sensors, including anemometers, barometers, temperature sensors, to collect real-time data about weather conditions [85]. Jamming or spoofing these sensors can result in the system receiving incorrect or manipulated data, leading to inaccurate weather assessments and forecasts. Moreover, the weather monitoring and interpretation system plays a critical role in the ship's decision making process, especially during adverse weather conditions. Sensor jamming or spoofing can compromise the accuracy and reliability of the weather data being collected. Inaccurate data can affect the system's ability to accurately interpret weather patterns, predict storm trajectories, and provide timely warnings to the crew, potentially leading to unsafe navigation.

DENIAL OF SERVICE (DOS) ATTACKS

The weather monitoring and interpretation system also requires real-time data from various sources like satellites, weather stations and sensors. A DoS attack can flood the system with a volume of traffic and the disruption of data flow to the weather monitoring system through a DoS attack can delay or distort critical weather information, potentially leading to erroneous decisions

and jeopardising the safety of the vessel [10]. Besides, the autonomous ship heavily relies on weather forecasts for route planning, speed adjustments and other operational decisions. A DoS attack on the weather monitoring system can prevent the timely receipt of weather updates, increasing the risk of navigating through dangerous weather without appropriate precautions.

Algorithm Undermined

Several machine learning models have already been utilised for predicting various weather parameters [86]. Adversarial examples can be fed into the algorithm to manipulate weather predictions in dangerous ways that are difficult to detect. For example, data poisoning attacks during the training process could introduce subtle biases into the model that distort forecasting. Besides, the biased learning can cause the model to generate biased weather predictions. Inaccurate or manipulated weather forecasts due to algorithm undermining can lead to financial loss and potentially life-threatening situations.

5: MITIGATION STRATEGIES

The OT systems discussed in the previous section are the bedrock of autonomy, enabling functions such as collision avoidance, navigation, propulsion, and environmental monitoring. Cyber-attacks on these systems can result in loss of propulsion, navigation malfunctions, or even loss of life. This heightened vulnerability is due to the inherent lack of intrinsic security capabilities within these systems. The severity of potential consequences underscores the crucial need for robust and comprehensive cybersecurity measures specifically tailored for autonomous ships. These measures encompass a spectrum of strategies and across organisational levels, from network segmentation, vigilant monitoring, stringent access controls, and robust encryption to risk-informed policies and crew training. It is essential to emphasise the integration of cybersecurity measures at every layer of the OT infrastructure and associated workflows. Without such concerted efforts, autonomous ships remain at significant risk of intrusions and manipulations.

Some mitigation measured are written down after the consideration of IACS Unified Requirements E26 and E27 on Cyber Resilience. These documents specifically address the utilization of computer-based systems that handle control, alarm, monitoring, safety, or internal communication functions subject to classification society requirements. It's crucial to understand that this publication is not designed to establish a foundation for, nor should it be construed as advocating external auditing or vetting of individual companies' and ships' approaches to cyber risk management.

5.1 MITIGATION MEASURES FOR SHORE CONTROL CENTRE (SCC)

Table 3 Mitigation Measures for Shore Control Centre

SHORE CONTROL CENTRE	
Cyber Risks	**Mitigation Strategies**
Unauthorised Access and Intrusions	- Alarm systems that transmit security alarms to the SCC should be designed and installed when intrusions into the vessel are detected [8]. - Tamper-resistant mechanisms should be implemented for critical data that should not be exposed to any external parties [8]. Any physical security measures designed to enhance a vessel's resilience against physical attacks should be taken into account. This includes ensuring that access doors to the vessel's interior are securely locked. - The SCC should have perimeter controls for the building and physical access control measures implemented [8]. The camera for intruder detections should also be deployed [57]. - Multi-factor authentication mechanisms such as identity cards together with biometrics are advised to be implemented to avoid unauthorised physical access to the shore control centre.

	- Multi-factor authentication for getting access to the system should be taken into account if the physical barrier fails. The commands sent from SCC in certain conditions shall be authenticated before being performed by the vessel.
Insider Threats	- Conduct regular training programs and workshops to educate SCC personnel about the risks associated with insider threats and how to recognise and report suspicious activities [58]. - Encourage a culture of security awareness, where employees are vigilant and proactive in identifying potential threats. - Conduct thorough background checks on all employees with access to sensitive systems, including criminal history, employment history, and credit checks where applicable. - Employ behavioural analytics and anomaly detection tools such as CCTV to monitor and identify unusual or suspicious activities among SCC staff.
Data Tampering and Modification	- Robust cryptographic mechanisms must be implemented to ensure authentication, confidentiality, integrity, and non-repudiation [8]. Additionally, the system should support encryption algorithms that effectively safeguard data confidentiality and integrity, while also meeting the data transmission time requirements essential for uninterrupted voyages [87]. - Redundancy in communication links used to receive and transmit information is a common place. It can be employed to independently cross check received data, ensuring the integrity of each channel and confirming that none of them has been compromised [88]. However, such pre-installed shared secrets between communicating parties must be securely installed and maintained to prevent any unauthorised usage. - The physical integrity of the onboard or SCC sensors must be protected in a way that sensitive data transmitted back to SCC is encrypted and validated [87].
Network & Communication Vulnerabilities	- Implementing a robust network segmentation strategy is crucial for isolating systems and data from less secure areas, thereby minimising the potential impact of a network breach [10, 33]. - The deployment of the SIEM (Security Information and Event Management) capability such as log management, real-time monitoring and alerting when it identifies network penetration would collectively enhance the security standard of the network infrastructure for autonomous vessels [10].

Supply Chain Attacks	- The supply chain encompassing all hardware and software components employed in autonomous ships demands safeguarding against both deliberate and inadvertent alterations that might occur over its lifecycle [8]. The ship owner should stimulate that suppliers, vendors and service providers meet specific security standards through a third-party certification [89]. - The products have a risk of being modified during the manufacturer's development environment and it is necessary for the vessel's owner to check the hash values and seals for the physical protection of the product prior to installation [8]. - Regularly monitor and update software and hardware components sourced from reputable sources to mitigate the risk of compromised components [10].
Code Injection & Malware infection	- Consistently update and apply patches to the software and systems within the SCC to mitigate known vulnerabilities [57]. - The USB ports may be inevitably present at SCC and thus automated scanning for devices connected to USB ports will be helpful in detecting malware infection [90]. - Install antivirus or anti-malware software at SCC's OS to detect and get alerted for known threats [91].
Social Engineering	- Conduct security awareness training for SCC operators to help them recognise and report phishing attempts and social engineering tactics [59]. Regular refresher training sessions are needed to keep employees informed about evolving social engineering tactics. - Phishing simulation exercises among SCC operators could be conducted to test their ability to identify phishing emails. Advanced email filtering solutions could be set to block phishing emails. - Multi Factor authentication schemes can be used to verify the authentic identity of the user when logging into the system and prevent further damage even though the credential of a SCC operator such as passwords has been disclosed.

5.2 MITIGATION MEASURES FOR COMMUNICATION SYSTEM

Table 4 Mitigation Measures for Communication System

Communication System: Satcom	
Cyber Risks	**Mitigation Strategies**
Data Modification and Corruption	- Manage the initial compilation of data and recognise when such changes have occurred and respond appropriately [33]. For example, deploying an Intrusion Detection System (IDS) to monitor the SATCOM network for suspicious activities or unauthorised attempts to modify or corrupt data. Promptly respond to detected threats. - Implement strong encryption protocols to secure data transmitted over SATCOM [8]. Employ robust authentication mechanisms to ensure that only authorised users can access and modify the data.
Jamming	- Utilise frequency diversity by operating on multiple frequency bands [30]. If one frequency is jammed, the communication can continue on an alternative frequency. - Employ anti-jamming technologies and make it difficult for jammers to disrupt communication effectively. - Use advanced signal filtering techniques and interference rejection technologies to minimize the impact of jamming signals and maintain clear communication.
Outdated VSAT Software	- Institute a structured patch management procedure to ensure timely updates and application of security patches for the VSAT software, enhancing its resilience against emerging threats [10]. - Conduct comprehensive vulnerability assessments and rigorous penetration testing to pinpoint vulnerabilities within the VSAT system and implement appropriate measures to rectify them effectively [10]. - Deploy advanced network intrusion detection and prevention systems to promptly identify and mitigate attacks aimed at exploiting vulnerabilities in outdated software, fortifying the overall security of the VSAT system [10].
Eavesdropping	- Utilise strong end-to-end encryption algorithms to protect the confidentiality of data over SATCOM. Considerations should be given to data confidentiality vulnerabilities while data in transit and data at rest [33]. - Data authentication mechanisms should ensure only authorised users have access to the communication system. Data authentication solutions should encompass secure transmission protocols, advanced identification techniques,

	and validation methods to ascertain the credibility of data sources [33].
Hijacking	- Segment the SATCOM network to isolate critical components and devices, reducing the potential attack surface and limiting the impact of a hijacking attempt [33]. - Promptly apply security patches and updates to address any known vulnerabilities that could be exploited by hijackers to gain control over the SATCOM system.
Spoofing	- Multi-layered authentication should be enabled. For example, digital signature schemes or blockchain-based identity management to verify the legitimacy of any commands sent over SATCOM links. - Build validity checks into autonomation systems to flag received SATCOM data that seem logically or physically inconsistent. - Encryption should be considered again to prevent the injection of spoofed data [8].
Denial of Service (DoS) Attacks	- Utilise measures like rate limiting, traffic filtering, and anomaly detection to protect the system against DoS attacks. - Introduce redundancy and failover mechanisms for communication links to alleviate the disruptive effects of potential DoS attacks [30]. - Vigilantly monitor network traffic and system performance to promptly identify and counteract DoS attacks in real-time.

