Guidelines for

Cyber Risk Management in Shipboard Operational Technology Systems

1st Edition
Published 22 Feb 2022

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

TERMS OF USE

The guidelines given in this document are solely intended for use as a reference or guide at the user's own risk. The authors and contributors do not hold responsible for the precision of any information or recommendations provided or neglected in this document or for any issues or failures caused as an effect of adhering to the guidelines provided in this document.

EXECUTIVE SUMMARY

Over 80 percent of the goods in the world are moved via sea trade. Ships are hugely reliant on technologies for their operations such as navigation, communication, propulsion, power management and cargo management, but cyber threats are still emergent. Weak cybersecurity controls and processes can potentially lead to severe consequences such as ship damage, loss of lives and also cause reputational and financial loss for the company, which might take years to recover economically. Hence, adopting an effective cyber risk management approach plays a vital role in safeguarding ships from cyberattacks.

The guidelines in this document aim to help maritime authorities better understand the potential cyber risks in major shipboard operational technology (OT) systems and also guide in implementing efficient cybersecurity practices onboard ships. High-level observations from the study are as follows:

- Lack of proper cybersecurity controls in the ship is one of the main reasons for cyberattacks. The interconnection between IT systems and OT systems, lack of crew awareness, use of weak passwords, default configurations, use of old versions of software, open USB ports and lack of encryption across the network are some of the major vulnerabilities that cyber attackers can easily exploit to compromise a ship system.
- While crew awareness is an important first step, it is vital to enforce proper security mechanisms to prevent hackers from accessing the shipboard systems and sensitive information.
- It is also crucial to consider human factors – being the weakest link – and enforce strict physical security measures.
- The cyber hygiene of a vessel must be assessed regularly to safeguard the vessel from the existing and new vulnerabilities.

The four OT systems considered in these guidelines are: Communication Systems, Propulsion, Machinery and Power Control Systems, Navigation Systems, Cargo Management Systems. In these guidelines, the cyber risks and impacts associated with the sub-systems of these major OT systems are discussed, and a detailed cyber risk assessment approach is provided to guide in assessing the cyber risks. Specific actionable mitigation measures are provided to mitigate these cyber risks. Finally, a checklist is also included to help maritime authorities and ship owners assess the cyber hygiene and security tiers of vessels.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS

AIS	Automatic Identification System
BWS	Ballast Water System
CAN	Controller Area Network
CCR	Cargo Control Room
CPA	Closest Point of Approach
DKIM	Domain Keys Identified Mail
DMZ	Demilitarized Zone
DPS	Dynamic Positioning System
ECDIS	Electronic Chart Display and Information System
FTP	File Transfer Protocol
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
ICS	Integrated Communication System
INMARSAT	INternational MARitime SATellite Organization
INS	Integrated Navigation System
IP	Internet Protocol
IT	Information Technology
NAVTEX	NAVigational TEleX
NMEA	National Marine Electronics Association
OS	Operating System
OT	Operational Technology
PC	Personal Computer
PKI	Public Key Infrastructure
RADAR	RAdio Detection And Ranging
RF	Radio Frequency
SATCOM	Satellite Communication System
SMB	Server message block
SMIME	Secure/Multipurpose Internet Mail Extensions
SSHv2	Secure Shell 2.0
USB	Universal Serial Bus
VDR	Voyage Data Recorder
VHF	Very High Frequency
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WLAN	Wireless Local Area Network

1 INTRODUCTION

With the growing demand for goods transportation by sea around the world, rapid technological advancements have been made to meet those demands in tandem. Despite their benefits, often, there is still a lack of effective adherence to cyber hygiene practices. Poor cybersecurity posture can have a significant impact on the safety of the vessel, crew and cargo. To this end, it is vital to keep the ship's systems, hardware, sensors and networks from being tampered with or accessed without authorisation. From a personal data protection perspective, it is critical to secure the computer systems since they contain personally identifiable information, intellectual property, sensitive data and information. In some cases, poor system setups allow an attacker to easily exploit a vulnerability. As vessels connect to the Internet to increase the efficiency of their operations and communications, OT systems correspondingly become more exposed to cyber-attacks as well.

The guidelines in this document aim to address the above issues by informing maritime authorities and ship owners who are responsible for investigating and determining the cyber hygiene and cyber-readiness of the vessels. Cognizant of the wide spectrum of cyber knowledge of its readers, this document is structured so that it is easy for adoption by ship owners – and enforcement by maritime authorities – while considering the balance of risks against costs. In turn, this helps ship owners implement feasible, cost-effective security solutions to secure OT systems in their vessels.

Several other guidelines published by organisations like the IMO, BIMCO, DNV and ABS, do focus on providing guidelines for maritime cyber risk management, though their target audience tend to be those at the management level. On the other hand, this document aims to provide actionable mitigation measures that can be readily adopted and used by engineers, IT specialists and vessel inspectors.

The structure of this document is as follows: First, it provides a description of the four shipboard OT systems and their sub-systems. Second, the cyber risks associated with the OT systems and their possible attack surfaces are listed, along with a description of possible attack scenarios. Third, mitigation measures for the corresponding cyber risks are outlined. A cyber risk assessment methodology to assess the cyber risks is also provided. Finally, the document provides a checklist using a tiered security approach for determining the cybersecurity hygiene of vessels. Thus, this document will serve as a practicable guide to those responsible for the cybersecurity of shipboard OT systems, such as engineers and IT/OT system specialists, as well as vessel inspectors. Figure 1 depicts the approach taken in producing these guidelines.

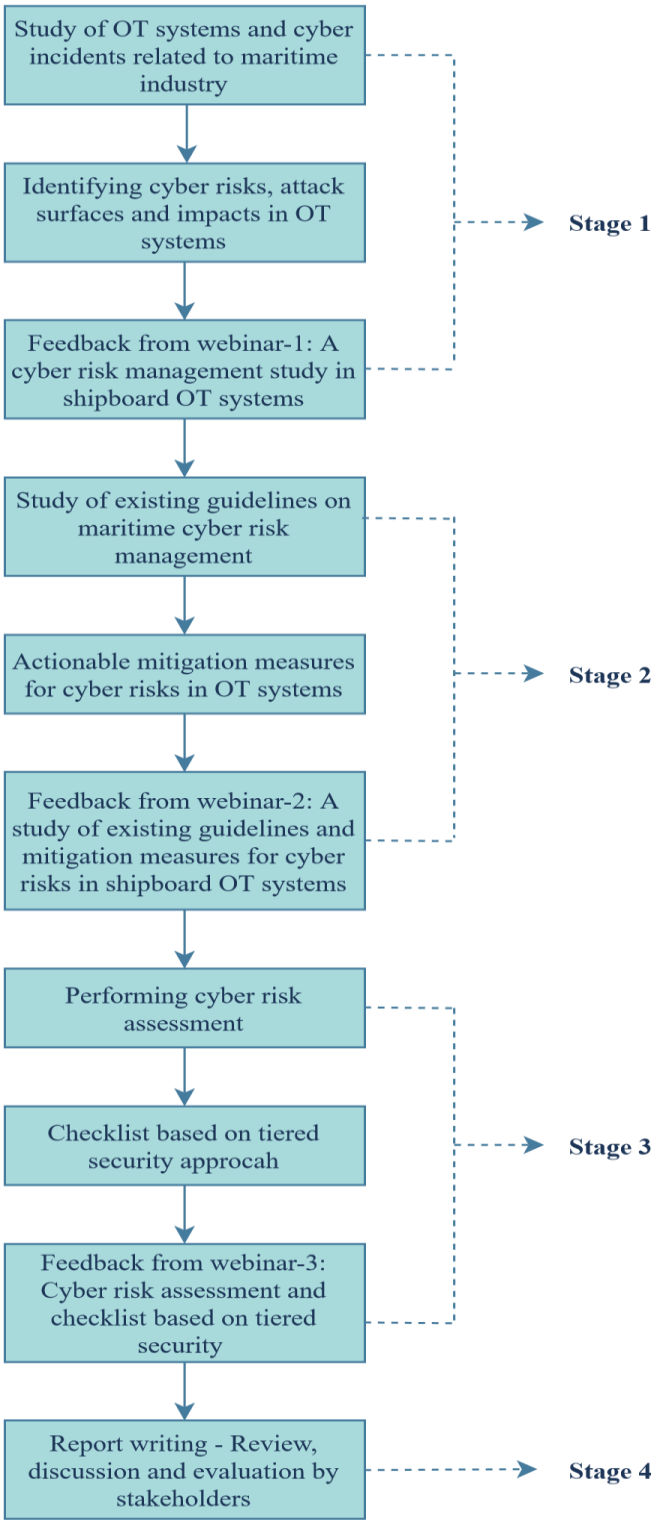

Figure 1 Roadmap for producing the new guidelines

Stage 1: The first stage involved a detailed study of various shipboard OT systems and sub-systems and real-time cyber incidents in the maritime industry. Once the sub-systems to be considered for the study were finalised along with the cyber risks in OT sub-systems and their impacts, the team visited an oil tanker and a container vessel to gain more insights into the operation of OT systems and their

specifications. Crew members were also interviewed. Findings from this stage were presented in a webinar and were well-received by different stakeholders.

Stage 2: This stage involved the study of existing guidelines published by various institutions and maritime organisations. Then, a set of actionable mitigation measures were framed for tackling the cyber risks identified in shipboard OT systems. Findings from this stage of research were presented in a second webinar and the team received feedback from various stakeholders.

Stage 3: During this stage, a cyber risk assessment approach was considered, and the risk scores of cyber risks identified in Stage 1 were evaluated against severity and likelihood in a 4x4 matrix. The team then opted for a tiered security approach to provide a checklist for determining the cyber hygiene of the vessel.

Stage 4: In this stage, the team finalised the guidelines after being reviewed by various stakeholders.

2 BACKGROUND

The technical advancements in the maritime industry have led to a rise in cyber threats, spurring the maritime industry to implement good cybersecurity practices onboard ships and ports. A few maritime cybersecurity guidelines have been published by various maritime organisations such as the International Maritime Organization (IMO), Baltic and International Maritime Council (BIMCO), American Bureau of Shipping, European Network and Information Security Agency (ENISA), Det Norske Veritas (DNV) and a multidisciplinary professional engineering institution knows as the Institution of Engineering and Technology. Table 1 lists the related guidelines and documents reviewed in this study.

Table 1 List of existing guidelines

Name of the organisation	Name of the document	Year of publication
American Bureau of Shipping (ABS)	The Guide for Cybersecurity Implementation for the Marine and Offshore Industries, ABS Cybersafety Volume 2	2021
Baltic and International Maritime Council (BIMCO)	Guidelines on Cyber Security Onboard Ships (Version 4)	2020
Det Norske Veritas (DNV)	Class guideline-Cyber Secure	2020
	Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation	2016
European Network and Information Security Agency (ENISA)	Good practices for cybersecurity in the maritime sector	2019
	Analysis of Cyber Security Aspects in the Maritime Sector	2011
International Maritime Organization (IMO)	Guidelines on Maritime Cyber Risk Management	2017
Institution of Engineering and Technology (IET)	Code of Practice Cyber Security for Ships	2017

According to the International Maritime Organization's (IMO) resolution MSC.428(98) *Maritime cyber risk management in Safety Management Systems*, any ship's Safety Management System (SMS) must consider cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) code [1]. It also encourages administrators to address the cyber risks appropriately in the SMS before the first annual verification of company's Document of Compliance on 1 January 2021. This resolution highlights IMO's *Guidelines on Maritime cyber risk*

management (MSC-FAL.1/Circ.3), where high-level recommendations on maritime cyber risk management are provided, to protect the maritime industry from the existing and rising cyber threats [2]. These guidelines put forward the five functional elements defined by the National Institute of Standards and Technology (NIST) cybersecurity framework, namely, identify, protect, detect, respond, and recover, which help effective cyber risk management [3]. It also insists that a productive cyber risk management should begin at the senior management level, and cyber risk awareness must be established at all tiers of an organization.

Along with references to NIST and ISO/IEC 27001 cybersecurity frameworks, the IMO's guidelines also refer to the *Guidelines on Cyber Security Onboard Ships Version 4 issued in 2020*, published and supported by various maritime organisations such as the Baltic and International Maritime Council (BIMCO), Chamber of Shipping of America (CSA), Digital Containership Association (DCA), Intercargo, Intermanager, INTERTANKO, ICS, IUMI, OCIMF, Sybass and World Shipping Council [4]. These guidelines address the importance of cybersecurity onboard ships with an aim to enhance the safety and security of ships and the crew. It also addresses the cyber risks and impacts in shipboard systems and advices the ship operators and ship owners on the required actions to ensure the security of shipboard systems.

In 2016, Det Norske Veritas (DNV) recommended a set of cybersecurity practices with the publication of *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*, targeting those in charge of cybersecurity in their organisations [5]. DNV's guidelines are built on the basis of recognised guidelines issued by organisations such as IMO and BIMCO. It highlights various cyber threat factors surrounding the maritime sector and focuses on cyber risk assessment and crucial improvements, verification, and validation mechanisms required for cybersecurity resilience in ships. Also, the *class guideline Cyber Secure* notation (October 2020 edition) by DNV addresses the cybersecurity of a ship's primary functions and the operational needs of ship owners [6]. The notations, Cyber Secure, Cyber Secure (Essential) and Cyber Secure (Advanced) covers 10 fundamental functions including propulsion, steering, power generation, navigation, etc., and is applicable where cyber risk management system is established and is implemented into existing procedures and systems. Additionally, the "+" notation allows ship owners to append additional functions for the notation.

The European Network and Information Security Agency published two documents relating to maritime cybersecurity. The first report, published in 2011, is on the *Analysis of Cyber Security Aspects in the Maritime Sector,* highlighted the cybersecurity issues and challenges in the maritime industry, along with recommendations for the same [7]. The second report on *Good Practices for Cybersecurity in the Maritime sector,* published in 2019, is focused on port cybersecurity, mainly targeting those in charge of IT and OT security within the port ecosystem [8]. The report outlines good practices for cybersecurity in the maritime port ecosystem, concerning both IT systems and OT systems. The security practices

given in this guide are categorised logically into three main groups, namely, policies, organisational practices, and technical practices.

Likewise, the Institution of Engineering and Technology, published *Code of Practice Cyber Security for Ships* in 2017, emphasizing the importance of enforcing appropriate security measures, considering the technological aspects in maritime systems [9]. The document recommends good practices on developing cybersecurity assessment plans, devising mitigation measures, and managing security breaches and incidents. Also, the *Guide for Cybersecurity Implementation for the Marine and Offshore Industries, ABS Cybersafety Volume 2,* published by the American Bureau of Shipping (ABS) in February 2021, provides cyber security requirements and recommendations for cyber-enabled systems. ABS provides four notations CS-System, CS-Ready, CS-1 and CS-2, upon compliance with the requirements given in this guide [10].

From the review of the guidelines published by various maritime organisations, it is visible that they focus on providing guidelines for maritime cyber risk management and their target audiences tend to be those at the management level. On the other hand, the guidelines in this document are framed in a way that they can be readily adopted by those responsible for the cybersecurity of shipboard OT systems such as engineers, IT/OT system specialists and vessel inspectors. These guidelines aim to address the cyber risks in shipboard operational technology (OT) systems and also provide actionable mitigation measures in the form of a checklist, which will serve as a guide for ship owners and maritime authorities to ensure cyber hygiene of their ships.

3 SHIPBOARD OT SYSTEMS

The number of cyber-attacks in the maritime industry has increased as hackers attempt to exploit vulnerabilities in shipboard OT systems. OT systems are those involved in various operations, including communication, propulsion, power management, navigation, and cargo management. As vessels connect to the Internet to enhance the efficiency of their operations and communications, OT systems become more vulnerable to cyber-attacks that interrupt ship operations. The OT systems considered in this study are Communication Systems, Propulsion, Machinery and Power Control Systems, Navigation Systems, Cargo Management Systems since their vulnerabilities pose a direct and significant threat to vessel operations and the safety of the crew and her cargo.

3.1 Communication Systems

Ship-to-ship communication and ship-to-shore communication are crucial for activities such as alerting, reporting and sending/receiving maritime safety information. Hence, equipping a secure and reliable communication medium for the ship is fundamental. The state-of-art communication technologies available at present have proven to be helpful to the seafarers and port authorities to stay connected, irrespective of their locations. Several functions/operations such as weather reporting, chart updates, email access, sending/receiving distress alerts, and position reporting are possible with the help of satellite communication systems. The sub-systems covered under communication systems include Satellite Communication System (SATCOM), Integrated Communication System (ICS), Voice Over Internet Protocol (VOIP) and Wireless Local Area Network (WLAN).

3.1.1 Satellite Communication System (SATCOM)

Vessels require a reliable connection to the Internet for essential operations and for the crew to stay in touch with their family while offshore. SATCOM technologies enable them to do that. The Satellite Internet is a wireless internet, where the signals are sent and received between the ground station and satellites revolving around the Earth [11]. A VSAT (Very Small Aperture Terminal) is a ground station used to transmit/receive data, voice, and video signals over a satellite communication network. A VSAT consists of two parts, such as the transceiver, which is placed outdoors, and a terminal device connected to the end user's computer, for data transmission [12]. All the connections are managed and configured through the VSAT web administration interface [13].