Communication system: Terrestrial	
Cyber Risks	**Mitigation Strategies**
Eavesdropping	- Use encrypted communication protocols like SSL/TLS etc to protect against eavesdropping of sensitive data. - Authenticate connections between the ship and shore to ensure communication is only occurring with trusted parties. This prevents Man-in-the-Middle attacks [33].
Jamming	- Limit broadcast range of wireless terrestrial communication to only what is necessary, minimising potential points of interference. - An incident response plan specially for dealing with jamming incidents should be developed to outline actions to be taken and minimize impacts.
Denial of Service (DoS) Attacks	- Employ load balancing techniques to efficiently distribute traffic across the network, mitigating the potential impact of

	DoS attacks [10]. Customise configurations on network devices to restrict the rate of incoming traffic, thus preventing resource depletion caused by malicious attacks [10]. - Establish backup communication channels or redundant systems to sustain crucial operations seamlessly in the face of DoS attacks [30].

5.3 MITIGATION MEASURES FOR AUTONOMOUS SHIP CONTROLLER (ASC)

Table 5 Mitigation Measures for Autonomous Ship Controller

Autonomous Ship Controller: Autonomous Engine Monitoring and Control System	
Cyber Risks	**Mitigation Strategies**
Denial of Service (DoS) Attacks	- Equipment related to the AEMCS is to be considered redundant and rapid restarts so that failures are minimized if an attack gets through defences [25]. Or the engine system control network architecture can be designed in a distributed manner to avoid a single point of failure. - Consider using specialised DoS mitigation services offered by security providers. These services can filter incoming traffic and mitigate DoS attacks by diverting traffic to a scrubbing centre before it reaches the ship's network.
Insufficient Authentication and Authorisation	- Confidentiality, Integrity and Availability (CIA) triad is to be ensured for data transmission and reception [25]. The principle of least privilege can be enforced. Establish role-based access controls, allowing only certain actions based on the assigned role of the authenticated user.
Outdated Software	- Implement a strict patch management process to regularly update and apply security patches to the motion control software [10]. - Stay informed about the latest updates and security patches provided by the software vendors and promptly apply them to address known vulnerabilities. - Conduct regular vulnerability assessments and penetration testing specific to the system software to identify and address vulnerabilities frequently [10].

Autonomous Ship Controller: Anchoring and Mooring System	
Cyber Risks	**Mitigation Strategies**
Malware Infections	- Install and regularly update reputable antivirus and antimalware software on all systems within the anchoring and mooring infrastructure to detect and eliminate malicious software [57]. - Keep all software, including the OS and applications used in the anchoring and mooring system, up to date with the latest security patches and updates to address known vulnerabilities [57].
Communication Disruption	- Implement redundancy in communication systems by having backup equipment and diverse communication paths to ensure that if one path is disrupted, communication can be seamlessly switched to an alternative path [61].

	- Communication must have suitable bandwidth for operations to ensure safety [33]. Implement data compression and optimisation techniques to reduce the amount of data transmitted, which can help maintain communication during periods of limited bandwidth.
Spoofed Sensor Data	- Implement cryptographic techniques such as digital signatures to authenticate and validate commands and messages exchanged between the ship's systems and external entities [8, 87]. Only accept and execute commands with valid authentication [87]. - Utilise secure communication protocols that provide encryption and data integrity assurance. Secure protocols prevent unauthorised parties from intercepting or altering the communication and commands [87]. - Ensure synchronized and accurate time across systems involved in anchoring and mooring. Use timestamps to validate the timelines and authenticity of commands, rejecting those outside acceptable time ranges. - Utilise trusted and tamper-resistant hardware and firmware components within the system to prevent physical tampering or unauthorised access that lead to spoofing.

Autonomous Ship Controller: Stability and Integrity System	
Cyber Risks	**Mitigation Strategies**
Data Tampering	- Implement redundant and diverse sensors to monitor critical parameters related to stability and integrity. Cross-verify data from multiple sensors to detect any inconsistencies or anomalies [57, 88]. - Use secure communication protocols and encryption to transmit sensor data. Ensure that the transmitted data is not intercepted, altered, or replaced by malicious entities. - Regularly calibrate and validate sensors to ensure accuracy and reliability of the data provided [57].

Autonomous Ship Controller: Cargo Handling System	
Cyber Risks	**Mitigation Strategies**
Unauthorised Access	- Implement strong and multifactor authentication mechanism to ensure that only authorised personnel can access the cargo management system [87]. - Implement Intrusion detection system to monitor the cargo management system for suspicious activities and potential unauthorised access [57]. - Enforce Timeout and Lockout policies to enforce access timeout mechanisms after a certain number of failed login

	attempts to prevent brute force attacks and unauthorised access.
Insider threats	- Implement strict access controls and adhere to the principle of least privilege [8]. Grant employees access only to the systems and data essential for their specific job roles. - Monitor log activities within the cargo management system to ensure consistent audit trails that can be reviewed to detect any suspicious activities.

5.4 MITIGATION MEASURES FOR AUTONOMOUS NAVIGATION SYSTEM (ANS)

Table 6 Mitigation Measures for Autonomous Navigation System

Autonomous Navigation System: Navigation and Situational Awareness	
Cyber Risks	**Mitigation Strategies**
GNSS	- Implement real-time monitoring of signal quality and integrity [10]. The system should be capable of detecting anomalies or disruptions in the GNSS signals and switch to alternative navigation methods if needed. - Integrate advanced signal processing techniques and algorithms to detect and mitigate jamming and spoofing attempts. Implement mechanisms that can identify unusual signal patterns and take appropriate action [60]. - Utilise secure timing sources and authentication mechanisms to verify the authenticity and accuracy of the GNSS signals. Implement cryptographic techniques to ensure that the received signals are from genuine satellites [92]. - Employ anti-jamming antennas that are designed to reject signals coming from directions other than the satellite constellation's expected path. These antennas can help in mitigating the impact of intentional interference.
Remote Sensing Equipment	- LiDAR and LADAR Systems: - Employ redundant LiDAR or LADAR sensors in critical areas of the ship to ensure continuous data collection even if one sensor fails or encounters interference [57]. - Monitor for any interference that may affect LiDAR performance and have mechanisms in place to switch frequencies or adjust parameters to avoid or mitigate interference. - Camera Systems: - Encrypt camera data during transmission and utilize secure communication protocols to prevent eavesdropping and unauthorised access to the video feed [8]. - Ensure cameras are tamper-proof and securely mounted to prevent physical tampering or vandalism that could compromise their functionality or view. - Apply privacy filters or masking techniques to the captured video feed to protect sensitive information or areas from being exposed, complying with privacy regulations. - RADAR Systems: - Use RADAR systems with frequency agility to switch frequencies in response to detected interference, ensuring continuous operation and accurate object detection. - Integrate redundant RADAR systems and a failover mechanism to switch to an alternative RADAR in case of system failure or disruption [57, 92].

Automatic Identification System (AIS)	- Implement strong encryption for AIS data during transmission to prevent eavesdropping and unauthorised access. Utilise authentication mechanisms to verify the authenticity of received AIS messages [92]. - Ensure that AIS equipment is configured securely with appropriate access controls. Limit access to authorised personnel and regularly update access credentials [92]. - Employ anomaly detection mechanisms to monitor AIS transmissions for unusual patterns or unexpected behaviour that could indicate malicious activity.
Denial of Service (DoS) Attacks	- Implement network traffic monitoring and filtering mechanisms to detect abnormal traffic patterns and filter out potentially malicious traffic associated with DoS attacks. - Implement redundant systems and failover mechanisms to ensure critical navigation and situational awareness functions remain operational even if one system is under a DoS attack [30]. - Configure network devices to limit the rate of incoming traffic, preventing overwhelming of systems and maintaining steady performance during an attack. - Utilise specialised DDoS protection services offered by service providers to filter and block malicious traffic before it reaches the navigation and situational awareness system. - Implement strong access controls and authentication [92] mechanisms to ensure that only authorised personnel have access to critical navigation and situational awareness systems [87].
Communication Interception	- Implement strong encryption algorithms and protocols to encrypt all communications between the ship and external entities, ensuring that intercepted data remains unreadable and secure [25]. - Establish secure communication channels such as VPNs to ensure that data transmitted over public networks remains protected and free from interception [60]. - Implement intrusion detection systems to monitor network traffic and detect any unusual activities that may indicate communication interception attempts [60]. - Enforce strict access control policies and authorisation mechanisms to ensure that only authorised individuals can access and modify the communication system [57]. - Deploy firewalls and segment the network to control and monitor traffic, preventing unauthorised access to critical communication components [87]. - Utilise secure and industry-recognised communication protocols that provide built-in security features to protect against interception [87].

Autonomous Navigation System: Route and Speed Optimisation and Planning System	
Cyber Risks	**Mitigation Strategies**
Algorithm Undermined	- Employ strong encryption and access controls to protect the integrity of algorithms. Utilise algorithms that are resistant to tampering and have built-in integrity checks [87]. - Conduct periodic audits and reviews of algorithms to identify any potential vulnerabilities or tampering attempts.
False Feedback	- Implement robust data validation techniques to ensure that the feedback received is legitimate and consistent with expected parameters. - Use a combination of sensors and data sources to cross-verify feedback and detect inconsistencies or anomalies [57].
Denial of Service (DoS) Attacks	- Employ network traffic monitoring and filtering to detect and mitigate DoS attacks in real-time [92]. - Use load balancing techniques and maintain redundant systems to distribute traffic and minimise the impact of DoS attacks [10].
Communication Interception	- Use strong encryption protocols and end-to-end encryption to protect communications from interception and eavesdropping [30]. - Implement secure key management practices to protect encryption keys and ensure they are not intercepted or misused. - Employ secure and industry-recognized communication protocols that provide built-in security features to prevent interception [87].

Autonomous Navigation System: Collision Avoidance System	
Cyber Risks	**Mitigation Strategies**
False data injection	- Incorporate redundant sensors to cross-verify data and detect discrepancies caused by false data injection or sensor manipulation [57]. - Utilise advanced data fusion algorithms to combine data from multiple sensors and identify inconsistencies.
Sensor manipulation	- Implement continuous integrity checks on sensor data to detect alterations or anomalies [57]. - Utilise cryptographic techniques to sign and verify data authenticity.
Communication Interception	- Implement strong encryption and authentication protocols to secure communication channels, making it difficult for adversaries to intercept data [8]. - Employ secure key management practices to protect encryption keys from unauthorised access. - Segment the network into zones with strict access controls, limiting the ability of attackers to move laterally and intercept communication [25].

	- Employ firewalls and intrusion detection systems to monitor and control network traffic [60].
Denial of Service (DoS) Attacks	- Deploy traffic monitoring and anomaly detection systems to identify sudden increases in network traffic or unusual patterns indicative of a DoS attack [60]. - Configure automated responses to mitigate the impact of such attacks. - Design the system with redundancy and failover mechanisms to ensure continuous operation despite DoS attempts [30].

Autonomous Navigation System: Weather Interpretation and Monitoring System	
Cyber Risks	**Mitigation Strategies**
Sensor Jamming and Spoofing	- Utilise redundant and diverse sensors for weather data collection to minimise the impact of sensor jamming or spoofing on the accuracy of the data [57]. - Incorporate cryptographic techniques to authenticate and validate sensor signals, ensuring the data received is from genuine and unaltered sources [57]. - Implement secure communication protocols to prevent interception and tampering of signals [87].
Denial of Service (DoS) Attacks	- Design the weather interpretation system with network resilience, allowing it to continue functioning even during a DoS attack by utilising backup communication channels and redundancy [25]. - Employ traffic monitoring and filtering mechanisms to detect and mitigate DoS attacks in real-time [60].
Algorithm Undermined	- Implement integrity checks within the algorithm to detect any unauthorised modifications or alterations to the code. - Utilise anomaly detection mechanisms to identify unexpected behaviour in the algorithm that may indicate tampering [60]. - Follow secure development practices, including regular code reviews, to ensure the robustness and integrity of the algorithm throughout its life cycle.

6: CYBER RISK ASSESSMENT

Having presented a list of attack vectors for the OT sub-systems, it is now imperative to scrutinise and classify these vectors to a cyber risk assessment. This section is dedicated to highlight the cyber risk assessment framework adopted for the identification and calculations of cyber risks associated with fundamental systems of an autonomous ship.

6.1 CYBER RISK ASSESSMENT FRAMEWORK

There are many risk assessment frameworks used in the industry. Some of the popular and commonly used ones are risk-matrix based approach, Fault Tree Analysis (FTA), Process Hazard Analysis (PHA), Hazard Identification (HAZID), Hazard Analysis and Critical Control Points (HACCP), Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects, and Criticality Analysis (FMECA). Most of these frameworks require expert opinions and feedback and therefore may contain some inherent biases. Improved and relatively less dependent on expert feedback and involvements are FMECA-ATT&CK framework [11, 93] and FMECA-ATT&CK-ATLAS framework [94]. For the identification and calculations of risks associated with OT sub-systems of an autonomous ship, we opted for FMECA-ATT&CK-ATLAS framework due to its simplicity and broad coverage of cyber threats not just for OT and IT systems but also for AI/ML systems. The main steps of FMECA-ATT&CK-ATLAS framework are depicted in Figure 4.

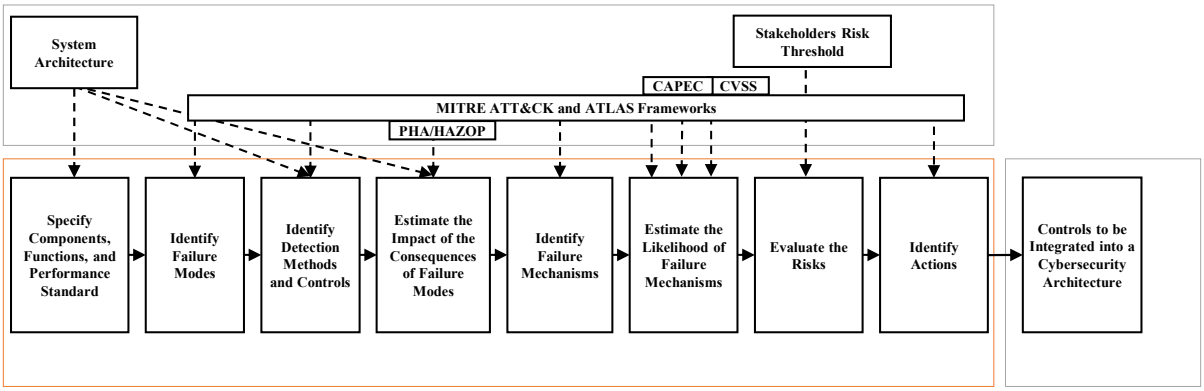

Figure 4 Overview of Proposed FMECA-based Approach Showing the Integrated Information Sources [11]

FMECA-ATT&CK-ATLAS (or "FAA" in short) works in top-down fashion. It keeps decomposing a big system into subsystems until fundamental building blocks are reached. At the granular level, it calculates the risk associated with each fundamental building block and then sum up all the risks associated with all the subsystem, for a system which is hierarchically at higher level of structure. Likelihood, impact and detectability of an attack are included in the risk equation and all the failure modes and mechanisms are deduced from MITRE ATT&CK and MITRE ATLAS tactics and techniques. MITRE ATT&CK is used for all the IT and OT related cyber-attacks whereas MITRE ATLAS is used for AI/ML related cyber-attacks.

Shore Control Centre is beyond the scope of this study's risk analysis. However, SCC plays a pivotal role in managing and controlling the operations of autonomous ships and they are central hubs for data management and communication. Such centralisation makes it attractive targets for cyberthreats seeking to exploit. Given these factors, this study assumes SCC to be categorised as high risk in the context of cybersecurity assessment for autonomous ship systems. The rest of the

systems represent the major functional divisions of a typical autonomous ship, each responsible for a specific aspect of its operation. But the complexity doesn't stop there. Each of these systems is further subdivided into subsystems, each with its unique purpose and responsibilities. For instance, the Autonomous Ship Controller consists of four distinct subsystems: Stability and Integrity System, Cargo Handling System, Anchoring and Mooring System, and Autonomous Engine Monitoring and Control System. These subsystems can further be subdivided into sub-subsystems. The Anchoring and Mooring System can have an AI Server, PLCs and a network switch. So, the risks are calculated for these sub-subsystems, which are at the lowest level in the hierarchical structure and summed up to get the risk value associated with Anchoring and Mooring System.

After applying the FAA framework to the entire autonomous ship, we obtained more than 5,000 risk values for autonomous ship systems. We classified the risks as 'Low', 'Medium' and 'High' and counted the number of risks against each component (subsystem) of the ship. A glimpse of our risk analysis is tabulated in Table 7. Using the FAA framework, we found that the Navigation Situation Awareness System and Ballast Water Management System exhibit the highest levels of risk exposure compared to the other systems. Evidently, some systems (e.g., Cranes) have a minor number of low, medium and high risks compared to critical systems (e.g., RADAR) have large number of low risk but they have not medium and high risks associated with them. Therefore, components with medium and high-risk ratings are categorised as high-risk. Additionally, we have established a threshold of 600 as the point at which a high number of low-risk components are also classified as high risk. In this particular situation, RADAR and the dynamic positioning controller are exceptions and are placed in the high-risk category.

Table 7 Classifying System into Different Risk Levels

Components	Number of Risks		
	Low	Medium	High
Navigation Situation Awareness System	427	32	2
Ballast Water Management System	33	10	1
Cranes	13	3	0
Autonomous Engine Monitoring and Control System – AI Server	460	1	0
Autonomous Engine Monitoring and Control System – PLCs	52	1	0
Engine	15	1	0
RADAR	604	0	0
Dynamic Positioning Controller	601	0	0
Cargo Handling System – AI Server	461	0	0
Stability and Integrity System – AI Server	460	0	0
Anchoring and Mooring System – AI Server	456	0	0
Route and Speed Optimisation Planning System	454	0	0
Automatic Identification System	414	0	0
Main Data Historian	388	0	0
Satellite Router	123	0	0
VHF	123	0	0
Broadband Router	103	0	0
Stability and Integrity System – Network Switch	83	0	0
Cargo Handling System – Network Switch	83	0	0

Anchoring and Mooring System – Network Switch	83	0	0
Autonomous Engine Monitoring and Control System – Network Switch	83	0	0
Perception System – Network Switch	83	0	0
Cargo Handling System – PLCs	53	0	0
Anchoring and Mooring System – PLCs	53	0	0
GNSS	27	0	0
Thrusters	16	0	0
PTZ Cameras	11	0	0
LiDAR	7	0	0
Sensor Fusion	7	0	0
Others	≤7	0	0

6.2 RISK EVALUATION

To better manage complex systems such as interconnected components, a structured approach is crucial. Hierarchical management offers a clear and systematic framework for dealing with such intricacies. At its core, hierarchical management involves breaking down a complex system into a series of manageable subsystems and organising them in a hierarchical structure. Figure 5 gives an overview of the OT systems of an autonomous ship that are considered in this study, and each is given a "tier colour", where red is associated with Tier T1 (highest urgency), yellow (Tier T2; medium urgency) and green (Tier T3; lowest urgency). A tiered approach will be used and presented in the checklist at the next section.