3.1.2 Integrated Communication System (ICS)

The ICS enables a centralised management of overall communications in a ship and ensures high operation efficiency and reliable communications. The key components include the VSAT modem, VOIP, WLAN access points, radio communication equipment and monitoring devices [14, 15]. Since a significant part of a ship's communication depends on VSAT, it can be the entry point for a wide

variety of attacks targeting other systems such as VOIP, access points and equipment monitoring systems in the ship.

3.1.3 Voice Over Internet Protocol (VOIP)

VOIP phones allow the crew to make and receive phone calls over the Internet. Navigating in isolated and remote areas calls for a communication lifeline that can provide 24/7 connectivity to the ports and offices, especially in harsh environmental conditions. A fast, reliable, cost-efficient, and secure communication system like VOIP phones helps to provide clear voyage-related instructions and safety information to the crew. Session Initiation Protocol is the protocol for controlling multimedia communications such as voice and video call sessions over Internet Protocol [16].

3.1.4 Wireless Local Area Network (WLAN)

A WLAN is a wireless network setup where multiple devices are connected to form a local area network. Routers can be connected to the VSAT modem and configured to use as Wi-Fi access points for connecting devices, creating a WLAN [17]. There can be several access points in the ship for various operational purposes and the crew's personal use, hence they must be secured. Apart from the vulnerabilities in an access point, if it is placed in a location where it can be physically accessed, they can be easily tampered with. Hence, it is vital to safeguard the access points [18].

3.2 Propulsion, Machinery & Power Control Systems

Performance parameters of various devices in a vessel's propulsion, machinery and power management need to be controlled and monitored for crucial vessel operations. The sub-systems considered under these systems include the Fuel Oil system, Engine Governor system, Alarm Monitoring and Control System, Power Management System, Emergency generator, and Batteries.

All the devices in the ship send and receive data to and from multiple devices and sensors simultaneously. OT systems use serial communication protocols like the NMEA (National Marine Electronics Association) network, a standard for serial data communications among shipboard systems. On the other hand, IT systems use Ethernet/IP networks for communication. In some cases, the OT systems in the serial communication network are connected to the IT network for services like system maintenance, system updates, equipment control and monitoring. And it is possible to control and monitor the parameters responsible for the operation of OT systems through a multi-function console or a PC, and this system may need to be connected to the Internet for operation purposes, remote updates, etc. Such interconnectivity between IT and OT systems acts as an attack surface for hackers to compromise shipboard systems.

It is important to note that serial communication protocols lack encryption and have no message authentication. This means attempts to enter OT systems cannot be easily defeated if an intruder can reach those systems through their network. Considering the poor security mechanisms in the VSAT

web administration interface, illicit access into the network through common means such as USB ports and phishing emails, become ready entry portholes in which an attacker can get into the vessel network [19]. Due to these vulnerabilities, a skilled and motivated attacker can easily find points to break into the serial network and tamper with the parameters that may cause malfunction to the OT systems.

3.2.1 Engine Governor System

Ship's engine is used for propelling a ship and power generation onboard. The engine system is used to control the mean speed of the engine under varying load states [20]. There are different types of engine systems, for example, in a dual-fuel engine, the two main controllers include the knock control unit and the dual fuel controller. The knock control unit is responsible for governing the fuel/air properties, while the dual fuel controller is responsible for controlling the engine speed. Serial communication network (e.g., NMEA/CAN network) is used as the mode of communication with the rest of the ship's machinery [21]. Some of the parameters that need to be considered in a ship's engine operations include quantity of fuel injected, pressure, combustion temperature, engine temperature and engine start/stop status [22].

3.2.2 Fuel Oil System

The fuel oil system is crucial for the ship's propulsion and power generation [23]. Marine engines convert the heat generated by burning the fuel oil into mechanical energy by combustion process. Fuel tank level, temperature and viscosity are some of the key parameters to be considered in a fuel oil system [22].

3.2.3 Alarm Monitoring and Control System

The alarm monitoring and control system helps to monitor and control all the alarms implemented on the ship through a multi-function console or a PC [24]. It connects the alarms associated with all the systems in the ship and emits visual or audio signals in the event of an emergency or system failure [21]. Since shipboard systems are susceptible to failures/malfunctions and various human factors, the alarm system plays a vital role in alerting the crew during system failures and emergencies.

3.2.4 Power Management System (PMS)

The power management system is responsible for providing an uninterrupted power supply to all the systems in the vessel. The PMS automates functions such as the start/stop of generators, voltage and frequency control and load control. Vessels are operated by various electronic devices, and cargo such as fuel containers and air-conditioned containers needs to be shipped by controlling certain properties such as temperature, pressure, etc. [21], hence disrupted power supply will affect vessel operations. The parameters to be considered in a PMS include generator status (start/stop), voltage, frequency, generator load, etc. [22]. All these parameters can be monitored and controlled through the power management system panel.

3.2.5 Emergency Generator and Batteries

An emergency generator provides backup power to crucial devices in the ship during main generator failure or a power outage. Both the batteries and the emergency generator can be used in case of an emergency. The generator can be controlled via power management system console, where voltage and frequency are monitored. During the loss of main power supply, when the electrical relay senses a low voltage or frequency, it will trigger the emergency generator to start automatically [25] [26] [27]. Vessels and cargo containers require a constant power supply throughout their voyage. Reefer containers that carry temperature-sensitive goods (such as drugs and perishable food) are especially vulnerable to disruptions in the power supply [21].

3.3 Navigation Systems

Vessels are equipped with many advanced navigation equipment systems that give accurate navigation data. Navigation systems can be entirely controlled by the system or situated elsewhere, with the vessel controlled via radio or other signals. Determining the correct position, speed and heading of the vessel is necessary to ensure that the vessel arrives at its destination safely and on schedule. Navigation systems include the following subsystems: electronic chart display and information system, radio detection and ranging, automatic identification system, global positioning system, dynamic positioning system, global maritime distress safety system, voyage data recorder, and integrated navigation system.

3.3.1 Electronic Chart Display and Information System (ECDIS)

Electronic Chart Display and Information System (ECDIS) is an electronic navigational chart system to identify locations and obtain directions for ship's voyage. ECDIS accurately pinpoints navigational locations with the help of the Global Positioning System (GPS). It also displays radar information, weather, ice conditions, speed, position and planned route of the ship [28].

ECDIS is a workstation PC installed in the ship's bridge, usually running on operating systems such as Windows or Linux. Interfaces connected to the ECDIS include the ship's radar, Automatic Identification System (AIS), position sensor, speed sensor and heading sensor. These interfaces frequently connect to the ship's Local Area Network (LAN) through NMEA (a combined electrical and data specification for communication between marine electronics), which in turn has a gateway to the Internet. Based on the specifications of the service provider and the onboard communication facilities, updates to the Electronic Navigational Charts (ENCs) are done through USB ports, data distribution media (e.g., DVD), email attachment (SATCOM) and internet download. All of these are possible attack surfaces that attackers can make use of, to gain unauthorised access to ECDIS [29].

3.3.2 Radio Detection and Ranging (RADAR)

RADAR system plays an important role in the safe navigation of a ship. It is a mandatory equipment for navigation, used in identifying, tracking, positioning of vessels, and to safely navigate a ship from one point to another. To avoid collisions, vessels rely on S-band and X-band frequency radar systems,

which can identify targets and display information on the screen, such as the ship's distance from land, floating objects, obstacles and other vessels in the vicinity. Interfaces connected to the RADAR include local ethernet switch and ethernet protocols, which may act as attack surfaces for attackers to gain access to the shipboard systems [30].

3.3.3 Automatic Identification System (AIS)

The AIS is primarily designed to allow ships to see and be seen by marine traffic in its vicinity. It aids in the identification of ships and navigational marks. AIS assists in obtaining specific information of the ships in a certain range, such as its name, speed, position, direction, rate of turn, destination, and physical parameters such as length, breadth, tonnage, beam, and draft, to neighboring ships and coastal authorities. AIS connects a standardised Very High Frequency (VHF) transceiver to a positioning system, such as a GPS receiver, as well as other electronic navigation sensors such as a gyrocompass or rate of turn indicator [31].

3.3.4 Global Positioning System (GPS)

The GPS is a crucial component that helps in determining accurate geographical locations for navigation. A GPS system comprises three systems: satellites, ground stations, and receivers. The GPS information is frequently replicated on other navigational equipment on the bridge, such as radars, automatic identification system, electronic navigation systems and communication systems, to aid in navigation. Differential GPS (DGPS), an improvement to the basic GPS signal, provides a much higher precision and enhanced safety in its coverage areas for maritime operations [32].

3.3.5 Dynamic Positioning System (DPS)

A Dynamic Positioning system is an automated computer-controlled system that maintains a vessel's position and heading by controlling its own propellers and thrusters. Position reference sensors, in addition to wind sensors, motion sensors, and gyro compasses, provide data to the computer about the vessel's position, the magnitude and direction of environmental forces impacting its position. The main functions of a DP system consist of the following:

- Estimating the vessel position and heading
- Determining the position and heading errors between setpoints and estimates
- Determining the corrective action to be applied
- Calculating the command to the thrusters [33]

3.3.6 Global Maritime Distress Safety System (GMDSS)

The Global Maritime Distress and Safety System (GMDSS) is a standard for usage of communication protocol, procedures and safety equipment which can be utilised at the time of distress situation by the ship. The GMDSS sends a distress signal via satellite or radio communication equipment. It is used as a medium for transmitting and receiving marine safety information, and also as a general

communication channel. INMARSAT, NAVTEX, Emergency Position Indicating Radio Beacon (EPIRB), Search and Rescue Locating Equipment, and Digital Selective Calling are the various components of GMDSS [34].

3.3.7 Voyage Data Recorder (VDR)

The Voyage Data Recorder (VDR) is an equipment which functions similar to an aircraft's "black box" and is responsible for collecting and preserving all the relevant information about a ship. This system records various data such as the ship's speed, direction, position, status of ship systems, information about the engine, fuel, etc., which will be helpful during an accident investigation to examine what had happened to the ship and crew. Additionally, VDR includes a voice recording system that can save up to last 12 hours of information [21].

3.3.8 Integrated Navigation System (INS)

Integrated Navigation System (INS) intensifies the operational efficiency and safety of ship's navigation by equipping a multifunctional display based on integration of at least two navigational functions. It is a software platform which includes data from the ECDIS and RADAR systems, with sensors for other navigation functions. The possible attack surfaces in INS are Server Message Block (SMB) service and remote desktop protocol [35].

3.4 Cargo Management Systems

Cargo management system assists in reliable control and tracking of cargo. The operations can be automated depending on the type of ship and cargo. The status of cargo and its related data is frequently available and managed over the internet, increasing the chances for cyberattacks. The subsystems covered in cargo management systems are cargo control room and ballast water system.

3.4.1 Cargo Control Room (CCR)

A cargo control room (CCR) is a place where the loading and unloading of cargo is controlled and monitored by a person in charge (PIC). The design and layout of a cargo control room can be determined based on the design of a ship, the requirements of owners and the capabilities of a particular shipyard. The CCR can be a separate room, or the controls can be placed on the ship's bridge. The PIC can control the loading/unloading of cargo, stripping pumps, check the valve positions and liquid levels in the cargo containers, through the equipment present in the CCR [36].

3.4.2 Ballast Water System (BWS)

A Ballast Water System (BWS) is a separate compartment within a ship that stores water as ballast to offer stability to the ship. The use of water in such a tank will help in adjusting the weight of the ship in abnormal conditions. The system's operation also involves pumping out the ballast water for temporary reduction of the draft of the vessel when it enters shallow waters [37] [21]. The ballast water

management system (BWMS) is another type of computer-controlled system to manage the treatment of ballast water in order to remove marine organisms and solid materials.

4 CYBER RISKS IN SHIPBOARD OT SYSTEMS

Vessels are highly dependent on digital technologies for integration of systems and automation of operations. While utilising new technologies for ship operations provides significant gain for the maritime industry in terms of efficiency, risks may still persist due to lack of security controls, poor system design and maintenance. Attacker can easily exploit the vulnerabilities in devices linked with the Internet such as the SATCOM for penetrating the vessel network. If OT systems are connected to Internet for operational and remote service purposes, then such interconnectivity will help attacker to penetrate OT network also, however this way of intrusion requires abundant skills. This section discusses the cyber risks associated with each of the OT sub-systems presented in Section 3. Appendix 1 provides a more detailed description of the cyber risks in shipboard OT systems.

4.1 Cyber Risks in Communication Systems

Satellite Communication System (SATCOM) & Integrated Communication System (ICS)

- **Phishing emails:** Authorised crew personnel use the computer in the ship's bridge to access emails for various purposes including, chart updates, software updates and receiving maritime information from their main office. Phishing emails target to deliver malware such as spyware, ransomware, viruses by tricking the victim to click on links or download infected files. This attack could result in data breaches and the unavailability of systems. Phishing emails are one of the common ways through which attackers can get into the ship's network [38].
- **Outdated VSAT software:** Often, the VSAT software is not updated or updated way after an update patch has been released. The vulnerabilities in the older versions of the software are often published in public resources, which cyber attackers can use to exploit and disrupt the vessel's operations that depend on SATCOM, as well as disrupt the communication between ship-shore [13].
- **Eavesdropping:** Usage of weak protocols like HTTP and Telnet in the VSAT web administration interface can allow the attacker to eavesdrop in the vessel network using packet sniffing tools and sniff credentials and sensitive information. It is also possible for the attacker to insert unintended data in the web interface or hijack the entire management session [13] [39].
- **Cross-site scripting attack:** Scripting attacks can also occur on a poorly built VSAT web administration interface. Attackers can find out about the vulnerabilities in various VSAT versions from resources published online. Faulty input sanitisation configurations can allow hackers to inject arbitrary client-side code. Due to this vulnerability, an attacker can impersonate a legitimate user and send malicious links, modify credentials, capture cookies and hijack the session [13] [39].
- **Unauthorised access of vessel network:** Usage of weak or default username and password credentials in the VSAT web administration interface can lead to unauthorised access of vessel network, through which an attacker can gain privileges such as administrative access, FTP access, and command-line access. With such privileges, an attacker can view/edit confidential files and

compromise other shipboard systems in the network. Most often, default passwords are not changed, or the passwords set are very weak, e.g., common passwords like 1234, abcd, which are easily cracked using brute force or dictionary attacks [13] [40].

Voice Over Internet Protocol (VOIP) [41]

- **Denial of Service (DoS) attack:** Hackers can launch a DoS attack by flooding the VoIP network server with SIP call-signalling messages, which will exhaust the maximum bandwidth available and disrupt the VOIP call traffic. This attack results in network unavailability, which in turn causes a lack of communication inside the ship and between the ship-shore. It is a serious threat to the crew and ship operations especially if the network is unavailable during an event of an emergency.
- **Eavesdropping:** Using an unencrypted network or a poorly encrypted network for VOIP calls might result in eavesdropping, causing a breach of confidentiality and privacy. Hackers will be able to gain personal and confidential information by unauthorised interception of an unencrypted VOIP traffic using packet sniffing tools like Wireshark.
- **Vishing:** Vishing (Voice-based Phishing) is an attack where an attacker pretends to be a legitimate source and tricks the victim into providing sensitive information. This attack is usually carried out by spoofing the caller ID, for which a lot of tools are available online. The motive of a vishing attack would be to manipulate the victim to gain sensitive information such as vessel location, cargo details, crew details etc.

Wireless Local Area Network (WLAN) [18]

- **Denial of Service (DoS) attack:** Hackers can launch a DoS attack by overwhelming the access point/router with fake connection requests, causing the network to slow down or halt, resulting in the unavailability of the internet and resources. These fake requests attempt to exhaust an access point's bandwidth capacity and prevent a legitimate request from reaching the target. DoS attack causes network unavailability and lack of communication between ship-shore, which is a serious threat to the crew and the vessel.
- **Access point tampering:** As vessels have large operating areas, several access points need to be placed in different locations for fast and stable access to the Internet. But if the access point is placed in a location where it can be physically accessed, tampering can occur as it just takes few seconds to revert the access point to factory default settings.
- **Eavesdropping/Session hijacking:** Encrypting the vessel network is crucial, as the lack of a secure encryption standard can allow hackers to intercept the vessel network. By using packet sniffing tools, hackers can eavesdrop in the vessel network and steal login credentials and other sensitive information. This can also lead to session hijacking, which is the exploitation of a valid computer session to gain unauthorised access to information or services in a computer system. Since the vessel

network is utilised for vessel operations and the crew's personal use, it is vital to encrypt the network using a secure encryption standard.