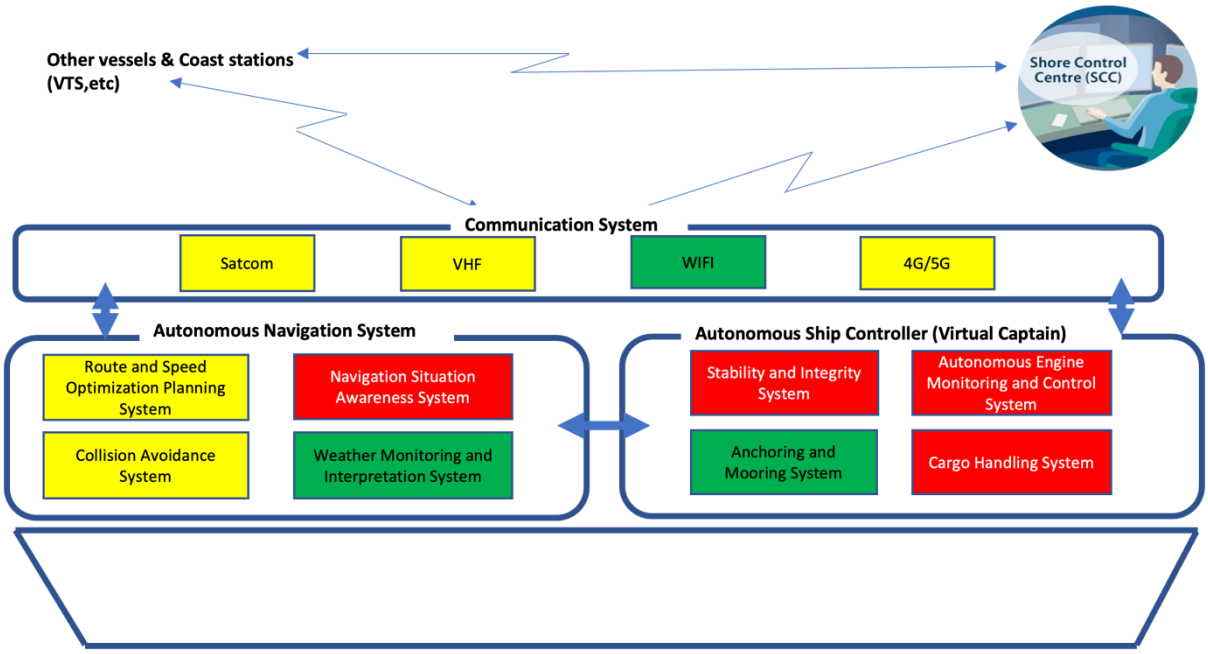

Figure 5 Tiered Security Level for System Overview

Vulnerabilities within high-risk systems present opportune targets for potential attackers, thereby posing a significant risk of financial loss to the organisation and disruption of ship operations. Medium-risk systems have relatively lower susceptibility to attacks; nevertheless, their compromise could lead to network unavailability and resource disruption. Systems categorised

as low risk face diminished probabilities of being targeted compared to the other two groups. However, any compromise within these systems, despite the reduced risk, can still jeopardise the safety of the ship, its crew, and cargo.

Table 8 High Risk Category

High Risk Systems	Attack Surfaces	Cyber-attack
Navigation situation awareness system	GNSS, AIS, LiDAR/LADAR/RADAR/Camera, physical damage, supply chain compromise, Radar signal	GNSS spoofing, GNSS jamming, AIS spoofing, sensor manipulation, communications interference
Stability and integrity system	Data sources, supply chain backdoors, communications	Data tampering, Denial-of-Service (DoS) Attacks
Autonomous engine monitoring and control system	Supply chain, engine management software, network links, sensors	Malware infection, communication disruption, spoofed sensor data
Cargo handling system	Shore-based coordination, cargo environment, cargo sensors, inventory logs	Unauthorised access, insider threats, malware installation

Table 9 Medium Risk Category

Medium Risk Systems	Attack Surfaces	Cyber-attack
Communication system - Satcom	Satellite, signal interception, user terminal, network links, supply chain, encryption keys, jamming, spoofing	Data modification and corruption, Outdated software vulnerability, Eavesdropping, Hijacking, Spoofing, Denial-of-Service (DoS) Attacks
Communication system – VHF and 4G/5G	Radio equipment, signal interception, jamming, Man-in-the-Middle Attacks, supply chain, physical access to infrastructure	Eavesdropping, Denial-of-Service (DoS) Attacks
Route and speed optimisation planning system	Sensors, telecommand interception, network intrusions, algorithms, connected network	Algorithm undermined, False feedback, Denial-of-Service (DoS) Attacks, Communication interception
Collision avoidance system	Sensors, algorithms, communication links, connected network, navigation data	False data injection, Sensor manipulation, Denial-of-Service (DoS) Attacks, Communication Interception

Table 10 Low Risk Category

Low Risk Systems	Attack Surfaces	Cyber-attack

Communication system – Wi-Fi	Wi-Fi access points, Wi-Fi signals, user credentials	Denial-of-Service (DoS) Attacks, unauthorised access
Weather monitoring and interpretation system	Sensors, weather data feeds, supply chain backdoors, algorithms, data links	Sensor jamming and spoofing, Denial-of-Service (DoS) Attacks, algorithm undermined
Anchoring and mooring system	Sensors, external communications, physical damage	Malware infection, communication disruption, spoofed sensor data

Based on the analysis defined in this section, the next section provides detailed and tiered checklists for incorporation of mitigation strategies for better defence of an autonomous ship.

7: CHECKLIST

By means of comprehensive cyber risk assessment of autonomous ships, one can categorise risks based on their respective risk scores, distinguishing between high, medium, and low-risk factors. This initial assessment sets the groundwork for a subsequent checklist, offering specific mitigation measures precisely tailored to address the identified cyber risks inherent to on-board systems of autonomous ships. Having a checklist and checking on the cyber hygiene level of the ship provides clear guidance to maritime stakeholders on the specific items, processes, and questions that should be considered during risk evaluations. A standardized checklist helps ensure a systematic and thorough risk evaluation is conducted consistently and a good checklist will incorporate all important areas, components, and risk factors that need to be examined for an autonomous ship.

7.1 TIERED SECURITY

This approach involves categorising assets by criticality and implementing corresponding levels of protection. Through the evaluation of cyber risk, the OT systems and their associated risks were categorised into, high, medium and low-risk categorises based on the likelihood of encountering various risks. By assigning systems, devices, and facilities to one of these tiers, maritime authorities can tailor security controls to the specific risks. The tiers are defined as shown in Table 11.

Table 11 Security Tier Definition

Security Tier	Security Tier Definition	Security Checklist
Tier 1	Tier 1 checklist comprises cybersecurity measures designed to address high-risk cyber threats. This indicates that the measures listed in this tier are strongly advised for implementation on ships.	Checklist aimed at risk mitigation within high-risk classification
Tier 2	Tier 2 checklist comprises cybersecurity measures designed to address medium-risk cyber threats. This indicates that the measures listed in this tier are recommended to have onboard.	Checklist aimed at risk mitigation within medium-risk classification
Tier 3	Tier 3 checklist comprises cybersecurity measures designed to address low-risk cyber threats. This indicates that the measures listed in this tier are good to have onboard.	Checklist aimed at risk mitigation within low-risk classification

Ultimately, a structured tiered checklist that are tailored to the security needs of autonomous ships allows maritime stakeholders to improve the safety at the right level across the entire ship ecosystem.

7.2 CHECKLIST WITH SECURITY TIERS

7.2.1 Checklist – Shore Control centre (SCC)

Table 12 Checklist – Shore Control Centre

OT Sub-systems	Cyber-risk Checklist	Mitigation Checklist	Security Tier
Shore Control Centre	Unauthorised Access and Intrusions	☐ T1-1 Implement multifactor authentication for remote access to shore control systems and networks. ☐ T1-2 Establish role-based access controls, aligning access permissions and privileges with personnel roles and responsibilities. ☐ T1-3 Segment shore control centre networks into separate security zones for operations, OT systems, IT systems, etc. ☐ T1-4 Deploy firewalls between network zones and set strict rules allowing only required traffic/ports.	1
	Insider threats	☐ T1-5 Implement an intrusion detection system and intrusion prevention system to continuously monitor networks for malicious activity such as setting alerts. ☐ T1-6 Provide regular cybersecurity awareness training for shore control personnel to shape staff mindset and avoid risky actions that could enable intrusions.	
	Data Tampering and Modification	☐ T1-7 Implement physical access controls like key card readers to restrict unauthorised entry to facilities. ☐ T1-8 Deployment CCTV cameras in shore facilities and identify unauthorised activities to monitor staff behaviour patterns. ☐ T1-9 Implement robust data integrity controls to detect any unauthorised changes to critical data.	
	Network and Communication Vulnerabilities	☐ T1-10 Encrypt sensitive data at rest and during transmission to protect it from tampering. ☐ T1-11 Use input validation mechanisms to ensure that data received is not tampered with during transmission.	

	Supply chain attacks Code Injection and malware infection Social engineering	☐ T1-12 Classify data based on its sensitivity and importance, applying different security measures based on data type. ☐ T1-13 Harden network devices and removing or disabling unnecessary services and ports. ☐ T1- 14 Establish a vendor risk assessment process to evaluate security practices of third-party suppliers. ☐ T1-15 Require vendors to provide detailed information about their security controls and protocols. ☐ T1-16 Implement vulnerability scanning and penetration testing on all vendor-supplied systems. ☐ T1-17 Provide staff training on supply chain risk awareness and reporting process. ☐ T1-18 Establish tamper-evident packaging and delivery practices for incoming equipment. ☐ T1-19 Implement anti-malware scanning tools on all shore control system endpoints, networks, and removable media such as USB drives. ☐ T1-20 Setup network-based anti-malware tools like firewalls to block known malware. ☐ T1-21 Establish strict patch management and software update processes to remediate code vulnerabilities. ☐ T1-22 Prohibit use of personal devices on shore control systems. ☐ T1-23 Establish security awareness and training programs to educate staff on social engineering techniques like phishing and vishing. ☐ T1-24 Limit public information available about shore centre personnel and systems that could assist adversaries. ☐ T1-25 Implement stimulated social engineering tests to build resilience and identify susceptible personnel. ☐ T1-26 Establish processes for identity verification before disclosing sensitive information.	

7.2.2 Checklist – Communication System

Table 13 Checklist - Communication System

OT Sub-systems	Cyber-risk Checklist	Mitigation Checklist	Security Tier
Satellite Communication System (SATCOM)	Data Modification and Corruption	☐ T2-1 Implement end-to-end encryption of satellite links to prevent interception and alteration of data. ☐ T2-2 Enable data authentication via hash functions or tokens to detect tampering. ☐ T2-3 Perform regular security audits and scans of satellite infrastructure. ☐ T2-4 Establish network segmentation and access controls to limit exposure.	2
	Jamming	☐ T2-5 Maintain backup communication channels that are not vulnerable to satellite jamming. ☐ T2-6 Implement frequency hopping spread spectrum technology to make jamming signals across the wide satcom frequency band difficult.	
	Outdated VSAT Software Vulnerabilities	☐ T2-7 Implement a robust patch management system that automates patching across the satcom ecosystem. ☐ T2-8 Implement additional monitoring like intrusion detection around unpatchable legacy satellite system components. ☐ T2-9 Establish policies and procedures to promptly test and apply critical security patches when they become available.	
Communication System – VHF, 4G and 5G	Eavesdropping	☐ T2-10 If possible, establish protected distribution system with redundant encryption for high priority command and control communications. ☐ T2-11 Establish secure key management procedures for distribution and storage of encryption keys or certificates. ☐ T2-12 Provide Satcom security training for personnel focused on eavesdropping prevention.	
	Hijacking	☐ T2-13 Encrypt necessary satellite command and control communications using standards like AES to prevent takeover of sessions.	

	Spoofing Denial of Service (DoS) Attacks	☐ T2-14 Conduct regular penetration testing of satellite infrastructure to validate security controls. ☐ T2-15 Deploy robust firewalls and anomaly detection systems on satellite terminals to identify and block spoofed traffic. ☐ T2-16 Install anti-spoofing antennas and filters on satellite terminal equipment to mitigate effects of tampered signals. ☐ T2-17 Analyse for unusual behaviours that could indicate spoofing. ☐ T2-18 Establish backup communication channels using different techniques like terrestrial radio as a redundancy. ☐ T2-19 Prioritise and allocate guaranteed bandwidth for critical satellite control and command links. ☐ T2-20 Implement infrastructure redundancies like backup ground stations and diverse satellite or radio links to maintain availability if DoS succeeds. ☐ T2-21 Rate limitations to ground station management interfaces to prevent resource exhaustion. ☐ T2-22 Establish DoS mitigation relationships with satellite operators and service providers.	
Communication System – Wi-Fi	Eavesdropping Denial of Service (DoS) Attacks	☐T3-1 Implement Wi-Fi encryption using the latest WPA2/WPA3 standards to encrypt ship traffic over the air. ☐ T3-2 Enable Wi-Fi access point traffic encryption settings like MAC address filtering to only allow authorised devices to connect ☐ T3-3 Maintain approved list of Wi-Fi devices authorised to connect to ship networks. ☐ T3-4 Establish inbound and outbound filtering on Wi-Fi access point firewalls to block known DoS vectors. ☐ T3-5 Set incident response plans to activate mitigations if DoS is detected on the Wi-Fi network.	3

7.2.3 Checklist – Autonomous Ship Controller (ASC)

Table 14 Checklist - Autonomous Ship Controller

OT Sub-systems	Cyber-risk Checklist	Mitigation Checklist	Security Tier
Autonomous Engine Monitoring and Control System (AEMCS)	Denial of Service (DoS) Attacks	☐ T1-27 Implement intrusion detection and prevention system to identify and block malicious network traffic associated with DoS attacks ☐ T1-28 Prioritise and allocate guaranteed bandwidth for engine telemetry and emergency control channels. ☐ T1-29 Continuously monitor engine network traffic patterns. ☐ T1-30 Establish engine control system resiliency processes to gracefully degrade non-essential services during DoS. ☐ T1-31 Implement secured audit logs to trace all authentication and authorisation events.	1
	Insufficient authentication and authorisation	☐ T1-32 Disable or remove any default accounts or unnecessary remote access services. ☐ T1-33 Enforce secure password policies for any necessary login credentials for engine systems. ☐ T1-34 Provide cybersecurity training for personnel focused on authentication best practices.	
	Outdated Software	☐ T1-35 Establish a schedule for regular software updates, including security patches and bug fixes. ☐ T1-36 Ensure that software vendor provides ongoing support and updates for the system. ☐ T1-37 Implement a robust patch management process to promptly apply security updates. ☐ T1-38 Regularly backup the software and system configurations to recover in cases of issues during updates. ☐ T1-39 Continuously monitor the system for signs of vulnerabilities or issues related to software updates.	

Stability and Integrity System (SIS) **Cargo Handling System (CHS)**	Data Tampering Unauthorised Access Insider threats	☐ T1-40 Implement strong encryption for data at rest and during transmission. ☐ T1-41 Enforce strict access controls to ensure that only authorised personnel can modify or access critical data. ☐ T1-42 Implement data integrity controls to detect and prevent unauthorised changes to critical data. ☐ T1-43 Log all access to sensitive data and monitor these logs for any unusual or unauthorised activities. ☐ T1-44 Segment the network to isolate the cargo handling system from less critical components, reducing the attack surface. ☐ T1-45 Assess the security practices of third party vendors providing services or equipment for the cargo handling system. ☐ T1-46 Implement strong user authentication methods, such as biometrics, to verify the identity of individuals accessing the system ☐ T1-47 Set up automated alerts for suspicious or unauthorised activities. ☐ T1-48 Establish an insider threat program that includes proactive monitoring, reporting mechanisms, and incident response procedures. ☐ T1-49 Promote a culture of security awareness among personnel, encouraging them to report any insider threat incidents. ☐ T1-50 Identify anomalous behaviour that may indicate insider threats.	
Anchoring and Mooring system	Malware infection Communication Disruption	☐T3-6 Install and regularly update antivirus and anti-malware software. ☐ T3-7 Use email and web filtering tools to block malicious attachments and links in the emails and web content. ☐ T3-8 Implement software whitelisting to allow only authorised and trusted applications to run on the system. ☐ T3-9 Keep the OS and software components up to date with security patches to address vulnerabilities. ☐ T3-10 Implement redundant communication links.	3

	Spoofed sensor data	☐ T3-11 Use reliable and fault-tolerant communication protocols that can recover from interruptions. ☐ T3-12 Ensure the availability of backup power supplies to maintain communication during power outages. ☐ T3-13 Conduct regular maintenance of communication equipment to identify and address potential issues before they lead to disruption. ☐ T3-14 Conduct regular communication testing and drills to ensure the effectiveness of backup and emergency procedures. ☐T3-15 Implement data authentication mechanisms to verify the authenticity and integrity of sensor data. ☐ T3-16 Use secure communication protocols and encryption for transmitting sensor data to prevent interception and tampering. ☐ T3-17 Employ redundant sensors and cross-reference their data to detect inconsistencies and anomalies. ☐ T3-18 Physically secure sensors to prevent tampering or unauthorised access. ☐ T3-19 Implement data validation mechanisms to ensure that sensor data is consistent and has not been tampered during transmission. T3-20 Ensure that the anchoring and mooring system complies with relevant maritime and cybersecurity regulations for sensor data integrity.	

7.2.4 Checklist – Autonomous Navigation System (ANS)

Table 15 Checklist - Autonomous Navigation System

OT Sub-systems	Cyber-risk Checklist	Mitigation Checklist	Security Tier
Navigation Situation Awareness System	GNSS	☐ T1-51 Implement signal authentication mechanisms to verify the authenticity of GNSS signals. ☐ T1-52 Deploy advanced jamming and spoofing detection systems to identify and respond to interference with GNSS signals. ☐ T1-53 Install backup navigation systems, such as inertial navigation or other satellite systems, to provide redundancy in case of GNSS disruption. ☐ T1-54 Use GNSS receivers with robust security features and regularly update their firmware to patch vulnerabilities. ☐ T1-55 Implement frequency hopping to make it more challenging for attackers to jam GNSS signals. ☐ T1-56 Encrypt GNSS data and communications to protect them from eavesdropping and tampering. ☐ T1-57 Employ cybersecurity measures, including intrusion detection systems, firewalls, and network segmentation, to safeguard GNSS data and infrastructure. ☐ T1-58 Configure the network to protect GNSS data from potential threats and unauthorised access. ☐ T1-59 Implement encryption for GNSS signals to protect them from spoofing and tampering. ☐ T1-60 Assess the security practices of third-party vendors providing GNSS equipment or services.	1
	LiDAR/LADAR/RADAR /Camera	☐ T1-61 Employ redundant sensor systems (LiDAR, LADAR, RADAR, and cameras) and integrate data fusion techniques to ensure continuous and reliable navigation.	