4.2 Cyber Risks in Propulsion, Machinery & Power Control Systems

Engine Governor System

- **Man-in-the-middle (MITM) attack:** An attacker can launch a MITM attack by gaining access to the vessel network and then tampering with the serial communication between the engine controllers and other devices, disrupting the engine's performance. Some of the parameters that could be tampered with include fuel injection quantity, pressure, combustion temperature, engine temperature, and engine start/stop status [21].
- **Malware attack:** As the engine parameters are monitored and controlled from a PC or a multi-function console, malware could be injected via USB ports in that system, which might cause the engine to malfunction, resulting in an explosion or physical damage affecting the crew, the ship, and the systems onboard [19].

Fuel Oil System

- **Man-in-the-middle (MITM) attack:** This attack occurs when an attacker breaks into the vessel network and manipulates the serial data relayed between the engine and fuel monitoring system and other devices in the serial network. Parameters such as fuel level, temperature, and viscosity, need to be monitored for safe operations. For example, the fuel level indicator in the fuel monitoring system can be tampered with to show the wrong fuel level, which might result in issues such as overloading the fuel storage tank or delay in reaching the destination [21].
- **Malware attack:** When malware is injected into the fuel monitoring system (via USB port), malicious code or commands might get executed in the system. Because of this, the fuel parameter configurations could get altered, which in turn malfunction the system, resulting in an explosion or physical damage affecting the crew and the ship [19].

Alarm Monitoring & Control System

- **Man-in-the-middle (MITM) attack:** Since all the alarms in the ship are monitored in the alarm monitoring and control panel, an attacker can launch a MITM attack by entering the ship network and modify alarm-related commands relayed between the systems onboard. An attacker may either suppress an alarm or raise fake alarms, and due to this, the crew may be unaware of a potential system failure or an emergency, putting lives and cargo at risk [21].
- **Malware attack:** Malware intrusion via USB ports in the alarm monitoring and control system might cause it to misfunction, threatening the safe voyage of the ship and crew [19].

Power Management System (PMS)

- **Man-in-the-middle (MITM) attack:** This attack can happen if a hacker breaks into the ship's network and manages to tamper with the serial data going in and out of the power management system. Misleading voltage and frequency values might result in a disrupted power supply to all the systems in the vessel and the cargo containers, impacting the vessel operations and the cargo [21].
- **Malware attack:** Malware intrusion via USB ports in the power management system might mislead its operations, resulting in a disrupted power supply to the ship. Due to this, vessel operations will be interrupted, and goods inside the cargo containers (e.g., Reefer container) may get damaged [19].

Emergency Generator and Batteries

Man-in-the-middle (MITM) attack and **malware attack** on the power management system are the two main cyber risks that affect an emergency generator. Cyberattacks that cause the power management system to fail may trouble the automatic start of the emergency generator as the generator controls are present in the power management system [21]. If an attacker compromises the power management system, the emergency generator may fail to kick in when there is a power outage or low voltage, hence affecting vessel operations and its cargo. For example, reefer containers carry temperature-sensitive goods that require constant electricity throughout the voyage.

4.3 Cyber Risks in Navigation Systems

Electronic Chart Display and Information System (ECDIS) [21]

- **Malware attack:** Malware can enter the ECDIS system when a crew member intentionally or unintentionally inserts a malware-infected USB drive into the USB port in the system, hence disrupting the operations of ECDIS.
- **Denial-of-Service (DoS) attack:** A DoS attack occurs when an attacker overloads the network with traffic, which takes the ECDIS offline and leaves the vessel without a means of safe navigation. Attacker may also steal ENCs (Electronic Navigation Charts) through unauthorised access to shipboard network via Internet.
- **Spoofing:** Due to lack of encryption and authentication, it is possible to spoof the incoming plain text messages from the NMEA network to the ECIDS, for example, tampering with the chart information in may result in ship collision.

Radio Detection and Ranging (RADAR)

- **Malware intrusion:** A possible way for malware intrusion into the RADAR system is when the captain opens a virus-laden email containing chart for updating. As the radar is connected to ECDIS over Ethernet protocols, when the chart is updated in ECDIS, the virus transfers and installs itself in ECDIS and makes its way to the radar through the local ethernet switch. This attack alters the radar display by deleting the targets displayed on the screen, essentially blinding the ship [42].

- **Man-in-the-middle (MITM) attack:** On the SMB (Server Message Block) service running in Radar, signing and security signatures are not required. An attacker can use these vulnerabilities in the SMB service to launch an MITM attack and execute code without authentication [43].

Automatic Identification System (AIS)

- **Spoofing:** If the AIS software does not have built-in security or authentication, a spoofing attack can be done by initiating a fake terrestrial tower that broadcasts AIS data. For example, broadcasting details of a non-existent ship on a collision course may result in a CPA alert, which might force the vessel to divert from its path and actually collide with an obstruction or run aground [44].
- **Replay attack:** An attacker may launch a replay attack by executing spoofed commands to delay the transmission time and resend it over and over, resulting in a DoS attack. This can result in disabling the AIS display.
- **Frequency hopping attack:** Port authorities provide specific instructions to the ship's AIS transponder to operate on a certain frequency. An attacker might be able to spoof such command to alter the frequency. Because of this frequency hopping attack, the ship will be unable to transmit or receive communications on the frequency, hence the vessel's details may not be visible on other ship's AIS display [45].

Global Positioning System (GPS)

- **GPS Spoofing:** An attacker can initiate a GPS spoofing attack by sending out fake GPS signals that are disguised as real signals. This will mislead the receiver into believing that its location is accurate, while in real, it is incorrect, as spoofed by the attacker. This attack may mislead ships to navigate wrongly and may also result in ship-to-ship and ship-to-land collisions [46].
- **GPS Jamming:** Attacker can cause interference on signals from Global Navigation Satellite System (GNSS). The jamming signal will be significantly greater than the GPS signal hence preventing GPS reception. This will cause GPS to display erroneous positions and present misleading information in AIS and ECDIS [47].

Dynamic Positioning System (DPS) [33]

- **Denial-of-Service (DoS) attack:** An attacker can cause a network storm on the Global Navigation Satellite System (GNSS) receiver and launch a DoS attack. This will cause unavailability of DP system as it receives signals (position information) from GNSS receiver. This may happen when the DP system's software is poor or unpatched.
- **Spoofing:** Spoofing involves transmitting the false signals to GNSS receiver, similar to GPS spoofing, resulting in displaying wrong position information in the DPS display. This will cause the ship to change its heading because of the misleading information in the DPS display.

- **Backdoor attack:** Attacker can perform a backdoor attack to gain unauthorised access to the DP system by installing malware that can surpass normal authentication to access the system. This will result in attacker taking control over the system and misleading the operations.

Global Maritime Distress Safety System (GMDSS)

- **Spoofing:** Due to the broadcast nature of VHF, GMDSS is vulnerable to cyber-attacks. Attacker can spoof the distress commands and deliver false information, hence causing confusion and delay in distress operations.
- **Eavesdropping:** It may be possible for an attacker to intercept distress messages by eavesdropping on the signals, thus resulting in loss of confidentiality [48].
- **Denial-of-Service (DoS) attack:** If a malware infected application is present in the system and it is run, then it may initiate a DoS attack, hence disrupting the communication between the ships and ship-shore. Issues with transmitting and receiving messages may lead to loss of lives during a distress situation [49].

Voyage Data Recorder (VDR) [21]

- **Malware attack:** With the presence of USB port in the voyage data recording unit, malware can be injected through an infected USB drive, through which attacker may gain access to the data stored in VDR and tamper with, steal, or destroy it.
- **Remote code execution:** Due to the vulnerabilities in the services running on VDR, attackers can execute code with administrative (root) privileges, thus consequently have unlimited access within the operating system. Such privileges may also allow an intruder to tamper with speed, position, heading readings and delete conversations from the bridge, delete radar images, etc.

Integrated Navigation System (INS) [35]

- **Man-in-the-middle (MITM) attack:** Due to the low encryption level used in remote desktop protocol server (terminal service) running in the INS, an attacker can carry out an MITM attack and gain unauthorised access to the system.
- **Remote code execution:** If older versions of SMB service (probably version 1.0) is run in INS, it may be subject to remote code execution. A remote attacker can exploit this vulnerability by executing malicious code without authentication, which allows for access to the system, where attacker can execute commands with root privileges and also tamper with sensitive information.

4.4 Cyber Risks in Cargo Management Systems

Cargo Control Room (CCR) [50]

- **Ransomware:** Usually cargo is controlled and monitored via a computer system connected to the vessel network, hence phishing emails crafted with malware such as ransomware may be sent to the person in charge of cargo control room. If a malicious link is accessed or a malicious file is

downloaded and installed, then ransomware will spread and infect the cargo monitoring system and other devices in the vessel network. Hence all the devices will be encrypted and cannot be accessed unless a ransom is paid. This will in turn cause economic loss and disrupt ship operations and cargo.

- **Malware attack:** Malware can be infused in the cargo monitoring system intentionally or unintentionally by plugging an infected USB device into the USB port. Hence, attacker can access the system and steal or tamper with cargo related information such as rates, cargo tracking number, place and date of delivery, etc. For example, attacker can tamper with the place of delivery to a wrong destination.

Ballast Water System (BWS)

- **Malware attack:** The monitoring and controlling of ballast water system can be done from the ship's bridge systems or engine control room system. If malware is injected through USB ports in those systems, attacker may send false commands regarding the increase or decrease of the water level in the ballast compartment, hence causing the vessel to lose its stability and sink [37].
- **Phishing emails:** Email attachments infected with malware may be sent to the system through which ballast water compartment is monitored. If that system is infected with malware, then attacker may compromise the system and tamper with the functioning of the sensors, actuators, etc., and damage the tubes and other parts of the ballast water system [21]. This will also cause the vessel to sink due to instability.

STRIDE: Example

From the analysis of attack surfaces and cyber risks in shipboard OT systems, it is visible that all the attributes of STRIDE (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of privilege) threat model are covered [51]. Few examples are as follows:

***S**poofing:* An adversary could spoof signals from GPS receiver to deliver misleading information for ship's navigation, due to lack of authentication mechanisms in GPS.

***T**ampering:* Due to the lack of encryption and authentication in serial communication protocols attacker may tamper with the communication relayed between the devices, resulting in loss of data integrity and control of the system.

***R**epudiation:* AIS messages are not authenticated, hence an adversary may spoof AIS messages to cause ship collision. Eventually if the system does not have logs to trace the perpetrator, then there is chance for repudiation.

***I**nformation Disclosure:* Lack of encryption in the vessel's Internet connection may lead to Information Disclosure. By using packet sniffing tools, hackers can eavesdrop in the vessel network and steal login credentials and other sensitive information.

D*enial of Service:* The attacker can conduct a Denial of Service (DoS) attack on the router by overwhelming the router with connection requests, causing the network to slow down or stop. This will prevent legitimate connections from accessing the resources, resulting in unavailability.

E*levation of Privilege:* Elevation of Privilege can occur when weak/default username and password credentials is used to login to VSAT web administration interface. Attacker can make use of such weaknesses and gain unauthorised administrative access to vessel network. With such privilege, an attacker would be able to read and modify confidential files and also compromise other shipboard systems in the network.

5 MITIGATION MEASURES

The mitigation measures provided in this section are specific to the cyber risks identified in the four major shipboard OT systems, namely, Communication Systems, Propulsion, Machinery and Power Control Systems, Navigation Systems, Cargo Management Systems. These mitigation measures cover three categories of measures, namely, technical, procedural and physical security measures. Few of the many measures include technical security measures such as firewalls and Virtual Private Networks (VPN), OT and IT traffic segregation, and anti-malware installation, physical security measures including access control lists and safeguarding sensitive devices, and procedural measures involving operating system and software updates, password reset mechanisms, crew awareness and training. Hence these security controls are recommended for the ship owners to enforce onboard their ships to protect from major cyber threats. Appendix 2 provides a more detailed description of the mitigation measures for managing the cyber risks in shipboard OT systems.

5.1 Mitigation Measures for Communication Systems

Table 2 Mitigation measures for Communication Systems

Satellite Communication System (SATCOM) and Integrated Communication System (ICS)	
Cyber Risks	***Mitigation Measures*** [4, 13, 52, 53]
Phishing emails (Malware attack)	• Antivirus software must be installed in the business computers. • Files and email attachments downloaded from emails must be scanned with antivirus software to check for virus/malware. • Regular data backup must be done and stored safely. • Crew awareness must be established on the following: - Ability to distinguish phishing emails from the real ones - Be aware that emails from unknown sources should be viewed carefully and suspicious email attachments should not be opened, especially not to enable macro function in Microsoft documents. - Be aware that they must not click on suspicious links • Email security should be implemented – For example, S/MIME (Secure Multipurpose Internet *Mail* Extension) can be implemented to encrypt the email and ensure authenticity and integrity of the email [54].
Outdated VSAT software	• Latest version of software must be installed in the VSAT terminals. • Software updates must be checked regularly to fix vulnerabilities. • All updates must be logged. • If remote service/maintenance or an update is made, the authenticity of the vendor service, update and the remote desktop connection should be verified manually (e.g., phone call) before access can be permitted for the specified requirement.
Eavesdropping	The terminal (VSAT) administration web interface should support secure protocols such as HTTPS, SSHv2.

Cross-site scripting	The VSAT web interface should have inbuilt security mechanisms such as input sanitisation (any suspicious inputs must be rejected), output encoding, CSP (Content Security Policy) to protect against scripting attacks [55].
Unauthorised access of vessel network: Administrative access, FTP access and Command-line access	• Firewall must be configured to allow only whitelisted sources or IP addresses within a subnet. • Virtual Private Network must be used while accessing the Internet. • IP address should be private, and it should not be available on any public domain (e.g., Shodan). • OS, antivirus, firewall and other applications used in the business computer (The computer used for accessing emails, and VSAT modem's web interface) must be updated/patched regularly. • Access to the business computer should be restricted to authorised personnel with administrative login and strong credentials. • The default username and password in VSAT modem must be changed. Password should be strong - for example, password with 8 characters and at least one uppercase letter and one special character is recommended. • Password reset mechanisms should be implemented; it is recommended to change password once in three months. • Do not write down passwords in notebooks or sticky notes; a secure password manager application or a password protected PDF/Word document can be used to store passwords. • Access to the business computer must be blocked after a number of failed login attempts, e.g., 5 tries • It is good to have multi-factor authentication (MFA) for accessing the business computer and VSAT web interface. • FTP must be disabled in the VSAT modem's web interface.
Voice Over Internet Protocol (VOIP)	
Cyber Risks	***Mitigation Measures*** [41, 56]
Denial of Service (DoS) attack	• Separate data traffic and voice traffic- Use a VLAN (Virtual Local Area Network)/Firewall dedicated for VOIP traffic. • The IT team must frequently monitor the VOIP network using Intrusion Detection Systems.
Eavesdropping	The VOIP traffic must be encrypted with a secure encryption standard.
Vishing	The crew must know that they should not provide any personal details or vessel information if they receive calls from unknown sources.
Wireless Local Area Network (WLAN)	
Cyber Risks	***Mitigation Measures*** [18, 57]
Denial of Service (DoS) attack	• Firewall must be configured to allow connection for whitelisted sources only. • The IT team must frequently monitor the network using Intrusion Detection Systems.
Access point tampering	Routers/access points must be kept in a secured location such as a locked closet.
Eavesdropping/Session hijacking	A secure encryption standard must be used in wireless networks. As a minimum level of security, WEP (Wired Equivalent Privacy) must be used. Stronger encryption standards like WiFi Protected Access3 is recommended.

5.2 Mitigation Measures for Propulsion, Machinery and Power Control Systems

Table 3 Mitigation measures for Propulsion, Machinery and Power Control Systems

Fuel Oil System, Engine Governor System, Alarm Monitoring & Control System, Power Management System, Emergency Generators and Batteries	
Cyber Risks	***Mitigation Measures***
Man-in-the-middle (MITM) attack	• SATCOM must be secured, as in Section 5.1. • Phishing email threat must be mitigated, as in Section 5.1. • OS, antivirus, and other applications in the engine and fuel monitoring system, alarm monitoring & control system and power management system must be updated frequently. • Crew access to the critical systems, and computers that control and monitor machinery must be regulated. • If remote service/maintenance is done on any of the systems, the authenticity of the vendor service and the remote desktop connection must be verified manually (e.g., phone call) and then access can be permitted. • OT network must be separated from the IT network by a Firewall/DMZ [4, 53]. • If a Serial-to-IP converter is used, it must support encryption, software updates must be done regularly, and credentials must be strong [58].
Malware attack (via USB ports)	• Antivirus software must be installed in the machinery control and monitoring systems. • Physical security measures must be implemented as follows: - Access control list for the crew to enter the engine control room or any other place where crucial machinery is present. - Access control list must be reviewed and updated regularly. • USB ports in the engine and fuel monitoring system, alarm monitoring and control system and power management system must be enabled only in admin login and disabled in other user logins (if any) and the system login credentials should have strong username and password. • USB port blockers can be used to block unused ports. • Dedicated charging points (ports) must be assigned for the crew. • USB cleaning station should be setup – A separate PC with antivirus software to scan the USB drives before use [4, 53].