	AIS Denial of Service	☐ T1-62 Maintain accurate time synchronization across sensors to ensure data consistency and proper data fusion. ☐ T1-63 Conduct routine testing and calibration of sensors to maintain their accuracy and performance. ☐ T1-64 Establish emergency failover systems that can take control in the event of a sensor failure or cyber threat detection. ☐ T1-65 Train onboard personnel to understand and monitor the autonomous system and to respond to sensor-related incidents. ☐ T1-66 Ensure seamless integration of sensor data with autonomous navigation control systems, maintaining data accuracy and trustworthiness. ☐ T1-67 Implement authentication and encryption of AIS data to prevent spoofing, tampering, and eavesdropping. ☐ T1-68 Validate and filter AIS data against other sources like RADAR to identify spoofing or falsified vessel positions. ☐ T1-69 Configure firewall rules to limit network access to AIS receiver to prevent unauthorised data manipulation. ☐ T1-70 Institute redundant and diverse AIS receivers and antennas to minimize disruption from jamming. ☐ T1-71 Conduct frequent AIS radio spectrum scans to identify interference or unauthorised transmissions. ☐ T1-72 Establish physical access controls around AIS receiver to prevent tampering or unauthorised device connections. ☐ T1-73 Enable AIS error correction and integrity checking like cyclic redundancy checks to identify tampered data. ☐ T1-74 Establish operational procedures to cross-check AIS information against other sources before acting on it. ☐ T1-75 Maintain backup communication channels like RADAR that are not dependent on AIS. ☐ T1-76 Develop navigation restoration procedures to recover capabilities after DoS impact.	

Route and Speed Optimisation Planning System	Algorithm Undermined False Feedback Denial of Service (DoS) Attacks Communication Interception	☐T2-23 Establish robust design requirements and testing procedures for route planning algorithms to validate correctness. ☐ T2-24 Implement input data validation, sanitization, and integrity checks to prevent poisoning of algorithm logic. ☐ T2-25 Enable cryptographic signing of authorised algorithm and route logic files to prevent unauthorised modification. ☐ T2-26 Establish strict change control processes governing any modifications to approved route planning algorithms. ☐ T2-27 Conduct code reviews and testing to verify integrity of algorithm implementations and calculations. ☐ T2-28 Segregate algorithm development, testing, and production instances to prevent unvalidated changes. ☐ T2-29 Train programmers on secure coding practices for safety-critical maritime algorithms and simulations. ☐ T2-30 Validate all sensor inputs to route planning systems for correctness. ☐ T2-31 Continuously monitor network traffic for unusual patterns of DoS. ☐ T2-32 Prohibit unprotected wireless connections into the route planning network.	2
Collision Avoidance System	False data Injection	☐T2-33 Validate sensor inputs to collision avoidance systems and cross-check against redundant sources. ☐ T2-34 Establish strict fail safes for collision avoidance responses if received data is suspect. ☐ T2-35 Continuously monitor collision avoidance system outputs for inconsistencies indicating false data. ☐ T2-36 Conduct penetration testing focused on collision avoidance systems to uncover potential vulnerabilities. ☐ T2-37 Enforce principle of least privilege in granting access to provide inputs or commands.	

	Sensor Manipulation	☐ T2-38 Log and audit all data inputs and commands processed by collision avoidance systems. ☐ T2-39 Implement configuration management to detect unauthorised modification of collision avoidance parameters. ☐ T2-40 Establish emergency disconnect of electronic navigation from automated collision avoidance. ☐ T2-41 Implement sensor data encryption to prevent interception or manipulation of readings. ☐ T2-42 Authenticate sensor data with digital signatures or certificates to validate readings originate from legitimate sources. ☐ T2-43 Establish redundancy and diversity of sensors measuring same parameters to cross-check outputs. ☐ T2-44 Conduct frequent sensor health checks and sanity validations of sensor readings. ☐ T2-45 Provide cybersecurity and insider threat awareness training to teams with sensor access. ☐ T2-46 Follow strict system decommissioning practices prior to disposal or reuse of sensors. ☐ T2-47 Establish effective backup and restoration procedures for sensor configurations. ☐ T2-48 Implement device authentication to validate legitimacy of any sensor prior to accepting data.	
Weather Monitoring and Interpretation System	Sensor Jamming and spoofing	☐T3-21 Conduct routine maintenance checks to ensure sensors are functioning correctly. Any unusual behaviour should trigger a sensor inspection. ☐ T3-22 Install duplicate sets of weather sensors, and ensure that the data from different sets matches. If there's a discrepancy, take the majority reading as the accurate one. ☐ T3-23 Establish baseline profiles for expected sensor data under normal conditions. When data deviates significantly from these profiles, investigate the cause.	3

	Denial of Service (DoS) Attacks	☐ T3-24 Calibrate weather sensors at regular intervals to maintain their accuracy. ☐ T3-25 Implement alert systems that trigger warnings when sensor data deviates significantly from historical patterns or established norms. ☐ T3-26 Have backup weather data sources available, such as handheld weather instruments, in case of sensor failures. ☐ T3-27 Regularly review and update the checklist and security measures to adapt to evolving threats and lessons learned from incidents. ☐ T3-28 Develop a well-defined incident response plan that outlines actions to take when a DoS attack is detected. ☐ T3-29 Use network firewalls to filter and block malicious traffic from reaching the system. ☐ T3-30 Consider using third-party DDoS mitigation services that can filter out malicious traffic. ☐ T3-31 Train staff to recognize signs of a DoS attack and understand their role in the incident response plan. ☐ T3-32 Engage third-party cybersecurity experts to conduct regular audits and penetration testing to identify vulnerabilities.	
	Algorithm Undermined	☐ T3-33 Mitigating risks in the algorithms of a weather monitoring and interpretation system is crucial for accurate weather predictions and reliable operation. Here's a checklist of mitigation measures: ☐ T3-34 Thoroughly validate and test weather prediction algorithms against historical data and known weather events to ensure accuracy. ☐ T3-35 Implement version control for algorithms, ensuring that changes are tracked and can be rolled back if necessary. ☐ T3-36 Implement robust input validation to filter out malicious data and prevent exploitation of algorithm vulnerabilities. ☐ T3-37 Periodically subject algorithms to independent code reviews and audits to identify vulnerabilities and errors. ☐ T3-38 Design algorithms to be resilient to anomalies and outliers in data, reducing the impact of incorrect or manipulated data.	

		☐ T3-39 Continuously train machine learning models and update algorithm parameters to adapt to evolving weather patterns. ☐ T3-40 Maintain transparency in algorithm design and operation, allowing stakeholders to understand how weather predictions are generated	

8: CONCLUSION

The integration of Operational Technology (OT) systems in autonomous ships is a pivotal advancement that brings transformative potential to the maritime industry. However, this advancement is not without its challenges, and cybersecurity emerges as a critical concern. The overview of cyber risks underscores the vulnerability of interconnected OT systems to various malicious activities, including Denial-of-Service (DoS) attacks, spoofing, malware infiltration, and sensor manipulation. These risks, if realised, can jeopardise vessel safety, operational efficiency, and environmental integrity. To mitigate these threats effectively, a multi-faceted approach is essential. Implementing robust cybersecurity measures, such as network segmentation, access controls, encryption, and real-time monitoring, can fortify the autonomous ship's digital infrastructure against potential intrusions. Additionally, fostering a culture of cybersecurity awareness and continuous crew training can significantly contribute to bolstering the human element, a crucial line of defence against cyber threats. A comprehensive understanding and systematic approach toward addressing cyber risks in autonomous ships are imperative for ensuring the successful, secure, and widespread adoption of this groundbreaking maritime technology.

ANNEX 1: COMPARISON WITH PREVIOUS WORK

In our earlier research, we incorporated viewpoints from conventional ship operations to discern the cybersecurity risks linked with OT systems [69]. This study has changed the target to be autonomous ships and further delivers a consolidation of OT system knowledge to advance MASS developments through disparate streams of research, projects and classification documentation. Both studies prescribe comprehensive cybersecurity controls to mitigate associated threats and vulnerabilities per system. The differing factor lies in the methodology employed for the risk assessment. The former study condenses complex risk factors into a matrix which can lead to an oversimplified view of multidimensional risks. Nuances may get lost in generalisation and wide rating bands may undermine precise risk analysis. However, the method applied in this study - FAA works in top-down fashion and it keeps decomposing a big system into subsystems until fundamental building blocks are reached. At the granular level, it calculates the risk associated with each fundamental building block and then sum up all the risks associated with all the subsystem, for a system which is hierarchically at higher level of structure. Likelihood, impact and detectability of an attack are included in the risk equation and all the failure modes and mechanisms are deduced from MITRE ATT&CK and MITRE ATLAS tactics and techniques. Compared to risk matrices which can potentially introduce human bias, MITRE could have deeper expertise in risk management, responding to real-world cyber threats effectively.

ACKNOWLEDGEMENTS

We extend our sincere appreciation to the following individuals and organisations for their invaluable contributions to the development of this version of guidelines:

- Dr. Victor Bolbot and Dr. Meriam Chaal, Aalto University
- Dr. Aybars Oruc, Founder, Cyber Onboard
- Dr. Kimberly Tam, University of Plymouth
- Philip Kwa, MSSD student, SUTD
- Dr Ahmed Amro, PhD student, NTNU
- Dr Yaxi Yang, Research Fellow, SUTD
- Sean Gunawan, Ivan Christian, Research Assistants, SUTD
- Jason Wong, PhD student, SUTD

Organisations:

- ClassNK
- CMA CGM
- CyberOwl
- Singapore Polytechnic

This work is carried out by iTrust, the Centre for Research in Cyber Security in the Singapore University of Technology and Design (SUTD) and funded by Singapore Maritime Institute (SMI) under the grant number SMI-2022-MTP-05. The team would like to thank the Maritime and Port Authority of Singapore (MPA) for its guidance and inputs throughout this study.