5.3 Mitigation Measures for Navigation Systems

Table 4 Mitigation measures for Navigation Systems

Electronic Chart Display and Information System (ECDIS)	
Cyber Risks	***Mitigation Measures***
Malware attack (via USB ports)	• Antivirus software must be installed in the ECDIS system to scan any external media before connecting it to the system. • ECDIS chart updates must be logged.

	• USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use USB port blockers to avoid unnecessary plugins.
Denial-of-Service (DoS) attack	• Installing firewall in the ECDIS system will restrict unauthorised IP addresses from entering the vessel network [59]. • Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems.
Spoofing	• Encryption across the NMEA network ensures that data is encrypted before transit and authenticated upon receipt. A secure Serial-to-IP converter that supports encryption & authentication can be used. • As Serial-to-IP converters have web interface for configuration, default username and password must be changed. • The converter device's software must be kept updated.
Radio Detection and Ranging (RADAR)	
Cyber Risks	***Mitigation Measures***
Malware intrusion	• Antivirus software must be installed on captain's computer, which is used for downloading ECDIS chart updates. This will refrain malware from spreading to the RADAR via ethernet switch connected to ECDIS. • Train crew to identify phishing emails.
Man-in-the-middle (MITM) attack	• By enforcing the signing (security signatures) to the underlying operating system of SMB service, MITM attack can be mitigated. SMB signing places a digital signature into each server message block, which is used by both SMB clients and servers to prevent "man-in-the-middle" attacks and guarantee that SMB communications are not altered [60]. • SMB signing available in Microsoft Windows Server 2003, Microsoft Windows XP, Microsoft Windows 2000, Windows NT 4.0, and Windows 98 [61].
Automatic Identification System (AIS)	
Cyber Risks	***Mitigation Measures***
Spoofing	• AIS messages needs to be authenticated. • To distinguish between real and spoofed signals, there needs to be a way to directly determine the location of the transmission. For example, using a RFeye desktop application, transmissions can be geolocated by Time Difference on Arrival (TDoA). • The RFeye software outputs geolocation results as PoA (Power on Arrival) and TDOA probability heat maps and overlays real-time AoA (Angle of Arrival) vectors onto map interfaces [62].
Replay attack (Denial-of-Service)	• Timestamps must be monitored on all AIS messages to prevent hackers from resending recorded messages after a certain length of time, thus reducing the chances for attacker to eavesdrop the message and resend it [63].
Frequency hopping attack	• Integrity and authenticity of AIS messages should be assured. • PKI schema can be adopted in AIS protocol for RF communications. • X.509, a well-known PKI standard where digital certificates are issued by official national maritime authorities, that act as certification authorities

	and also configured in transponders with other stations identifiers (MMSI and call sign). X.509 authenticates messages exchanged between ships and with port authorities [64].
Global Positioning System (GPS)	
Cyber Risks	***Mitigation Measures***
GPS Spoofing	• GPS/GNSS receiver should detect spoofed signal from mix of authentic and spoofed signals by using anti-spoofing techniques like absolute power monitoring, spatial processing [65].
GPS Jamming	Usage of anti-jamming technique like spectrum monitoring enables GPS jammers to be detected and located by mobile direction-finding systems. Unintentional jamming can then be warned, and malicious attackers can be prosecuted [66].
Dynamic Positioning System (DPS)	
Cyber Risks	***Mitigation Measures***
Denial-of-Service (DoS) attack	• Allowing and denying specific IPs: Allowing only legitimate IP addresses or blocking ones from known attackers. Installing firewall in the DPS system will allow only known IP addresses [59]. • Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems. • The DP control system software must be updated.
Spoofing	• GPS/GNSS receiver should detect spoofed signal from mix of authentic and spoofed signals by anti-spoofing techniques such as absolute power monitoring, spatial processing [65].
Backdoor attack	An advanced antivirus can detect and prevent malware and malicious attacks. Many backdoors are installed through malware, so it is essential to install an antivirus tool capable of detecting such threats [67].
Global Maritime Distress and Safety System (GMDSS)	
Cyber Risks	***Mitigation Measures***
Spoofing	• Messages exchanged between ships and with port authorities must be authenticated. • PKI schema can be adopted in GMDSS to ensure authenticity of messages exchanged. • Implementing email security such as S/MIME or DKIM can also be helpful if confidential information is passed via email [68].
Eavesdropping	The software and tools used in GMDSS system must be updated to avoid providing attackers with chances of exploiting vulnerabilities and downloading malware into the system through which they can eavesdrop.
Denial-of-Service (DoS) attack	Use of firewall in GMDSS system will prevent DoS attack by allowing only known IP addresses [59].
Voyage Data Recorder (VDR)	
Cyber Risks	***Mitigation Measures***
Malware attack (via USB ports)	• Before inserting any external media into the VDR system, scan the media for virus/malware using antivirus software. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins.

	• Use port blockers to avoid unnecessary plugins. • Regular data backup (data recorded in the VDR) must be done and stored safely.
Remote code execution	Most of the vessels uses older version of VDR (Furuno VR-3000 and VR-5000). Updated versions can help prevent remote code execution [69].
Integrated Navigation System (INS)	
Cyber Risks	***Mitigation Measures***
Man-in-the-middle (MITM) attack	Remote desktop protocol server (terminal service) running in the underlying operating system (Windows) of INS is vulnerable to a man-in-the-middle attack due to low encryption level used. The vulnerability can be exploited by a remote attacker to gain access to the INS. This MITM attack can be prevented by enforcing strong cryptography [70].
Remote code execution	• Update the operating system with a security patch released by the manufacturer to prevent this attack. • **SMB 3.1.1** - the latest version of Windows SMB - was released along with server 2016 and Windows 10. **SMB 3.1.1** includes security enhancements such as enforcing secure connections with newer (SMB2 and later) clients and stronger encryption protocols [70].

5.4 Mitigation Measures for Cargo Management Systems

Table 5 Mitigation measures for Cargo Management Systems

Cargo Control Room (CCR)	
Cyber Risks	***Mitigation Measures***
Ransomware (via phishing emails)	• Antivirus software must be installed in cargo control computer system to protect the system from virus laden emails. • Regular data backup must be done and stored safely. • Train crew to identify phishing emails. • Crew should not click on links from unknown sources or reveal personal or sensitive operational details in emails.
Malware attack (via USB ports)	• Antivirus software must be installed in the computer system to scan any USB drives connects to the system. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use port blockers to avoid unnecessary plugins.
Ballast Water System (BWS)	
Cyber Risks	***Mitigation Measures***
Malware attack (via USB ports)	• It is critical that any external media is scanned for malware on a standalone system before being plugged into any shipboard network. Antivirus software helps in scanning any external media for malware before being plugged into the system.

	• USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use port blockers to avoid unnecessary plugins.
Phishing emails	• Antivirus software must be installed in the system to protect the system from phishing emails. • Regular data backup must be done and stored safely. • Train crew to identify phishing emails. • Crew should not click on links from unknown sources or reveal personal or sensitive operational details in emails.

6 CYBER RISK ASSESSMENT

Cyber risk assessment is an important part of cyber risk management. After identifying the threats, vulnerabilities and impacts of cyber risks in shipboard systems, the next step is to assess the likelihood and the severity of these risks with a cyber risk assessment approach. With frequent software updates and maintenance services, the operating condition of a system also changes correspondingly. Regular risk assessments help ship owners to understand and uncover existing and unknown vulnerabilities in a system, thereby ensuring a better understanding of the impacts of the risks, which also motivates them to enforce appropriate security measures in place.

The risk assessment approach used in this document involves calculating the risk score for each of the OT sub-systems using 4-by-4 risk score matrix, by determining:

- Likelihood: The possibility that a cyber incident will occur
- Severity: The impact caused by the occurrence of the cyber incident

6.1 Determining the Likelihood

The likelihood of occurrence of a cyber incident should be measured in terms of threats and vulnerabilities. The likelihood score/label will be determined by factors such as the technical capabilities and resources required for an attacker to exploit a particular vulnerability, human factors, and the complexity of an attack. Table 6 depicts the definition and label for assigning likelihood scores of 1 to 4.

Table 6 Definition of likelihood of a cyber incident

Score	Label	Likelihood Definition
4	**High**	- Attack can be performed remotely or with physical access to open ports and systems in the vessel. - Can be performed with very minimal or no technical knowledge and with publicly available resources (e.g., Shodan, ExploitDB). - Can be attacked from external network.
3	**Medium High**	- Attack can be performed with basic technical knowledge. - Can be performed with no change in exploits published online. - Possible if the attacker is in either an internal or external network.
2	**Medium Low**	- Attack can be performed with moderate technical knowledge. - Can be performed with minor changes in exploits published online. - Possible if the attacker is in either an internal or external network.
1	**Low**	- Attack can be performed with advanced technical knowledge. - Requires chaining of multiple exploits. - Requires physical/remote access to the OT system where there is restricted access.

6.2 Determining the Severity

The severity scores are determined based on the impact of a cyber-attack, i.e., the level of confidentiality, integrity, and availability breach, the extent of environmental damage and economic loss incurred to the company. Table 7 depicts the four-step scale is used to measure the severity of the impacts arising from a cyber-attack.

Table 7 Definition of severity of the impacts arising from a cyber attack

Score	Label	Severity Definition
4	**Critical**	Consequences of a cyberattack on the vessel operations, crew, and the enterprise, such as: - All operation systems, data, and resources unavailable, impacting safe operations. - Impact on the lives of crew members e.g., collision, explosion, sinking of ship, imbalance of ship, loss of life. - Economic loss to the enterprise.
3	**Severe**	Cyberattacks that lead to: - Unauthorised access of the vessel network, system, data, and other resources that affect day-to-day vessel operations such as navigation, communication, propulsion, generators, cargo. - Disruption of vessel network. - Disruption of ship-to-shore communication link.
2	**Moderate**	Cyberattack prevents or impairs the normal authorised functionality of networks, systems, or applications by exhausting resources. - Lack of availability of systems, data. - Misleading communication between OT systems, causing damage to the ship, cargo and disrupting its operations.
1	**Light**	Suspected or potential unauthorised access to the vessel systems which leads to data breach (sensitive/non-sensitive information).

6.3 Risk Evaluation

The risks are determined by the likelihood of exploiting a given cyber incident and the impacts arising from it. A risk matrix is used to depict this diagrammatically. Figure 2 shows a 4-by-4 risk score matrix for determining risk level for each cyber risk, where the risk score is derived by multiplying the "Likelihood" and "Severity" scores. Each of the cyber risks in the OT sub-systems (discussed in Section 3) are taken into consideration, and the impact and likelihood are assessed based on Tables 6 and 7 respectively. The risk scores are then assigned to the risks in each OT sub-system.

Table 8 shows the risk score classification within the risk score matrix. In the risk score matrix shown in Figure 2, the red boxes indicate the systems that are of high risk with their risk scores ranging between 12 and 16, and the yellow boxes depict the systems that are of medium risk with risk scores between 3 and 9, whereas the green boxes display the systems that are of lower risk with the risk scores 1 and 2.

Table 8 Risk score classification

Risk Level	Risk Score
High (Red)	12-16
Medium (Yellow)	3-9
Low (Green)	1-2

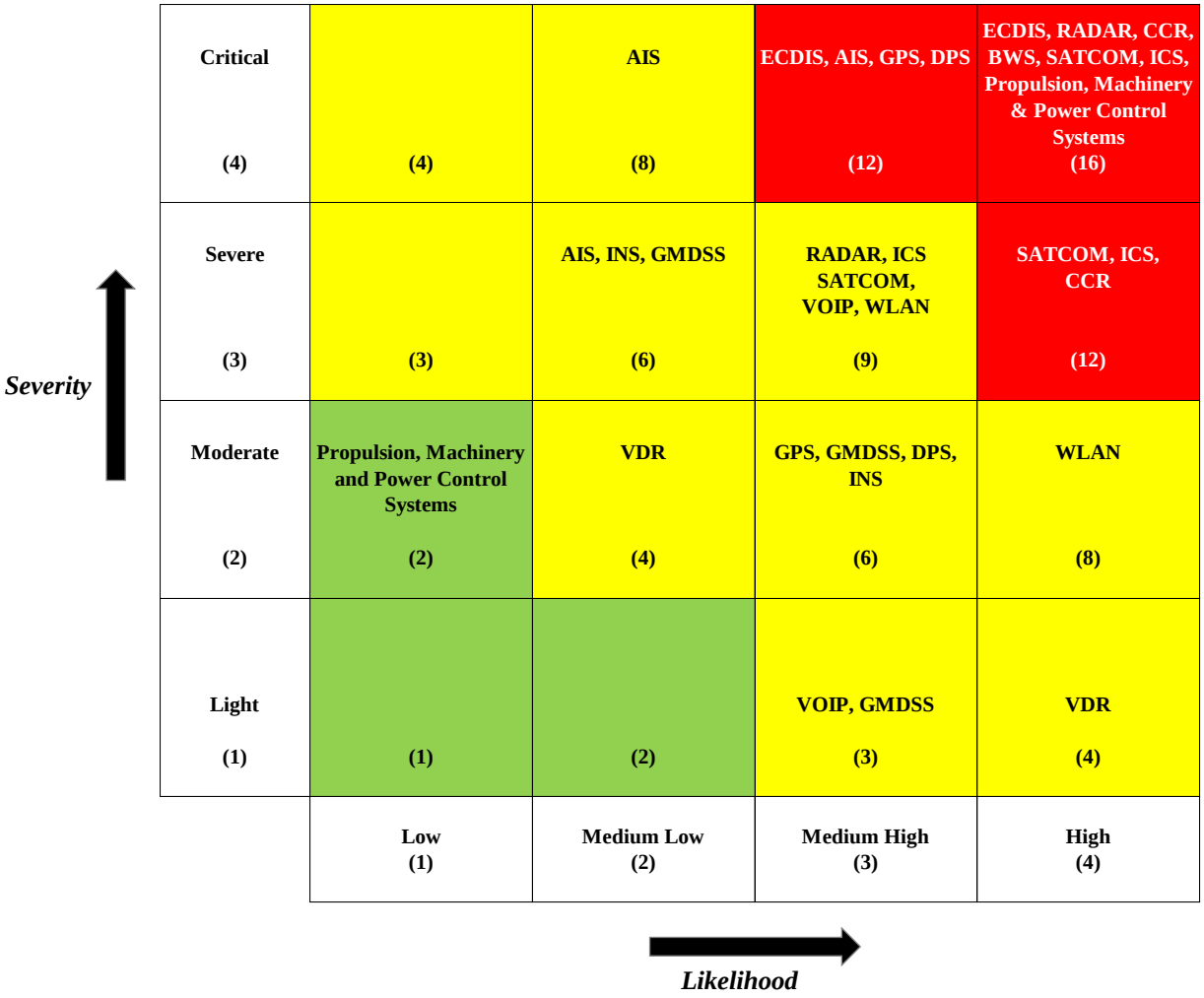

Figure 2 Risk score matrix

From Figure 2, it can be observed that most of the crucial shipboard systems such as SATCOM, ICS, Propulsion systems and machinery, ECDIS, RADAR, CCR, GPS, DPS, and BWS fall under the high-risk category. The vulnerabilities in these systems can easily be exploited by attackers, causing economic loss to the company and disrupt ship operations. The medium-risk systems, as shown in yellow boxes, have comparatively fewer chances of being attacked, but the risks can still cause the unavailability of network and resources. Systems that are of low risk have lesser chances of being attacked when compared to the other two categories; however, they may affect the safety of the ship, its crew and cargo. Appendix 3 includes an explanation of the severity and likelihood scores assigned for each of the risks associated with an OT sub-system.

Tables 9 to 11 depict the list of shipboard systems under high risk, medium risk, and low risk categories, along with the attack surfaces and the list of cyberattacks. It is observable that some of the attack types are common among shipboard systems, and their risk scores are different because the difficulty level of exploits, attack surfaces, and the level of participation in the OT and IT network vary for each system and the associated type of attack. Thus, the risks are assessed based on the knowledge of a system's functionality and vulnerabilities, dependency on internet connectivity, and the flow of data between systems.

Table 9 High risk category

High risk systems	Attack surface	Cyber-attack
ECDIS	USB ports, serial communication network, outdated software	Malware attack, spoofing, Denial-of-Service (DoS) attack
SATCOM, ICS	Phishing emails, VSAT system/modem	Malware attack via Phishing emails, unauthorised administrative access, FTP access, command-line access
AIS	AIS software, AIS messages (VHF radio communication)	Spoofing
DPS	DP system software, GNSS Receiver	Denial-of-Service (DoS) attack
GPS	GPS/GNSS receiver	GPS spoofing
RADAR	Ethernet switch	Malware intrusion
CCR	Phishing emails, USB ports	Ransomware, Malware attack
BWS	Phishing emails, USB ports	Phishing emails, Malware attack
Propulsion, Machinery & Power Control Systems	USB ports	Malware attack

Table 10 Medium risk category

Medium risk systems	Attack surface	Cyber-attack
SATCOM, ICS	VSAT system/modem	Cross-site scripting, eavesdropping, exploiting vulnerabilities in old software versions
AIS	AIS software, AIS messages (VHF radio communication)	Replay attack, Frequency hopping attack
GPS	GPS/GNSS receiver	GPS jamming
WLAN	Access point (router)	Denial of Service (DoS) attack, access point tampering, eavesdropping/session hijacking
VOIP	VOIP protocol (Session Initiation Protocol)	Denial of Service (DoS) attack, eavesdropping, vishing
GMDSS	Very High Frequency (VHF) radio communication, poor/outdated software	Eavesdropping, spoofing, Denial-of-Service (DoS) attack

RADAR	SMB (Server Message Block) service	Man-in-the-middle (MITM) attack
DPS	GNSS receiver, DP system software	Spoofing, Backdoor attack
INS	SMB (Server Message Block) service, Remote desktop protocol	Man-in-the-middle (MITM) attack, Remote code execution
VDR	USB ports, VDR system	Malware attack, Remote code execution

Table 11 Low risk category

Low risk systems	Attack surface	Cyber-attack
Propulsion, Machinery & Power Control Systems	Serial communication network	Man-in-the-middle (MITM) attack

7 CHECKLIST

It may not be possible to have a 100% cyber-secure ship, but it is still possible – and indeed, the responsibility of shipowners - to alleviate the severity and likelihood of a risk with an effective cyber risk management strategy. Performing risk assessment and enforcing appropriate mitigation measures can help to reduce the consequences that arise from cyberattacks. Along with this, having a checklist and checking on the cyber hygiene level of the vessel regularly can help shipowners make sure that the most crucial safety measures are in place.

From cyber risk assessment, OT systems and their corresponding risks were classified into high, medium, and low risk categories according to their risk scores. Now that the risk categories of the systems are known, a checklist with the recommended mitigation measures can help ensure the cyber hygiene of vessels. The checklist in this document provides actionable mitigation measures to each cyber risk associated with a shipboard system. The checklist is actionable and easy to implement since the balance of risks versus costs is considered.

7.1 Tiered Security

A tiered security approach is introduced in the checklist. Tiered security approach adopted in this document consists of three security tiers (Tier 1, Tier 2, Tier 3), where a tier of security refers to the *urgency of cyber risks* of a ship to be managed. The tiers are defined as shown in Table 12.

Table 12 Security tier definition

Security Tier	Security tier definition	Risk score range	Checklist
Tier 1	Tier 1 checklist includes cybersecurity measures for managing high risk cyber threats, which means that the measures stated under this tier are ***highly recommended*** for vessels to implement on-board.	12–16 (Table 9)	Checklist for mitigating risks in high- risk category
Tier 2	Tier 2 checklist includes cybersecurity measures for managing medium risk cyber threats, which means that the security controls mentioned under this tier are ***recommended to have on-board***.	3–9 (Table 10)	Checklist for mitigating risks in medium risk category
Tier 3	Tier 3 checklist includes cybersecurity measures for managing low risk cyber	1–2 (Table 11)	Checklist for mitigating risks

Security Tier	Security tier definition	Risk score range	Checklist
	threats, which means that the measures listed under this tier are ***good to have on-board***, even though the risk level is low.		in low- risk category

This checklist with a tiered approach will help maritime authorities ensure and enhance the cyber hygiene of their vessels. After risk assessment is done, the maritime authorities and shipowners may choose to mitigate the cyber risks at any one or all of the security levels (High, medium, low) by implementing the list of mitigating actions provided under each security tier (Tier 1, Tier 2, Tier 3). If Tier 1 checklist is passed, then the vessel is safeguarded from high-risk cyber threats, and if Tier 2 checklist is passed, the vessel is safe from medium risk cyber threats, and finally if Tier 3 checklist is passed, the vessel is protected against low-risk cyber threats also.

7.2 Checklist with Security Tiers

The mitigation checklist and security tier classification for cyber risks associated with OT sub-systems are given in Tables 13 to 16.

Table 13 Checklist - Communication Systems

Communication Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
1. Satellite Communication System (SATCOM) 2. Integrated Communication System (ICS) 1. Satellite Communication System (SATCOM) 2. Integrated Communication System (ICS)	❒ Unauthorised access of vessel network	❒ **T1-1** Firewall is configured to allow only whitelisted sources or IP addresses within a subnet. ❒ **T1-2** Virtual Private Network is used while accessing the Internet. ❒ **T1-3** IP address is private, and it is not available on any public domain (e.g., Shodan). ❒ **T1-4** OS, antivirus, firewall and other applications used in the business computer (The computer used for accessing emails, and VSAT modem's web interface) is updated/patched regularly. ❒ **T1-5** Access to the business computer is restricted to authorised personnel with admin login and strong credentials are used for login. ❒ **T1-6** The default username and password in VSAT modem is changed.	**1**

Communication Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
(cont'd)		❒ **T1-7** The password for accessing the VSAT web interface is strong - For example, password with 12 characters and at least one uppercase letter and one special character is recommended. ❒ **T1-8** Password reset mechanisms are implemented – It is recommended to change password once in three months. ❒ **T1-9** A secure password manager application or a password protected PDF/Word document is used to store passwords (if in use). ❒ **T1-10** Block access to the business computer after 3 failed login attempts. ❒ **T1-11** Multi-factor authentication (MFA) is set up for accessing the business computer and VSAT web interface. ❒ **T1-12** FTP is disabled in the VSAT modem's web interface.	
	Phishing emails Phishing emails (cont'd)	❒ **T1-13** Antivirus software is installed in the business computer. ❒ **T1-14** Files and email attachments downloaded from emails are scanned with antivirus software before opening it. ❒ **TI-15** Regular data backup is done and stored safely. ❒ **T1-16** Crew awareness is established on the following: o Ability to distinguish phishing emails from the real ones o Be aware that that emails from unknown sources should be viewed carefully and suspicious email attachments should not be opened, especially not to enable macro function in Microsoft documents. o Be aware that they must not click on suspicious links ❒ **T1-17** Email security is implemented in Outlook/Gmail – For example, S/MIME (Secure Multipurpose Internet *Mail* Extension) can be implemented to	

Communication Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
		encrypt the email and ensure authenticity and integrity of the email.	
	Outdated VSAT software	❒ **T2-1** Latest version of VSAT software is installed. ❒ **T2-2** Software updates are checked regularly to fix vulnerabilities. ❒ **T2-3** All updates are logged. ❒ **T2-4** If remote service/maintenance or an update is made, the authenticity of the vendor service, update and the remote desktop connection is verified manually (e.g., phone call) and then access is permitted for the specified requirement.	**2**
	Eavesdropping	**T2-5** The VSAT web interface supports/uses secure protocols such as HTTPS, SSHv2.	**2**
	Cross-site scripting	**T2-6** The VSAT web interface has inbuilt security mechanisms such as input sanitisation (any suspicious inputs must be rejected), output encoding, CSP (Content Security Policy) to protect against scripting attacks.	**2**
3. Voice Over Internet Protocol (VOIP)	Denial-of-Service (DoS) attack	❒ **T2-7** Network is frequently monitored by the IT team using Intrusion Detection Systems. ❒ **T2-8** All VOIP calls pass through the firewall.	**2**
	Eavesdropping	**T2-9** The network through which VOIP calls are initiated/received is encrypted.	**2**
	Vishing	**T2-10** The crew is aware that they must not provide any personal details or vessel information if they receive calls from unknown sources.	**2**
4. Wireless Local Area Network (WLAN)	Denial-of-Service (DoS) attack	❒ **T2-11** Network is frequently monitored by the IT team using Intrusion Detection Systems. ❒ **T2-12** Firewall is configured to allow only whitelisted sources.	**2**
	Access point tampering	**T2-13** Routers/access points are kept in a secured location such as a locked closet.	**2**
	Eavesdropping/session hijacking	**T2-14** A secure encryption standard is used in wireless networks.	**2**

From Table 13, it can be observed that most of the cyber risks in sub-systems under communication systems fall under Tier 2 and Tier 1 due to high severity and likelihood levels. Vessels are constantly connected to the Internet through satellite communication systems for various ship operations and email access. The usage of default/weak credentials in the VSAT modem web administration interface and phishing emails are some of the easiest ways for an attacker to barge into the ship network. Through these ways, an attacker can compromise the vessel network and tamper with the communication between shipboard systems, which will affect vessel operations. The compromised network could be a starting point for any type of attack on the rest of the shipboard systems in that network, hence it is very crucial to enforce the mitigation measures given in this checklist under Tier 1. The checklist in Tier 1 itself acts as the first layer of defence to the cyber risks addressed under Tier 2 of communication systems.

Table 14 Checklist - Propulsion, Machinery & Power Control Systems

Propulsion, Machinery & Power Control Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
5. Fuel Oil System 6. Engine Governor System 7. Alarm Monitoring and Control System 8. Power Management System 9. Emergency Generators and Batteries	Malware attack (via USB ports)	❒ **T1-18** Physical security measures are implemented: o Access control list for the crew to enter the engine control room or any other place where crucial machinery is present. o Access control list is reviewed and updated regularly. ❒ **T1-19** USB ports in the engine and fuel monitoring system, alarm monitoring and control system and power management system is enabled only in admin login and disabled in other user logins (if any). ❒ **T1-20** The admin login credentials in engine and fuel monitoring system, alarm monitoring and control system and power management systems have strong password. ❒ **T1-21** Antivirus software is installed in the engine and fuel monitoring system, alarm monitoring & control system and power management system. ❒ **T1-22** USB port blockers are used to block unused ports in the engine and fuel monitoring system, alarm monitoring and control system and power management system. ❒ **T1-23** Dedicated charging points (ports) are assigned for the crew.	**1**

Propulsion, Machinery & Power Control Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
		❒ **T1-24** USB cleaning station (a separate PC with antivirus software to scan the USB drives before use) is setup.	
	Man-in-the-middle (MITM) attack	❒ **T3-1** SATCOM is secured, as in No.1 and 2 in Table 12. ❒ **T3-2** Phishing email threat is mitigated as in No.1 and 2 in Table 12. ❒ **T3-3** OS, antivirus, and other applications used in the engine and fuel monitoring system, alarm monitoring & control system and power management system are updated. ❒ **T3-4** Crew access to the critical systems, and computers that control and monitor machinery is regulated. ❒ **T3-5** If remote service/maintenance is done on any of the systems, the authenticity of the vendor service and the remote desktop connection is verified manually (e.g., phone call) and then access is permitted. ❒ **T3-6** OT network is separated from the IT network by a demilitarized zone (DMZ)/Firewall. ❒ **T3-7** If a Serial to IP converter is in use, encryption is enabled, the converter software is up to date, and strong login credentials are used.	**3**

The two major cyber risks in Propulsion, Machinery & Power Control Systems include malware attacks via USB ports and the MITM attack, as shown in Table 14. The USB ports in machinery monitoring and control systems is one of the ways in which an attacker can initiate a malware attack. As such, it is very crucial to enforce strict physical security controls and create awareness among the crew to protect against malware attacks through removable media (Tier 1 checklist). Apart from the technical and procedural security measures under Tier 3, safeguarding satellite communication systems and enforcing appropriate security measures to protect against malware attacks (via phishing emails) play a major role in mitigating the MITM attack threat in Propulsion, Machinery & Power Control Systems. This acts as a top layer of security to these systems; in case an attacker compromises the vessel network, different types of attacks can be launched on the machinery monitoring and control systems connected to that network. Even though the likelihood of this attack is low, if the attack is successful, it would give an attacker the ability to tamper with the functionality of the system. Hence implementing the security measures in Tier 3 checklist can help mitigate MITM threat.

Table 15 Checklist - Navigation Systems

Navigation Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
10. Electronic Chart Display and Information System (ECDIS)	Malware attack (via USB ports)	❒ **T1-25** Antivirus software is installed in the system. ❒ **T1-26** Chart updates are logged. ❒ **T1-27** USB ports are safeguarded - enabled only in admin login and disabled in other user logins or only enabled by the captain of the ship whenever there is a need to use USB or port blockers are used to avoid unnecessary plugins.	**1**
	Denial-of-Service (DoS) attack	**T1-28** Firewall is installed in the system to allow only known IP addresses.	
	Spoofing	❒ **T1-29** ECDIS software and the underlying operating system is updated. ❒ **T1-30** If a Serial to IP converter is in use, encryption is enabled, the converter software is up to date, and strong login credentials are used.	
11. Radio Detection and Ranging (RADAR)	Malware intrusion	❒ **T1-31** Antivirus software is installed in the system. ❒ **T1-32** RADAR software and the underlying operating system must be updated	**1**
	Man-in-the-middle (MITM) attack	**T2-15** Server Message Block signing (SMB Signing) is enforced on the RADAR system's underlying operating system.	**2**
12. Automatic Identification System (AIS)	Spoofing	**T1-33** AIS messages are authenticated (e.g., PKI schema, geolocate transmissions by TDOA)	**1**
	Replay attack	**T2-16** Timestamp is monitored on all messages.	**2**
	Frequency hopping attack	**T2-17** AIS messages are authenticated (e.g., PKI schema to authenticate the messages exchanged between ships and with port authorities).	
13. Global Positioning System (GPS)	Spoofing	**T1-34** Anti-spoofing technique (e.g., Absolute power monitoring) is utilised in the GNSS receiver to detect the spoofed signals.	**1**
	Jamming	**T2-18** Anti-jamming technique (e.g., Spectrum monitoring technique) is utilised in the GNSS receiver to detect the GPS jammers.	**2**

Navigation Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
14. Dynamic Positioning System (DPS)	Denial-of-Service (DoS) attack	❒ **T1-35** Firewall is installed in the system to allow only known IP addresses. ❒ **T1-36** DP control system software is updated.	**1**
	Spoofing	**T2-19** Anti-spoofing technique (e.g., Absolute power monitoring) is utilised in the GNSS receiver to detect the spoofed signals.	**2**
	Backdoor	**T2-20** Antivirus software is installed in the DP system to detect the malware.	**2**
15. Global Maritime Distress and Safety System (GMDSS)	Eavesdropping	**T2-21** The software used in the GMDSS system is updated.	**2**
	Denial-of-Service (DoS) attack	**T2-22** Firewall is installed in the system to allow only known IP addresses.	
	Spoofing	**T2-23** Messages exchanged between ships and port authorities are authenticated (e.g., PKI schema)	
16. Voyage Data Recorder (VDR)	Malware attack (via USB ports)	❒ **T2-24** Antivirus software is used to scan any external media before connecting to the system. ❒ **T2-25** USB ports are safeguarded - enabled only in admin login and disabled in other user logins or only enabled by the captain of the ship whenever there is a need to use USB or port blockers are used to avoid unnecessary plugins. ❒ **T2-26** Regular data backup (data recorded in the VDR) is done and stored safely.	**2**
	Remote code execution	**T2-27** VDR software is up to date.	
17. Integrated Navigation System (INS)	Man-in-the-middle (MITM) attack	**T2-28** The remote desktop connection is encrypted.	**2**
	Remote code execution	**T2-29** Operating system is up to date.	**2**

The mitigation checklist and security tiers for the cyber risks identified in navigation systems are provided in Table 15. The cyber risks associated with the sub-systems under navigation systems fall under the high risk and medium risk category. An attacker can easily gain access to high-risk systems by introducing malware through USB ports, overloading network with traffic to perform a DoS attack, and manipulating NMEA plain text messages. On the other hand, medium-risk systems are vulnerable to MITM attacks, eavesdropping, remote code execution, etc. Hence it is essential to implement the mitigation measures under Tier-1 and Tier-2 to help mitigate these attacks.

Finally, Table 16 includes the mitigation checklist and security tiers for cyber risks in cargo management systems. Cargo management systems are prone to malware attacks via USB ports and phishing emails, hence it is crucial to enforce the security measures under Tier-1 to avoid the consequences of these attacks.

Table 16 Checklist - Cargo Management Systems

Cargo Management Systems			
OT sub-system(s)	**Cyber risk checklist**	**Mitigation checklist**	**Security tier**
18. Cargo Control Room (CCR)	Ransomware (via phishing emails)	❒ **T1-37** Antivirus software is installed in the system. ❒ **TI-38** The crew is well-trained to identify phishing emails. ❒ **T1-39** Regular data backup is done and stored safely.	**1**
	Malware attack (via USB ports)	❒ **T1-40** Antivirus software is installed to scan the USB drives before connecting it to the system. ❒ **T1-41** USB ports are safeguarded - enabled only in admin login and disabled in other user logins or only enabled by the captain of the ship whenever there is a need to use USB or port blockers are used to avoid unnecessary plugins.	**1**
19. Ballast Water System (BWS)	Phishing emails	❒ **T1-42** Antivirus software is installed in the system. ❒ **T1-43** The crew is well-trained to identify suspicious emails. ❒ **T1-44** Regular data backup is done and stored safely.	**1**
	Malware attack (via USB ports)	❒ **T1-45** Antivirus software is installed in the system to scan any external media for malware before being plugged into the system. ❒ **T1-46** USB ports are safeguarded - enabled only in admin login and disabled in other user logins or only enabled by the captain of the ship whenever there is a need to use USB or port blockers are used to avoid unnecessary plugins.	