List of authors contributing to the guidelines:
Meixuan Li, Research Assistant, iTrust, SUTD
Awais Yousaf, Research Fellow, iTrust, SUTD
Mark Goh Voon Wei, Assistant Director, iTrust, SUTD
Jianying Zhou, Professor, Centre Director, iTrust, SUTD
Sudipta Chattopadhyay, Assistant Professor, iTrust, SUTD

For queries related to the guidelines, please write to itrust@sutd.edu.sg

REFERENCES

1. Tijan E, Jović M, Aksentijević S, Pucihar A. Digital transformation in the maritime transport sector. Technological Forecasting and Social Change. 2021 September; 170(120879).
2. Internation Maritime Organization. MSC 100/20/Add.1 Annex 2: Framework for the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS). [Online].; 2019 [cited 2023 October 10. Available from: https://maiif.org/wp-content/uploads/2019/06/MSC-100_20-Annex-20-1.pdf
3. Ahvenjärvi S. The Human Element and Autonomous Ships. International Journal on Marine Navigation and Safety of Sea Transportation. 2016 September; 10(3): 517-521.
4. Mallam SC, Nazir S, Sharma A. The human element in future Maritime Operations – perceived impact of autonomous shipping. Ergonomics. 2019 September; 63(3): 334-345.
5. Kavallieratos G, Spathoulas G, Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. Sensors. 2021 March; 21(5): 1691.
6. Bolbot V, Theotokatos G, Boulougouris , Vassalos D. Safety related cyber-attacks identification and assessment for autonomous inland ships. In International Seminar on Safety and Security of Autonomous Vessels (ISSAV); 2019; Helsinki. p. 1-15.
7. Yoo J, Jo Y. Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology. Sensor. 2023 May; 23(11): 1-19.
8. Cho S, ORYE E, Visky G, Prates V. Cybersecurity Considerations in Autonomous Ships. [Online].; 2022 [cited 2023 October. Available from: https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf
9. Chaal M, Banda OV, Basnet S, Hirdaris , Kujala P. An initial hierarchical systems structure for systemic hazard analysis of autonomous ships. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC); 2019; Helsinki. p. 140-153.
10. Kwa PTH. Cyber Risk Management Guidelines for Autonomous Ships. Master Thesis. Singapore : Singapore University of Technology and Design, Information Systems Technology and Design; 2023.
11. Amro A, Gkioulos , Katsikas S. Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. ACM Transactions on Privacy and security. 2023 March; 26(2): 1-33.
12. Munin , Grant. Final Report Summary-MUNIN (Maritime Unmanned Navigation through Intelligence in Networks). [Online].; 2019 [cited 2023 October 10. Available from: https://www.semanticscholar.org/paper/Final-Report-Summary-MUNIN-%28-Maritime-Unmanned-in-%29-Munin-Grant/5aebf0ce4f2da30bc665f4745b069a8f6b6729b1
13. Richardsen PW. DNV GL - REVOLT. [Online].; 2018 [cited 2023 October 10. Available from: https://www.bluebird-electric.net/artificial_intelligence_autonomous_robotics/Revolt_DNV_GL_ASV_Unmanned_Battery_Cargo_Vessel.htm
14. Ship Technology. Rolls-Royce reveals vision of remote and autonomous shipping through AAWA project latest findings. [Online].; 2016 [cited 2023 October 10. Available from:

https://www.ship-technology.com/news/newsrolls-royce-reveals-vision-of-remote-and-autonomous-shipping-through-aawa-project-latest-findings-4863708/?cf-view

15. Mayflower Autonomous Ship. The Mayflower Autonomous Ship Project. [Online].; 2020 [cited 2023 October 10. Available from: https://mas400.com
16. Hertzenberg B. Yara Birkeland. [Online].; 2023 [cited 2023 October 10. Available from: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/
17. POSH Excellence Through Safety. Partnered with ST Engineering on sea trials of autonomous vessel technology on our harbour tug, POSH Harvest. [Online].; 2021 [cited 2023 October 10. Available from: https://posh.com.sg/partnered-with-st-engineering-on-sea-trials-of-autonomous-vessel-technology-on-our-harbour-tug-posh-harvest/
18. O'Dwyer. MOL conducts joint study on autonomous collision avoidance. [Online].; 2020 [cited 2023 October 10. Available from: ://smartmaritimenetwork.com/2020/10/21/mol-conducts-joint-study-on-autonomous-collision-avoidance/
19. Baird Maritime. VESSEL REVIEW | ZHI FEI – CHINESE-BUILT 300TEU BOXSHIP BOASTS AUTONOMOUS NAVIGATION FEATURES. [Online].; 2021 [cited 2023 October 10. Available from: https://www.bairdmaritime.com/ship-world/boxship-world/vessel-review-zhi-fei-chinese-built-300teu-boxship-boasts-autonomous-navigation-features/
20. Shipbuilding News. Samsung Heavy Industries succeeds autonomous vessel navigation. [Online].; 2023 [cited 2023 October 10. Available from: HYPERLINK https://www.hellenicshippingnews.com/samsung-heavy-industries-succeeds-autonomous-vessel-navigation/
21. Tissari J, Makkonen H, Jokioinen E, Tuominen R, Saarni J, Jalonen R, et al. Remote and Autonomous Ships The next steps. [Online].; 2016 [cited 2023 October 10. Available from: https://www.utupub.fi/bitstream/handle/10024/157117/aawa-whitepaper-210616-1.pdf?sequence=1&isAllowed=y
22. Skredderberget A. The first ever zero emission, autonomous ship. [Online].; 2023 [cited 2023 October 10. Available from: https://www.yara.com/knowledge-grows/game-changer-for-the-environment/
23. American Bureau of Shipping. ABS Awards AIP to Smart Maritime Autonomous Vessel Technology. [Online].; 2021 [cited 2023 October 10. Available from: https://news.cision.com/american-bureau-of-shipping/r/abs-awards-aip-to-smart-maritime-autonomous-vessel-technology,c3834763
24. Mitsui O.S.K. Lines. Advanced Support Technologies for Safer Vessel Operation. [Online].; 2023 [cited 2023 October 10. Available from: "https://www.mol.co.jp/en/sustainability/innovation/case/safety/
25. Korean Register. Guidance for Autonomous Ships. [Online].; 2022 [cited 2023 October 10. Available from: http://krs.westus.cloudapp.azure.com/Files/KRRules/KRRules2022/data/data_other/ENGLISH/gc28e000.pdf
26. Maritime UK. MASS UK Industry Conduct Principles and Code of Practice 2022 (V6). [Online].; 2022 [cited 2023 October 10. Available from: https://www.maritimeuk.org/priorities/innovation/maritime-uk-autonomous-systems-regulatory-working-group/mass-uk-industry-conduct-principles-and-code-practice-2022-v6/

27. American Bureau of Shipping. Autonomous and Remote Control Functions. [Online].; 2021 [cited 2023 October 10. Available from: https://safety4sea.com/wp-content/uploads/2021/07/ABS-Autonomous-and-Remote-Control-Functions-2021_07.pdf
28. IRCLASS - Indian Register of Shipping. Guidelines on Remotely Operated Vessels and Autonomous Surface Vessels. [Online].; 2021 [cited 2023 October 10. Available from: http://www.irclass.org/media/5777/asv-guidelines_dec-2021_new.pdf
29. ClassNK. Guidelines for Automated/Autonomous Operation on ships (Ver.1.0). [Online].; 2020 [cited 2023 October 10. Available from: https://maritimecyprus.com/wp-content/uploads/2020/01/classnk-autonomous.pdf
30. Bureau Veritas. Guidelines for Autonomous Shipping. [Online].; 2019 [cited 2023 October 10. Available from: https://erules.veristar.com/dy/data/bv/pdf/641-NI_2019-10.pdf
31. China Classification Society. GUIDELINES FOR AUTONOMOUS CARGO SHIPS. [Online].; 2018 [cited 2023 October 10. Available from: https://www.ccs.org.cn/ccswzen/articleDetail?id=201910000000003792
32. DNV. Autonomous and remotely-operated ships. [Online].; 2018 [cited 2023 October 10. Available from: https://www.dnv.com/maritime/publications/remote-controlled-autonomous-ships-paper-download.html
33. Lloyd's Register. Cyber-enabled ships: ShipRight procedure – autonomous ships. [Online].; 2016 [cited 2023 October 10. Available from: https://issuu.com/lr_marine/docs/lr_cyber-enabled_ships_shipright_pr
34. Porathe T, Prison J, Man Y. Situation Awareness in Remote Control Centres for Unmanned Ships. In Human Factors in Ship Design & Operation; 2014; London.
35. Kim M, Joung TH, Jeong B, Park HS. Autonomous shipping and its impact on regulations, technologies, and industries. Journal of International Maritime Safety, Environmental Affairs, and Shipping. 2020 June; 4(2): 17-25.
36. Veitch E, Alsos OA. A systematic review of human-AI interaction in autonomous ship systems. Safety Science. 2022 April; 152(105778): 1-23.
37. Dybvik H, Veitch E, Steinert M. EXPLORING CHALLENGES WITH DESIGNING AND DEVELOPING SHORE CONTROL CENTERS (SCC) FOR AUTONOMOUS SHIPS. Proceedings of the Design Society: International Conference on Engineering Design. 2020 June; 1: 847-856.
38. Lynch KM, Banks VA, Roberts APJ, Radcliffe S, Plant KL. What factors may influence decision-making in the operation of Maritime autonomous surface ships? A systematic review. Theoretical Issues in Ergonomics Science. 2022 December.
39. Rødseth ØJ, Kvamstad B, Porathe T, Burmeister HC. Communication architecture for an unmanned merchant ship. In 2013 MTS/IEEE OCEANS; 2013; Bergen. p. 1-9.
40. Felski A, Zwolak K. The Ocean-Going Autonomous Ship—Challenges and Threats. Journal of Marine Science and Engineering. 2020 January; 8(1).
41. Deng X, Wang L, Gui J, Jiang P, Chen X, Zeng F, et al. A review of 6G autonomous intelligent transportation systems: Mechanisms, applications and challenges. Journal of Systems Architecture. 2023 September; 142(102929).
42. Höyhtyä , Huusko J, Kiviranta M, Solberg K, Rokka J. Connectivity for autonomous ships: Architecture, use cases, and research challenges. In 2017 International Conference on Information and Communication Technology Convergence (ICTC); 2017; Jeju.