8 CONCLUSIONS

As shipboard systems are interconnected and rely on the Internet for operational requirements and remote services, cybersecurity controls onboard ships need to strengthen. Several maritime cyber-attacks have been reported, and such attacks can be ascribed to flaws in the application of proper security controls and lack of crew awareness on maritime cybersecurity. The guidelines in this document will help identify the severity of risks and enforce appropriate security controls. The checklist included in these guidelines will help ship owners assess the cyber hygiene of their vessels and enhance cyber safety onboard vessels accordingly. These guidelines are easy to understand and implement, hence it will guide shipowners and maritime authorities in enforcing good cybersecurity practices to manage the cyber risks associated with shipboard OT systems.

9 ACKNOWLEDGEMENTS

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-2020-MA-04. The team would like to thank the Maritime and Port Authority of Singapore (MPA) for its guidance and inputs throughout this study. We would also like to extend our thanks to American Bureau of Shipping (ABS), Klynveld Peat Marwick Goerdeler (KPMG), Centre of Excellence in Maritime Safety (CEMS) in Singapore Polytechnic (SP), and Singapore Shipping Association (SSA) for their valuable feedback on the draft version guidelines.

List of authors contributing to the guidelines:

- Priyanga Rajaram, Senior Research Assistant, iTrust, SUTD
- Ruchitha Dumbala, Senior Research Assistant, iTrust, SUTD
- Mark Goh Voon Wei, Senior Manager, iTrust, SUTD
- Prof. Jianying Zhou, Co-center Director, iTrust, SUTD

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

10 REFERENCES

[1] "Maritime Cyber Risk Management in Safety Management Systems," International Maritime Organization, 2017.

[2] "Guidelines on Maritime Cyber Risk Management," International Maritime Organization, London, 2017.

[3] National Institute of Standards and Technology (NIST), "NIST Cybersecurity Framework," [Online]. Available: https://www.nist.gov/cyberframework.

[4] "Guidelines on Cyber Security Onboard Ships (Version 4)," BIMCO, CSA, DCA, INTERTANKO, INTERCARGO, INTERMANAGER, ICS, IUMI, OCIMF, SYBASS, WSC, 2020.

[5] "Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation," Det Norske Veritas, 2016.

[6] Det Norske Veritas, "Class Guideline Cyber Secure," Det Norske Veritas, 2020.

[7] "Analysis of Cyber Security Aspects in the Maritime Sector," European Network and Information Security Agency, 2011.

[8] "Port Cybersecurity - Good practices for cybersecurity in the maritime sector," European Network and Information Security Agency, 2019.

[9] "Code of Practice Cyber Security for Ships," Institution of Engineering and Technology, London, 2017.

[10] American Bureau of Shipping (ABS), "The Guide for Cybersecurity Implementation for the Marine and Offshore Industries, ABS Cybersafety Volume 2," American Bureau of Shipping (ABS), 2021.

[11] R. Oaks, "What Is Satellite Internet?," 31 March 2021. [Online]. Available: https://www.satelliteinternet.com/resources/what-is-satellite-internet/.

[12] "Very Small Aperture Terminal (VSAT)," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/vsat-very-small-aperture-terminal.

[13] M. Wingrove, "How to ensure VSAT modems cannot be hacked," 05 December 2019. [Online]. Available: https://www.rivieramm.com/news-content-hub/news-content-hub/ensure-vsat-modems-cannot-be-hacked-57065.

[14] "Shipboard Integrated Communications System," ST Engineering, 2021.

[15] Thales group, "Shipboard Communication & Management," [Online]. Available: https://www.thalesgroup.com/en/markets/defence-and-security/radio-communications/naval-communications/shipboard-communication.

[16] Borderless Hub, "Ship to Shore," [Online]. Available: https://www.borderlesshub.com/ship-to-shore/.

[17] Riviera Maritime Media Ltd, “The complete guide to VSAT,” Riviera Maritime Media Ltd, 2019.

[18] WebTitan, “Most Common Wireless Network Attacks,” 19 April 2018. [Online]. Available: https://www.webtitan.com/blog/most-common-wireless-network-attacks/.

[19] C. Cimpanu, “Ships infected with ransomware, USB malware, worms,” 12 December 2018. [Online]. Available: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.

[20] S. Sethi, “Types of Governors for Engines Used On Ships,” 25 September 2020. [Online]. Available: https://www.marineinsight.com/tech/types-of-governors-for-engines-used-on-ships.

[21] B. Hyra, “Analyzing the Attack Surface of Ships,” Denmark, 2019.

[22] Shippipedia, “Ship Automation & Control System,” [Online]. Available: http://www.shippipedia.com/ship-automation-control-system/.

[23] Anish, “Marine Heavy Fuel Oil (HFO) For Ships – Properties, Challenges and Treatment Methods,” 01 January 2021. [Online]. Available: https://www.marineinsight.com/tech/marine-heavy-fuel-oil-hfo-for-ships-properties-challenges-and-treatment-methods/.

[24] Anish, “Different Types of Alarms on Ships,” 14 January 2021. [Online]. Available: https://www.marineinsight.com/marine-safety/different-types-of-alarms-on-ship/.

[25] Electro Technical Officer, “All about Emergency Generator on ship,” [Online]. Available: https://electrotechnical-officer.com/all-about-emergency-generator-on-ship/.

[26] Anish, “How is Power Generated and Supplied on a Ship?,” 25 September 2020. [Online]. Available: https://www.marineinsight.com/marine-electrical/how-is-power-generated-and-supplied-on-a-ship/.

[27] Mohit, “Ways of starting and testing emergency generator,” 09 July 2020. [Online]. Available: https://www.marineinsight.com/tech/generator/ways-of-starting-and-testing-emergency-generator/.

[28] S. Bhattacharjee, “What is Electronic Chart Display and Information System (ECDIS)?,” Marine insight, 04 12 2020. [Online]. Available: https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/.

[29] Y. Dyryavyy, “Can You Hack An Ecdis?,” UKMPA, 26 08 2015. [Online]. Available: https://www.pilotmag.co.uk/can-you-hack-an-ecdis-yevgen-dyryavyy/.

[30] S. Bhattacharjee, “Marine Radars and Their Use in the Shipping Industry,” 8 January 2021. [Online]. Available:]https://www.marineinsight.com/marine-navigation/marine-radars-and-their-use-in-the-shipping-industry/.

[31] M. B. M. K. Dimitrios Dalaklis, “Vulnerabilities of the Automatic Identification System in the Era of Maritime Autonomous Surface Ships,” in *9th NMIOTC Annual Conference (Fostering Projection of Stability through Maritime Security: Achieving Enhanced Capabilities and Operational Effectiveness)*, 2018.

[32] “GPS.GOV,” [Online]. Available: https://www.gps.gov/applications/marine/.

[33] O. C. &. A. Rinnan, “Who Said That DP Does Not Rhyme With Cybersecurity?,” 2016.

[34] S. Bhattacharjee, “Introduction to Global Maritime Distress Safety System (GMDSS) – What You Must Know,” Marine Insight, 06 September 2021. [Online]. Available: https://www.marineinsight.com/marine-navigation/introduction-gmdss-global-maritime-distress-safety-system/.

[35] I. R. A. J. a. D. Z. Boris Svilicic, “A Study on Cyber Security Threats in a Shipboard Integrated Navigational System,” *Journal of Marine Science and Engineering*, p. 11, 2019.

[36] Wikipedia, “Cargo control room,” [Online]. Available: https://en.wikipedia.org/wiki/Cargo_control_room. [Accessed 21 July 2021].

[37] S. Lagouvardou, “Maritime Cyber Security: concepts, problems and models,” 2018.

[38] M. Wingrove, “Secure VSAT to prevent cyber attacks,” 16 April 2020. [Online]. Available: https://www.rivieramm.com/news-content-hub/news-content-hub/secure-vsat-to-prevent-cyber-attacksnbsp-58986.

[39] R. Foggia, “CVE-2019-15652: SatLink VSAT Vulnerabilities,” 21 November 2019. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cve-2019-15652-satlink-vsat-vulnerabilities/.

[40] E. Robinson, “Hacked – a real life story of exploiting vessel VSAT,” 25 May 2020. [Online]. Available: https://smartmaritimenetwork.com/2020/05/25/hacked-a-real-life-story-of-exploiting-vessel-vsat/.

[41] C. McCraw, “12 VoIP Security Vulnerabilities and How to Fix Them,” 06 May 2020. [Online]. Available: https://getvoip.com/blog/2020/05/06/voip-security/.

[42] M. Wingrove, “‘Impregnable’ radar breached in simulated cyber attack,” 2018. [Online]. Available: https://www.rivieramm.com/news-content-hub/news-content-hub/impregnable-radar-breached-in-simulated-cyber-attack-25158.

[43] I. R. V. F. c. a. D. M. ´. c. Boris Svilicic, “Towards a Cyber Secure Shipboard,” *THE JOURNAL OF NAVIGATION*, vol. 73, p. 12, 2020.

[44] “Automatic Identification Systems (AIS), its Benefits and Threats,” 2016. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/faq-automatic-identification-systems-ais-benefits-and-threats.

[45] D. G. S. R. Joseph DiRenzo, “The Little-known Challenge of Maritime Cyber Security,” [Online]. Available: http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberSecurityCorfu7-5-15.pptx.pdf.

[46] Connectivity, “Understanding GPS spoofing in shipping: How to stay protected,” 2020. [Online]. Available: https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/.

[47] D. A. Grant, “GPS Jamming and its impact on maritime navigation,” 10 May 2010. [Online]. Available: https://www.gla-rad.org/content/uploads/2018/01/gps-jamming-and-its-impact-on-maritime-navigation-presentation.pdf.

[48] Nettitude, “Marine and Offshore Cyber Briefing: Cyber Risks in Communication Systems,” [Online]. Available: https://cdn2.hubspot.net/hubfs/3021880/NETT_2019_M&O_Cyber%20Risks%20in%20Communication%20Systems_0711.pdf. [Accessed 28 October 2020].

[49] G. Z. C. V. Dennis Bothur, “A critical analysis of security vulnerabilities and countermeasures,” 2017.

[50] M. B. N.Kala, “Cyber Preparedness in Maritime Industry,” *International Journal of Scientific and Technical Advancements,* vol. 5, no. 2, p. 28, 2019.

[51] “STRIDE (security),” 2021. [Online]. Available: https://en.wikipedia.org/wiki/STRIDE_(security). [Accessed November 25].

[52] Riviera Newsletters, “10 tips to reduce the risk of cyber attacks at sea,” 02 May 2018. [Online]. Available: https://www.rivieramm.com/opinion/opinion/10-tips-to-reduce-the-risk-of-cyber-attacks-at-sea-24875.

[53] Witherby, BIMCO, ICS, Cyber Security Workbook for On Board Ship Use, Livingston: Witherby Publishing Group Ltd, 2021.

[54] D. C. M. P. C. D. David Maguire, “S/MIME for message signing and encryption,” 23 March 2021. [Online]. Available: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/smime/smime?view=exchserver-2019.

[55] “Cross-site scripting,” [Online]. Available: https://portswigger.net/web-security/cross-site-scripting.

[56] VoIP Info, “What Is Telephony Denial of Service and How to Prevent It,” 15 July 2019. [Online]. Available: http://www.voipinfo.net/telephony-denial-of-service-and-how-to-prevent-it/.

[57] J. Karasek, “Security 101: Protecting Wi-Fi Networks Against Hacking and Eavesdropping,” 13 June 2018. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-protecting-wi-fi-networks-against-hacking-and-eavesdropping.

[58] K. Munro, “Hacking Serial Networks on Ships,” 25 June 2018. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-serial-networks-on-ships/.

[59] o. Developer, “How to Mitigate DoS Attacks,” [Online]. Available: https://developer.okta.com/books/api-security/dos/how/.

[60] G. Weadock, “SMB Signing and Security,” 31 Jan 2010. [Online]. Available: https://www.networkworld.com/article/2229737/smb-signing-and-security.html.

[61] “Overview of Server Message Block signing,” [Online]. Available: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing.

[62] “AIS Spoofing Detection with TDOA,” CRFS, [Online]. Available: https://www.crfs.com/blog/ais-spoofing-detection-with-tdoa/.

[63] Kaspersky, “What Is a Replay Attack?,” [Online]. Available: https://www.kaspersky.com/resource-center/definitions/replay-attack.

[64] A. P. Marco Balduzzi and Kyle Wilhoit, “A Security Evaluation of AIS,” [Online]. Available: https://www.n0secure.org/wp-content/uploads/2016/06/wp-a-security-evaluation-of-ais.pdf.

[65] M. A. F. S. A. K. S. M. A. U. A. Mukhtar Ahmad, “Impact and Detection of GPS Spoofing and Countermeasures against Spoofing,” 2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019 , 2019.

[66] “How to deal with GPS jamming and spoofing,” CRFS, July 2020. [Online]. Available: https://www.crfs.com/blog/how-to-deal-with-gps-jamming-and-spoofing/.

[67] B. Martens, “What Is a Backdoor & How to Prevent Backdoor Virus Attacks in 2021,” SafetyDetectives, 31 May 2021. [Online]. Available: https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/.

[68] “Set up DKIM to prevent email spoofing,” [Online]. Available: https://support.google.com/a/answer/174124?hl=en.

[69] R. Santamarta, “Maritime Security: Hacking into a Voyage Data Recorder (VDR),” IOActive, 9 December 2015. [Online]. Available: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/.

[70] I. R. A. J. a. D. Z. Boris Svilicic, “A Study on Cyber Security Threats in a Shipboard Integrated Navigational System,” *Journal of Marine Science and Engineering,* p. 11, 2019.

[71] M. Cooney, “IBM warns of rising VoIP cyber-attacks,” Network World, 01 December 2016. [Online]. Available: https://www.csoonline.com/article/3146526/ibm-warns-of-rising-voip-cyber-attacks.html.

[72] Offshore Energy, “Nightmare Scenario: Ship Critical Systems Easy Target for Hackers,” 21 December 2017. [Online]. Available: https://worldmaritimenews.com/archives/238869/nightmare-scenario-ship-critical-systems-easy-target-for-hackers/.

[73] “Understanding GPS spoofing in shipping: How to stay protected,” 31 01 2020. [Online]. Available: https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/.

[74] O. Delagrange, “Cyber risks and the marine cargo market,” 15 03 2018. [Online]. Available: https://kennedyslaw.com/thought-leadership/article/cyber-risks-and-the-marine-cargo-market/.

[75] K. Kochetkova, “Maritime industry is easy meat for cyber criminals,” 22 May 2015. [Online]. Available: https://www.kaspersky.com/blog/maritime-cyber-security/8796/.

11 APPENDIX

11.1 Appendix 1 – Cyber Risks in Shipboard OT Systems

Table 17 Cyber risks - Communication Systems

Communication Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
1. **Satellite Communication System (SATCOM) –** SATCOM system enable the vessels and crew to stay connected to the internet, no matter how far the vessel is from the land. The VSAT (Very Small Aperture Terminal) is a ground station/modem used to transmit/receive data, voice, and video signals over a satellite communication network. All the connections are managed and configured through the VSAT web administration interface.	• Phishing emails • VSAT modem	• Phishing email (Malware attack) • Exploiting the vulnerabilities in old software versions • Eavesdropping due to the use of weak protocols (HTTP, Telnet) • Cross-site scripting • Unauthorised administrative access	• Phishing emails tend to deliver malware such as spyware, ransomware, viruses by tricking the victim to click on links or download files which cause unavailability of systems and data breach. • Hackers can get access to the vessel network by exploiting the vulnerabilities in the old version of VSAT software resulting in disruption of day-to-day vessel operations and lack of communication between ship-shore. • By eavesdropping in the vessel network, an attacker can sniff credentials and sensitive information, resulting in a breach of confidentiality. • Scripting attacks occur on a poorly configured VSAT web administration interface. Attacker can input malicious code, modify credentials, capture cookies and hijack the session. • Usage of weak or default credentials in the VSAT web administration interface can	• Ethical hackers discovered that some VSAT modems only support insecure protocols for their management and application [38]. • In February, Dryad Global and Red Sky Alliance published a report identifying new phishing emails attempting to deliver malware [38]. • Yangosat's ethical hackers hacked the communication system of the ship [40].
2. **Integrated Communication System (ICS) –** ICS enables a centralised management and control of the ship's overall communications and provides high operation efficiency and				

Communication Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
faster incident response. The key components include the VSAT modem, VOIP, WLAN access points, radio communication equipment and monitoring devices. Since a significant part of a ship's communication depends on VSAT, it can be the entry point for a wide variety of attacks targeting other systems such as VOIP, access points and equipment monitoring systems in the ship.			lead to unauthorised access of vessel network, through which attacker can gain privileges such as administrative access, FTP access and command-line access. With such privileges, an attacker can view/edit confidential files and compromise other shipboard systems in the network.	
3. Voice Over Internet Protocol (VOIP) – VOIP is used to make and receive phone calls over the internet. A fast, reliable, and secure communication system is needed to provide clear and immediate instructions to ensure crew and passenger safety.	Network server/ Session Initiation Protocol	• Denial of Service (DoS) attack • Eavesdropping • Vishing	• Hackers can flood the VoIP network server with SIP call-signalling messages, which will exhaust the maximum bandwidth available and slow down or stop the system traffic. This will result in lack of communication inside the ship and between ship-shore. • Eavesdropping can result in loss of confidentiality and privacy. Hackers can gain personal and confidential information by unauthorised interception of a vessel VOIP network. • Vishing occurs when an attacker spoofs the caller ID and tricks recipient into providing sensitive data such as vessel	There are no known Cyber incidents in maritime industry regarding VOIP, but there are other incidents [71].

Communication Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
			location, cargo details, crew details, etc., by pretending to be a legitimate source.	
4. Wireless Local Area Network (WLAN) – A WLAN is a wireless network setup where two more devices are connected to form a local area network. Routers can be connected to the VSAT modem and configured to use as Wi-Fi access points.	Access point (router)	• Denial of Service (DoS) attack • Access point tampering • Eavesdropping/session hijacking	• Hackers can launch a DoS attack by overwhelming the access point with fake requests, causing the network to slow down or stop, resulting in the unavailability of internet onboard. • If the access point is placed in a location where it can be physically accessed, tampering can occur. It takes just seconds to revert the access point to factory default settings. • Due to the use of weak encryption standards, hackers can intercept the vessel traffic and steal login credentials or sensitive data and hijack the entire session.	There are no known cyber incidents in the maritime industry regarding WLAN. However, there are many incidents in other sectors. For example, a cybersecurity expert has demonstrated that it is possible to hack into airline WIFI networks from the ground and view the internet activity of passengers and intercept their information. Also, he was also able to gain access to the cockpit network and SATCOM equipment. He claims the same technique could be used for ships [18].

Table 18 Cyber risks - Propulsion, Machinery & Power Control Systems

Propulsion, Machinery & Power Control Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
5. Fuel Oil System – The fuel oil system is used for ship propulsion and to generate power by utilizing the energy acquired from burning the oil. Tank level, temperature and viscosity are some of the key parameters to be considered in a fuel oil system.	• Serial communication network (e.g., NMEA/CAN) • Open USB ports	• Man-in-the-middle (MITM) attack • Malware attack	• Fuel level indicator can be tampered with to show the wrong fuel level, which might result in issues such as overloading the fuel storage tank or delay in reaching the destination. • Malware intrusion via USB ports in the fuel monitoring/control systems might cause dysfunction, resulting in an explosion or any other physical damage.	Naval Dome, an ethical hacking group, have proven that it is possible to compromise fuel system [72].
6. Engine Governor System – Engine governor is a crucial component of the ship, which is used to control the mean speed of the engine under varying load states. Communication with the ship's machinery is done through the serial communication network (e.g., NMEA/CAN). Some of the parameters that need to be considered in a ship's engine operations include fuel consumption, combustion temperature, engine temperature and engine start/stop status.	• Serial communication network (e.g., NMEA/CAN) • Open USB ports	• Man-in-the-middle (MITM) attack • Malware attack	• Tampering with the serial communication between the controllers and other equipment might slow down or disrupt the engine performance. • Malware intrusion via USB ports in the engine monitoring/control systems might cause dysfunction, resulting in an explosion or any other physical damage.	Two maritime cyber incidents reported on unauthorised usage of USB drives, which disrupted ship operations and caused financial damage [19].
7. Alarm Monitoring and Control System – The alarm monitoring and control system monitors and controls all the alarms implemented on the ship. It connects the alarms	• Serial communication network (e.g., NMEA/CAN) • Open USB ports	• Man-in-the-middle (MITM) attack • Malware attack	• An attacker can launch a MITM attack by modifying alarm-related commands relayed between the systems onboard. An attacker may either suppress an alarm or raise fake alarms, and due to this, the crew may be unaware of a	

Propulsion, Machinery & Power Control Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
associated with each of the systems in the ship and emits visual or audio signals in the event of emergency or failure.			potential system failure or an emergency, putting lives and cargo at risk. • Malware intrusion via USB ports in the alarm monitoring and control systems might cause dysfunction, threatening the safe voyage of ship and crew.	
8. Power Management System – The goal of this system is to provide an uninterrupted power supply to all the components in the vessel. The PMS automates functions such as the start/stop of generators, voltage and frequency control and load control.	• Serial communication network (e.g., NMEA/CAN) • Open USB ports	• Man-in-the-middle (MITM) attack • Malware attack	• Tampering with the voltage and frequency values might result in a disrupted power supply to all the systems in the vessel and cargo containers, affecting vessel operations and cargo. • Malware intrusion via USB ports in the power management system might cause dysfunction, affecting the vessel operations and cargo containers.	
9. Emergency Generators and Batteries – The purpose of an emergency generator is to provide backup power to the crucial device in the ship in case the main generator fails or if a power outage occurs unexpectedly. Both the batteries and the emergency generator can be used in case of an emergency. The generator control is present in the power management system panel, where voltage and frequency are monitored	• Serial communication network (e.g., NMEA/CAN) and open USB ports in the power management system	• Man-in-the-middle (MITM) attack and malware attack on the power management system	• Cyberattacks that cause the power management system to fail will trouble the automatic start of the emergency generator since the emergency generator control is present in the power management system. If an attacker compromises the power management system, the emergency generator may fail to kick in when there is a power outage or low voltage, hence affecting vessel operations and its cargo. For example, reefer containers carry temperature-sensitive goods that require constant electricity throughout the voyage.	

Table 19 Cyber risks - Navigation systems

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
10. Electronic Chart Display and Information System (ECDIS) – ECDIS utilises the feature of the Global Positioning System (GPS) to accurately pinpoint the navigational points. It is interfaced with other navigational equipment such as the Gyro compass, RADAR, AIS, and the position, heading, speed sensors in a serial communication network (NMEA). One of the majorly used method for updating charts is with the help of removable media.	• Malware attack (via USB Port) • Old OS/Software (Not updated, no firewall configuration) • Serial communication network (NMEA) – Unencrypted/Unauthorized	• Malware attack via USB ports • Denial-of-service (DoS) attack • Spoofing the ship's real position – by hacking the ECIDS machine itself or spoofing incoming plan text messages to the ECIDS form NMEA network	• When a crew member intentionally or unintentionally inserts a malware-infected USB drive into the USB port in the system, malware can enter the system and disrupt the operations of ECDIS. • A DoS attack occurs when an attacker overloads the network with traffic, which takes the ECDIS offline and leaves the vessel without means for safe navigation. • Due to lack of encryption and authentication, it is possible to spoof the incoming plain text messages from the NMEA network to the ECIDS, for example, tampering with the chart information (e.g., ship's position/location) may result in ship collision.	A newly built ship was delayed from sailing for many days as its ECDIS was infected by a virus [4].
11. Radio Detection and Ranging (RADAR) – RADAR is a mandatory equipment for navigation, used in identifying, tracking, positioning of vessels, and to safely navigate a ship from one point to another. Vessels depend on S-band and X-band frequency RADAR system for navigation as it can	• Network Switch • Server Message Block service	• Malware Intrusion • Man-in-the-middle (MITM) attack	• Malware may have the ability to alter the radar display by deleting targets on the display, essentially blinding the ship. • Due to the vulnerabilities in SMB service, attacker may be able to gain unauthorised access to the system and execute code without authentication.	Naval Dome ethical hackers successfully deleted radar targets in the vessel's radar screen, hence blindfolding the vessel [42].

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
detect targets and display the information on the screen.				
12. Automatic Identification System (AIS) – AIS is primarily designed to allow ships to see and be seen by marine traffic in its vicinity. AIS assists in obtaining specific information of the ships in a certain range, such as its name, speed, position, direction, rate of turn, destination, and physical parameters such as length, breadth, tonnage, beam, and draft, to neighboring ships and coastal authorities. AIS connects a standardised Very High Frequency (VHF) transceiver to a positioning system, such as a GPS receiver, as well as other electronic navigation sensors such as a gyrocompass or rate of turn indicator.	• AIS Software • AIS messages • VHF	• Spoofing • Replay attack (DoS) • Frequency hopping attack	• A spoofing attack can be done by initiating a fake terrestrial tower that broadcasts AIS data. For example, broadcasting details of a non-existent ship on a collision course may result in a CPA alert, which might force the vessel to divert from its path and actually collide with an obstruction or run aground. • An attacker can launch a replay attack by executing spoofed commands to delay the transmission time and resend it over and over causing a DoS attack. This can result in disabling the AIS display. • Port authorities provide specific instructions to the ship's AIS transponder to operate on a certain frequency. An attacker might be able to spoof such command to alter the frequency. Because of this frequency hopping attack, the ship will be unable to transmit or receive communications on the frequency, hence the vessel's details may not be visible on other ship's AIS display.	-

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
13. Global Positioning System (GPS) – The GPS is a crucial component that helps in determining accurate geographical locations for navigation. A GPS system comprises three systems: satellites, ground stations, and receivers. The GPS information is frequently replicated on other navigational equipment on the bridge, such as radars, automatic identification system, electronic navigation systems and communication systems, to aid in navigation.	• GPS receiver • GNSS frequencies	• GPS spoofing • GPS jamming	• An attacker can initiate a GPS spoofing attack by sending out fake GPS signals that are disguised as real signals. This will mislead the receiver into believing that its location is accurate, while in real, it is incorrect, as spoofed by the attacker. This attack may mislead ships to navigate wrongly and may also result in ship-to-ship and ship-to-land collisions. • Attacker can cause interference on signals from Global Navigation Satellite System (GNSS). The jamming signal will be significantly greater than the GPS signal hence preventing GPS reception. This will cause GPS to display erroneous positions and present misleading information in AIS and ECDIS.	A number of GPS spoofing incidents have been reported [73].
14. Dynamic Positioning System (DPS) – A Dynamic Positioning system is an automated computer-controlled system that maintains a vessel's position and heading by controlling its own propellers and thrusters. GNSS receiver and other Position reference sensors in addition to wind sensors, motion sensors, and	• GNSS receiver • DP system	• Denial of Service (DoS) attack • Spoofing • Backdoor attack	• Causing network storm on the Global Navigation Satellite System (GNSS) receiver to initiate a DoS attack will cause unavailability of DP system as it receives signals (position information) from GNSS receiver. • Spoofing involves transmitting false signals to GNSS receiver, which results in displaying wrong position information in the DPS display. This will cause the ship to change its	An incident was reported in 2015 where malware was mistakenly downloaded onto a Mobile Offshore Drilling Unit, which impacted the DP system [33].

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
gyro compasses, provide data to the computer about the vessel's position, the magnitude and direction of environmental forces impacting its position.			heading because of the misleading information in the DPS display. • Attacker can perform a backdoor attack to gain unauthorised access to the DP system by installing malware that can surpass normal authentication to access the system. This will result in attacker taking control over the system and misleading the operations.	
15. Global Maritime Distress and Safety System (GMDSS) – The Global Maritime Distress and Safety System (GMDSS) is a standard for usage of communication protocol, procedures and a safety equipment which can be utilised at the time of distress situation by the ship. The GMDSS sends a distress signal via satellite or radio communication equipment. It is used as a medium for transmitting and receiving marine safety information, and also as a general communication channel.	• VHF radio	• Spoofing • Eavesdropping • Denial-of-Service (DoS) attack	• Due to the broadcast nature of VHF, attacker can spoof the distress commands and deliver false information, hence causing confusion and delay in distress operations. • It may be possible for an attacker to intercept distress messages by eavesdropping on the signals, resulting in confidentiality breach. • If a malware infected application is present in the system, then it may initiate a DoS attack, hence disrupting the communication between the ships and ship-shore. Issues with transmitting and receiving messages may lead to loss of lives during a distress situation.	

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
16. Voyage Data Recorder (VDR) – The Voyage Data Recorder (VDR) is an equipment which functions similar to an aircraft's "black box" and is responsible for collecting and preserving all the relevant information about a ship such as the ship's speed, direction, position, status of ship systems, information about the engine, fuel, etc., which will be helpful during an accident investigation to examine what had happened to the ship and crew. Additionally, VDR includes a voice recording system that can save up to last 12 hours of information.	• USB ports • VDR system	• Malware attack • Remote code execution	• With the presence of USB port, malware can be injected through an infected USB drive, through which attacker may gain access to the data stored in VDR and tamper with, steal, or destroy it. • Due to the vulnerabilities in the services running on VDR, attackers can execute code with administrative (root) privileges, thus consequently have liberated access within the operating system, including tampering with the information stored in VDR.	In 2012, a crew member injected malware into VD through a USB pen drive, as a result of which data was destroyed [21].
17. Integrated Navigation System (INS) – Integrated Navigation System (INS) intensifies the operational efficiency and safety of ship's navigation by equipping a multifunctional display based on integration of at least two navigational functions. It is a software	• Server Message Block (SMB) Service • Remote desktop protocol	• Remote Code Execution • Man-in-the-middle (MITM) Attack	• Older version of SMB service may be subject to remote code execution. Attacker can exploit this vulnerability by executing malicious code without authentication and execute commands with root privileges and also tamper with sensitive information. • Due to the low encryption level in remote desktop protocol server (terminal service) running in the INS, an attacker can launch a	-

Navigation Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
platform which includes data from the ECDIS and RADAR systems, with sensors for other navigation functions.			MITM attack and gain unauthorised access to the system.	

Table 20 Cyber risks – Cargo Management Systems

Cargo Management Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
18. Cargo Control Room (CCR) – A cargo control room (CCR) is a place where the loading, unloading of cargo is controlled and monitored by a person in charge (PIC). The design and layout of a cargo control room can be determined based on the design of a ship, the requirements of owners and the capabilities of a particular shipyard. The CCR can be a separate room, or the controls can be placed on the ship's bridge. The PIC can control the loading/unloading of cargo, stripping pumps, check the valve positions and liquid levels in the cargo containers, through the equipment/system present in the CCR.	• Phishing emails • USB ports	• Ransomware • Malware attack	• If a malicious link is accessed or a malicious file is downloaded from email, then ransomware may spread and infect the cargo monitoring system and other devices in the vessel network. Hence all the devices will be encrypted and cannot be accessed unless a ransom is paid. • Malware can be infused in the cargo monitoring system by plugging an infected USB device into the USB port. Hence, attacker can access the system and steal or tamper with crucial cargo related information.	Somali criminals are reported to have a system that can breach a vessel's onboard container manifest to steal highly priced cargo [74]. In August 2011 hackers hacked into Iranian Shipping Line cargo system and manipulated cargo information, which caused the cargo to be lost or delivered to a wrong location [75].
19. Ballast Water System (BWS) – A Ballast Water System (BWS) is a separate compartment within a ship that stores water as ballast to offer stability to the ship. The use of water in such a tank will help in adjusting the weight of the ship in abnormal conditions. The system's operation also involves pumping out the ballast water for temporary reduction of the draft of the vessel when it enters	• USB ports • Phishing emails	• Malware attack • Phishing emails	• If malware is injected through USB ports in ballast water monitoring system, attacker may be able to control it and send false commands regarding the increase or decrease of the water level in the ballast compartment, hence causing the vessel to lose its stability and sink. • If the ballast water monitoring system is infected with malware	Naval Dome ethical hackers attacked the Machinery Control System (MCS) of a ship through an infected USB drive, and their first target was the ballast system. The attack caused the valves and pumps to dysfunction [21].

Cargo Management Systems				
OT sub-system(s)	**Attack surfaces**	**Cyber risks**	**Impacts of cyber risks**	**Cyber incidents**
shallow waters. The main components of ballast water system include level indication system, valve control system, main bilge system, water ingress alarm system.			(malicious URLs or attachments via phishing emails), then attacker may compromise the system and tamper with the functioning of the sensors, actuators, etc., and damage the tubes and other parts of the ballast water system.	

11.2 Appendix 2 – Mitigation Measures

Table 21 Mitigation measures - Communication Systems

Communication Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
1. Satellite Communication System (SATCOM) 2. Integrated Communication System (ICS)	Usage of weak or default credentials in the VSAT system leads to **unauthorised access of vessel network**, through which attacker can gain privileges such as **administrative access, FTP access and command-line access**, where one can view/edit confidential files and compromise systems.	• Firewall must be configured to allow only whitelisted sources or IP addresses within a subnet. • Virtual Private Network must be used while accessing the Internet. • IP is made private, and it should not be available on any public domain (e.g., Shodan). • OS, antivirus, firewall and other applications used in the business computer (The computer used for accessing emails, and VSAT modem's web interface) must be updated/patched regularly. • Access to the business computer should be restricted to authorised personnel with administrative login and strong credentials. • The default username and password in VSAT modem must be changed. Password should be strong - for example, password with 8 characters and at least one uppercase letter and one special character is recommended. • Password reset mechanisms should be implemented; it is recommended to change password once in three months. • Do not write down passwords in notebooks or sticky notes; a secure password manager application or a password protected PDF/Word document can be used to store passwords.