43. Hoshino A, Umeda A, Nishina T, Kimura H, Hakozaki K, Ode T, et al. Evaluation of visual image for remotely controlled ship. Artificial Life and Robotics. 2020 January; 25: 294-300.
44. Höyhtyä M, Martio J. Integrated Satellite–Terrestrial Connectivity for Autonomous Ships: Survey and Future Research Directions. Remote Sensing. 2020 August ; 12(15).
45. Jovanović I, Perčić M, Vladimir N. Identifying differences between power system of conventional and autonomous ship with respect to their safety assessment. In The 18-th International Conference on Electrical Machines, Drives and Power Systems ELMA 2023; 2023; Varna.
46. King T, Welter CV, Svensen TE. Stability barrier management for large passenger ships. Ocean Engineering. 2016 October ; 125: 342-348.
47. International Maritime Organisation. Ship Design and Stability. [Online].; 2019 [cited 2023 October 10. Available from: https://www.imo.org/en/OurWork/Safety/Pages/ShipDesignAndStability-default.aspx
48. Chaal M, Banda OAV, Glomsrud J, Basnet S, Hirdaris S, Kujala P. A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science. 2020 December; 132(104939).
49. Thombre S, Zhao Z, Schmidt HR, García MV, Malkamäki T, Bhuiyan ZH, et al. Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review. IEEE Transactions on Intelligent Transportation Systems. 2022 January; 23(1): 64-83.
50. Wang J, Xiao Y, Li T, Chen PCL. A Survey of Technologies for Unmanned Merchant Ships. IEEE Access. 8 December ; 8: 224461-224486.
51. Ohn SW, Namgung H. Requirements for Optimal Local Route Planning of Autonomous Ships. Journal of Marine Science and Engineering. 2023 December; 11(1).
52. Longo G, Martelli M, Russo E, Zaccone R. Collision-avoidance capabilities reduction after a cyber-attack to the navigation sensors. In Conference Proceedings of iSCSS; 2022. p. 1-9.
53. Duc DN, Huu TT, Nananukul N. A Dynamic Route-Planning System Based on Industry 4.0 Technology. Algorithms. 2020 November; 13(12): 308.
54. Heffner K, Rødseth Ø. Enabling Technologies for Maritime Autonomous Surface Ships. Journal of Physics: Conference Series. 2019; 1357(012021).
55. Ramos MA, Utne IB, Mosleh A. Collision avoidance on maritime autonomous surface ships: Operators' tasks and human failure events. Safety Science. 2019 July; 116: 33-44.
56. Wu Y, Pelot RP, Hilliard C. The Influence of Weather Conditions on the Relative Incident Rate of Fishing Vessels. An International Journal. 2009 July; 29(7): 985-999.
57. Bolbot V, Theotokatos , Boulougouris , Vassalos. A novel cyber-risk assessment method for ship systems. Safety Science. 2020 November; 131(104908).
58. Tam K, Jones K. Cyber-Risk Assessment for Autonomous Ships. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security); 2018; Glasgow. p. 1-8.
59. Tam K, Jones K. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. WMU Journal of Maritime Affairs. 2019 January; 18(6).
60. Silverajan , Ocak , Nagel. Cybersecurity Attacks and Defences for Unmanned Smart Ships. In International Conference on Internet of Things (iThings) and IEEE Green Computing and

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018; Halifax. p. 15-20.

61. Hogg T, Ghosh S. Autonomous merchant vessels: examination of factors that impact the effective implementation of unmanned ships. Australian Journal of Maritime & Ocean Affairs. 2016 September; 8(3): 206-222.
62. Santamarta R. Maritime Security: Hacking into a Voyage Data Recorder (VDR). [Online].; 2015 [cited 2023 October 10. Available from: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/
63. Manulis M, Bridges CP, Harrison R, Sekar V, Davis A. Cyber security in New Space. International Journal of Information Security. 2020 May; 20: 287-311.
64. Loukas G, Gan D, Vuong T. A Review of Cyber Threats and Defence Approaches in Emergency Management. Future Internet. 2013 May; 5(2): 205-236.
65. Stelkens-Kobsch TH, Hasselberg A, Mühlhausen T, Carstengerdes N, Finke M, Neeteson C. Towards a more Secure ATC Voice Communications System. In 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC); 2015; Prague. p. September.
66. ELMARADY AA, RAHOUMA K. Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment. IEEE Access. 2021 October; 9: 143997-144016.
67. Kavallieratos G, Katsikas S, Gkioulos V. Cyber-Attacks Against the Autonomous Ship. In CyberICPS 2018 and SECPRE 2018; 2018; Barcelona. p. 20-36.
68. Kelvin J, Kimberly T, Papadaki M. Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference. 2016 April; 1(1).
69. Rajaram P, Dumbala R, Goh M, Zhou J. Guidelines for Cyber Risk Management in Shipboard OT Systems. [Online].; 2022 [cited 2023 October 10. Available from: https://itrust.sutd.edu.sg/news-events/news/guidelines-for-cyber-risk-management-in-shipboard-ot-systems/
70. Tusher M, Munim , Notteboom, TE, Kim TE, Nazir. Cyber security risk assessment in autonomous shipping. Maritime Economics & Logistics. 2022 January; 34: 208-227.
71. Romanovskiy VV, Ivanov VS, Shniak BV. Electric drive of anchor and mooring mechanisms on see-going ships. In PROCEEDINGS OF THE II INTERNATIONAL SCIENTIFIC CONFERENCE ON ADVANCES IN SCIENCE, ENGINEERING AND DIGITAL EDUCATION: (ASEDU-II 2021); 2022; Krasnoyarsk.
72. Wróbel , Montewkab , Kujala. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability Engineering and System Safety. 2017 March; 165: 155-169.
73. Lagouvardou. Maritime Cyber Security: concepts, problems and models. Master Thesis. Denmark: Technical University of Denmark, Department of Management Engineering; 2019.
74. Zăgan , Raicu. Understanding of the cyber risk on board ship and ship stability. Annals of "Dunarea de Jos" Universitv of Galati. Fascicle XI, Shipbuilding. 2019 November; 42: 81-90.
75. Seferoglu , Turk AS. Review of Spoofing and Jamming Attack on the Global Navigation Systems Band and Countermeasure. In 9th International Conference on Recent Advances in Space Technologies (RAST); 2019; Istanbul. p. 513-520.

76. Aybars O. Potential Cyber Threats, Vulnerabilities, and Protections of Unmanned Vehicles. Journal of Unmanned Vehicle Systems. 2022 January; 10(1): 51-58.
77. Brooks Z. Hacking driverless vehicles. [Online].; 2016 [cited 2023 October 10. Available from: https://defcon.org/images/defcon-21/dc-21-presentations/Zoz/DEFCON-21-Zoz-Hacking-Driverless-Vehicles.pdf
78. Tu J, Ren M, Manivasagam S, Liang M, Yang B, Du R, et al. Physically Realizable Adversarial Examples for LiDAR Object Detection. In IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); 2020; Seattle. p. 13713-13722.
79. Alguliyev , Imamverdiyev , Sukhostat. Cyber-physical systems and their security issues. Computers in Industry. 2018 September; 100: 212-223.
80. Mednikarov B, Tsonev , Lazarov. Analysis of Cybersecurity Issues in the Maritime Industry. Information & Security: An International Journal. 2020 September; 47(1): 27-43.
81. Hyra. Analyzing the Attack Surface of Ships- Brace yourself cyber pirates are coming. Master Thesis. Denmark: Technical University of Denmark(DTU), Department of Applied Mathematics and Computer Science; 2019.
82. Glasius R, Komoda , Gielen CAM. Neural Network Dynamics for Path Planning and Obstacle Avoidance. Neural Networks. 1995; 8(1): 125-133.
83. Kissner. Hacking Neural Networks: A Short Introduction. ArXiv. 2019 November.
84. Androjna , Brcko , Pavic , Greidanus. Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering. 2020 October; 8(10): 776.
85. Huang ZQ, Chen YC, Wen CY. Real-Time Weather Monitoring and Prediction Using City Buses and Machine Learning. Sensors. 2020 September; 20(18): 5173.
86. Karvelis P, Mazzei , Biviano , Stylios. PortWeather: A Lightweight Onboard Solution for Real-Time Weather Prediction. Sensors. 2020 June; 20(11): 3181.
87. Kavallieratos , Diamantopoulou , Katsikas K. Shipping 4.0: Security Requirements for the Cyber-Enabled Ship. IEEE Transactions on Industrial Informatics. 2020 October; 16(19): 6617-6625.
88. Yağdereli E, Gemci C, Aktaş AZ. A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation. 2015 October; 12(4): 369-381.
89. European Union Agency For Security. Good practices for cybersecurity in the maritime sector. [Online].; 2019 [cited 2023 October 10. Available from: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
90. BIMCO. The Guidelines on Cyber Security onboard Ships - Version 4. [Online].; 2020 [cited 2023 October 10. Available from: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx?rev=e86ee4330cce44d7b90ad718e8af3c2e
91. Wingrove. 'Impregnable' radar breached in simulated cyber attack. [Online].; 2018 [cited 2023 October 10. Available from: https://www.rivieramm.com/news-content-hub/news-content-hub/impregnable-radar-breached-in-simulated-cyber-attack-25158
92. Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. Cybersecurity challenges in the maritime sector. Network. 2022 March; 2(1): 123-138.

93. Amro A, Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security. 2022 November; 22: 249-288.
94. Yousaf A, Amro A, Kwa TH, Li M, Zhou J. Cyber risk assessment of cyber-enabled autonomous cargo vessel. 2023. Publishing.