Communication Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
		• Access to the business computer must be blocked after a number of failed login attempts, e.g., 5 tries • It is good to have multi-factor authentication (MFA) for accessing the business computer and VSAT web interface. • FTP must be disabled in the VSAT modem's web interface.
	Phishing emails tend to deliver **malware** such as spyware, ransomware, viruses by tricking the victim to click on links or download files which cause unavailability of systems and information.	• Antivirus software must be installed in the business computers. • Files and email attachments downloaded from emails must be scanned with antivirus software to check for virus/malware. • Regular data backup must be done and stored safely. • Crew awareness must be established on the following: - Ability to distinguish phishing emails from the real ones - Be aware that emails from unknown sources should be viewed carefully and suspicious emails should not be opened - Be aware that they must not click on unknown links • Email security should be implemented– For example, S/MIME (Secure Multipurpose Internet *Mail* Extension) can be implemented to encrypt the email and ensure authenticity & integrity of the email.
	Hackers can get access to the vessel network by exploiting the vulnerabilities in **outdated VSAT software** resulting in disruption of day-to-day vessel operations and lack of communication between ship-shore.	• Latest version of software must be installed in the VSAT terminals. • Software updates must be checked regularly to fix vulnerabilities. • All updates must be logged. • If remote service/maintenance or an update is made, the authenticity of the vendor service, update and the remote desktop connection should be verified manually (e.g., phone call) before access can be permitted for the specified requirement.
	Usage of Weak protocols like HTTP, telnet leads to **eavesdropping.**	The terminal (VSAT) administration web interface should support secure protocols such as HTTPS, SSHv2.

Communication Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
	Cross-site scripting attack results in taking control over VSAT modem or hijacking the session by which an attacker can view, modify, and steal credentials affecting the operations of SATCOM.	The VSAT web interface should have inbuilt security mechanisms such as input sanitisation (any suspicious inputs must be rejected), output encoding, CSP (Content Security Policy) to protect against scripting attacks.
3. Voice Over Internet Protocol (VOIP)	Hackers can launch a **Denial-of-Service (DoS) attack** by flooding the VoIP network server with SIP call-signalling messages, which will slow down or stop the system traffic.	• Separate data traffic and voice traffic- Use a VLAN (Virtual Local Area Network)/Firewall dedicated for VOIP traffic. • The IT team must frequently monitor the VOIP network using Intrusion Detection Systems.
	Poor encryption/lack of encryption in the network – **Eavesdropping.**	• The VOIP traffic must be encrypted with a secure encryption standard.
	Vishing occurs when an attacker spoofs the caller ID and tricks recipients to provide sensitive data by pretending to be a legitimate source.	• The crew must know that they should not provide any personal details or vessel information if they receive calls from unknown sources.
4. Wireless Local Area Network (WLAN)	Hackers can launch a **Denial-of-Service (DoS) attack** by overwhelming the access point with fake requests, causing the network to slow down.	• Firewall must be configured to allow connection for whitelisted sources only. • The IT team must frequently monitor the network using Intrusion Detection Systems.
	Access point tampering can occur, if it is not placed safe.	• Routers/access points must be kept in a secured location such as a locked closet.
	Poor encryption/lack of encryption in the network leads to **eavesdropping/session hijacking.**	• A secure encryption standard must be used in wireless networks. As a minimum level of security, WEP (Wired Equivalent Privacy) must be used. Stronger encryption standards like WiFi Protected Access3 is recommended.

Table 22 Mitigation measures - Propulsion, Machinery and Power Control Systems

Propulsion, Machinery and Power Control Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
5. Fuel Oil System 6. Engine Governor System 7. Alarm Monitoring & Control System 8. Power Management System 9. Emergency Generators and Batteries	**Malware attack** via USB ports deliver malware in the machinery monitoring and control systems	• Antivirus software must be installed in the machinery control and monitoring systems. • Physical security measures must be implemented as follows: - Access control list for the crew to enter the engine control room or any other place where crucial machinery is present. - Access control list must be reviewed and updated regularly. • USB ports in the engine and fuel monitoring system, alarm monitoring & control system and power management system must be enabled only in admin login and disabled in other user logins (if any) and the system login credentials should have strong username and password. • USB port blockers should be used to block unused ports. • Dedicated charging points (ports) must be assigned for the crew. • USB cleaning station should be setup – A separate PC with antivirus software to scan the USB drives before use.
	Man-in-the-middle (MITM) attack – Tampering the serial communication network and misleading the communication between OT systems causing dysfunction	• SATCOM must be secured, as in Section 5.1. • Phishing email threat must be mitigated, as in Section 5.1. • OS, antivirus, and other applications in the engine and fuel monitoring system, alarm monitoring & control system and power management system must be updated frequently. • Crew access to the critical systems, and computers that control and monitor machinery must be regulated. • If remote service/maintenance is done on any of the systems, the authenticity of the vendor service and the remote desktop connection must be verified manually (e.g., phone call) and then access can be permitted. • OT network must be separated from the IT network by a DMZ/Firewall. • If a Serial-to-IP converter is used, it must support encryption, software updates must be done regularly, and credentials must be strong.

Table 23 Mitigation measures - Navigation systems

Navigation Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
10. Electronic Chart Display and Information System (ECDIS)	**Malware** can enter the system and disrupt operations, if a malware-infected USB drive is injected into the USB port.	• Antivirus software must be installed in the ECDIS system to scan any external media before connecting it to the system. • ECDIS chart updates must be logged. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use USB port blockers to avoid unnecessary plugins.
	An attacker may overload the network to perform **Denial-of-Service (DOS)** attack.	• Installing firewall in the ECDIS system will restrict unauthorised IP addresses from entering the vessel network • Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems.
	Spoofing the serial communication network can mislead the operations.	• Encryption across the NMEA network ensures that data is encrypted before transit and authenticated upon receipt. A secure Serial-to-IP converter that supports encryption & authentication can be used. • As Serial-to-IP converters have web interface for configuration, default username and password must be changed. • The converter device's software must be kept updated.
11. Radio Detection and Ranging (RADAR)	**Malware** can enter into RADAR via virus-laden emails and disrupt operations	• Antivirus software must be installed on captain's computer, which regularly connects to ECDIS for chart updates. This will refrain malware from spreading to the RADAR via ethernet switch connected to ECDIS. • Train crew to identify malicious or phishing emails.
	Man-in-the-middle (MITM) attack – results in unauthorised access of the system	• By enforcing the signing (security signatures) to the underlying operating system of SMB service, MITM attack can be mitigated. SMB signing places a digital signature into each server message block, which is used by both SMB clients and servers to prevent "man-in-the-middle" attacks and guarantee that SMB communications are not altered. • SMB signing available in Microsoft Windows Server 2003, Microsoft Windows XP, Microsoft Windows 2000, Windows NT 4.0, and Windows 98.

Navigation Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
12. Automatic Identification System (AIS)	**Spoofing** – Attacker transmits fake AIS data, causing collision	• AIS messages needs to be authenticated. • To distinguish between real and spoofed signals, there needs to be a way to directly determine the location of the transmission. For example, using a RFeye desktop application, transmissions can be geolocated by Time Difference on Arrival (TDoA). • The RFeye software outputs geolocation results as PoA (Power on Arrival) and TDOA probability heat maps and overlays real-time AoA (Angle of Arrival) vectors onto map interfaces.
	Replay attack – Attacker may repeatedly transmit spoofed commands to delay the message transmission time	• Timestamps must be monitored on all AIS messages to prevent hackers from resending recorded messages after a certain length of time, thus reducing the chances for attacker to eavesdrop the message and resend it.
	Frequency hopping attack – Attacker may tamper with the information regarding frequency of signals	• Integrity and authenticity of AIS messages should be assured. • PKI schema can be adopted in AIS protocol for RF communications. • X.509, a well-known PKI standard where digital certificates are issued by official national maritime authorities, that act as certification authorities and also configured in transponders with other stations identifiers (MMSI and call sign). X.509 authenticates messages exchanged between ships and with port authorities.
13. Global Positioning System (GPS)	**Spoofing** - An attacker can initiate a GPS spoofing attack by sending out fake GPS signals that are disguised as real signals	• GPS/GNSS receiver should detect spoofed signal from a mix of authentic and spoofed signals by using anti-spoofing techniques like absolute power monitoring, spatial processing.
	Jamming – Attacker may cause interference on GNSS signals	Usage of anti-jamming technique like spectrum monitoring enables GPS jammers to be detected and located by mobile direction-finding systems. Unintentional jamming can then be warned, and malicious attackers can be prosecuted.
14. Dynamic Positioning System (DPS)	Causing network storm on GNSS receiver results in **Denial-of-Service (DOS)** attack, leading to unavailability of DP system.	• Allowing and denying specific IPs: Allowing only legitimate IP addresses or blocking ones from known attackers. Installing firewall in the DPS system will allow only known IP addresses.

Navigation Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
		• Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems. • The DP control system software must be updated.
	Spoofing attack involves transmitting the false signals to GNSS receiver.	• GPS/GNSS receiver should detect spoofed signal from mix of authentic and spoofed signals by anti-spoofing techniques such as absolute power monitoring, spatial processing.
	An attacker can perform a **backdoor attack** to gain unauthorised access to the DP system by installing malware.	An advanced antivirus can detect and prevent malware and malicious attacks. Many backdoors are installed through malware, so it is essential to install an antivirus tool capable of detecting such threats.
15. Global Maritime Distress and Safety System (GMDSS)	**Spoofing** the distress commands can affect distress operations	• Messages exchanged between ships and with port authorities must be authenticated. • PKI schema can be adopted in GMDSS to ensure authenticity of messages exchanged. • Implementing email security such as S/MIME or DKIM can also be helpful if confidential information is passed via email.
	Eavesdropping – Confidentiality breach	The software and tools used in GMDSS system must be updated to avoid providing attackers with chances of exploiting vulnerabilities and downloading malware into the system through which they can eavesdrop.
	Denial-of-Service (DOS) attack casing unavailability of system	Use of firewall in GMDSS system will prevent DoS attack by allowing only known IP addresses.
16. Voyage Data Recorder (VDR)	**Malware attack-** Malware can be injected into VDR for unauthorised access to data	• Before inserting any external media into the VDR system, scan the media for virus/malware using antivirus software. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use port blockers to avoid unnecessary plugins. • Regular data backup (data recorded in the VDR) must be done and stored safely.
	Vulnerabilities in services running on VDR allow attackers for **remote code**	Most of the vessels uses older version of VDR (Furuno VR-3000 and VR-5000). Updated versions can help prevent remote code execution.

Navigation Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
	execution with administrator (root) privileges.	
17. Integrated Navigation System (INS)	Attacker can gain unauthorised access and control to the system through **Man-in-the-middle (MITM)** attack.	Remote desktop protocol server (terminal service) running on the INS is vulnerable to a man-in-the-middle attack due to low encryption level used. The vulnerability can be exploited by a remote attacker to gain access to the INS. This MITM attack can be prevented by operating system secure setup by forcing strong cryptography.
	Remote code execution- Attacker gains an unauthorized access to the system and **execute remote code.**	• Update the operating system with a security patch released by the manufacturer to prevent this attack. • **SMB 3.1.1** - the latest version of windows SMB - was released along with server 2016 and windows 10. **SMB 3.1.1** includes security enhancements such as enforcing secure connections with newer (SMB2 and later) clients and stronger encryption protocols.

Table 24 Mitigation measures - Cargo Management systems

Cargo Management Systems		
OT sub-system(s)	**Cyber risks**	**Mitigation measures**
18. Cargo Control Room (CCR)	**Ransomware** may spread via **phishing emails** and cause system unavailability	• Antivirus software must be installed in cargo control computer system to protect the system from virus laden emails. • Regular data backup must be done and stored safely. • Train crew to identify malicious or phishing emails. • Crew should not click on links from unknown sources or reveal personal or sensitive operational details in emails.
	Malware attack- Malware injected via USB ports in the cargo monitoring system can disrupt cargo operations	• Antivirus software must be installed in the computer system to scan any USB drives connects to the system. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use port blockers to avoid unnecessary plugins.
19. Ballast Water System (BWS)	**Malware attack-** Attacker may gain unauthorised access and control the increase or decrease of the water level in the ballast compartment	• It is critical that any external media is scanned for malware on a standalone system before being plugged into any shipboard network. Antivirus software helps in scanning any external media for malware before being plugged into the system. • USB ports must be disabled and only enabled by the captain of the ship whenever there is a need to use USB or enabled only in admin login and disabled in other user logins. • Use port blockers to avoid unnecessary plugins.
	Phishing emails trigger victim to download malicious content, hence resulting in system compromise.	• Antivirus software must be installed in the system to protect the system from phishing emails. • Regular data backup must be done and stored safely. • Train crew to identify malicious or phishing emails. • Crew should not click on links from unknown sources or reveal personal or sensitive operational details in emails.

11.3 Appendix 3 - Risk Score Evaluation

Table 25 Risk score evaluation - Communication Systems

Communication Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
1. Satellite Communication System (SATCOM) 2. Integrated Communication System (ICS)	Phishing emails	Phishing emails tend to deliver malware such as spyware, ransomware, viruses by tricking the victim to click on links or download files which causes unavailability of systems and information (4)	It is easy for attacker to send malicious URLs/files and it can be done from anywhere in the world (4)	**16**
	Outdated VSAT software	May result in unauthorised systems access. Attacker can get access to vessel network by exploiting the vulnerabilities resulting in disruption of day-to-day vessel operations and lack of communication between ship-shore (3)	Attacker can find out the vulnerabilities in old(er) version of software from resources published online and exploit them easily (3)	**9**
	Eavesdropping	By eavesdropping in the network, attacker can sniff credentials, sensitive information, insert unintended data, or hijack entire management session. This also results in loss of confidentiality (3)	Attacker can use packet sniffing tools with basic technical knowledge and sniff credentials, sensitive information, insert unintended data, or hijack entire management session. Attacker can find out about the vulnerabilities from resources published online (3)	**9**
	Cross-site scripting	This results in attacker taking control over VSAT modem or hijacking the session by which he/she can view, modify, and steal credentials affecting the operations of SATCOM (3)	Basic technical knowledge is enough to carry out the attack. Attacker can find out about the vulnerabilities in various VSAT versions from resources published online (3)	**9**
	unauthorised access of vessel network	Unauthorised access to vessel network (3)	If default/weak password is used, attacker can easily get into vessel network. Passwords	**12**

Communication Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
			may be available in public resources like Shodan. Attacker can perform brute force/dictionary attack if common or weak passwords are used (4)	
3. Voice Over Internet Protocol (VOIP)	Denial-of-Service (DoS) attack	Causes unavailability of network for communication, ship-to-shore communication link is disrupted (3)	An attacker can perform this attack from anywhere in the world with publicly available tools/software with basic technical knowledge. IPs may be published online (e.g., Shodan) (3)	**9**
	Vishing	Crew may give out sensitive ship information (1)	An attacker can perform this attack from anywhere in the world with publicly available tools, software, and online services with minimal technical knowledge (3)	**3**
	Eavesdropping	Loss of confidentiality/privacy. Hacker can find out personal and confidential information by unauthorised interception of vessel VOIP network (3)	Hacker can intercept the session with basic technical knowledge by using tools like Wireshark (3)	**9**
4. Wireless Local Area Network (WLAN)	Denial-of-Service (DoS) attack	Network unavailability, ship-to-shore communication link is disrupted (3)	Hacker can flood the target from anywhere with publicly available tools/software with basic technical knowledge. IPs may be published online (e.g., Shodan) (3)	**9**
	Access point tampering	Tampering the access point settings will change the configured functionality of it (2)	Possible that crew can do it intentionally/unintentionally and no technical knowledge is required (4)	**8**
	Eavesdropping/session hijacking	Loss of confidentiality. Hacker can steal credentials by unauthorised interception of vessel network (3)	Hacker can sniff on the session with well-known tools like Wireshark (3)	**9**

Table 26 Risk score evaluation - Propulsion, Machinery & Power Control Systems

Propulsion, Machinery & Power Control Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
5. Fuel Oil System 6. Engine Governor System 7. Alarm Monitoring & Control System	Malware attack (via USB ports)	Propulsion, machinery, and power control systems might dysfunction due to virus or other types of malware attacks via USB ports resulting in an explosion or any other physical damage (4)	The crew may inject malware via USB ports. No technical knowledge is required (4)	**16**
8. Power Management System 9. Emergency Generators and Batteries	Man-in-the-middle (MITM) attack	Impairs the normal functionality of systems by misleading the communication between OT systems e.g., tampering the fuel level, pressure, temperature, voltage level, alerts, etc. (2)	To tamper with the serial communication network, an attacker needs to gain remote access or physical access to engine control systems or machinery monitoring systems in the ship. A lot of technical knowledge is required since they need to find a way to get into the serial network (1)	**2**

Table 27 Risk score evaluation - Navigation Systems

Navigation Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
10. Electronic Chart Display and Information System (ECDIS)	Malware attack (via USB ports)	If navigation chart cannot be accessed due to unavailability of ECDIS, it may result in ship collision, leading to loss of life (4)	The crew may inject malware via USB ports. No technical knowledge is required (4)	**16**
	Denial-of-Service (DoS) attack	DoS attack will take ECDIS offline, hence impacting safe operation of vessel (4)	Hacker can flood the target from anywhere with publicly available tools/software with basic technical knowledge (3)	**12**

Navigation Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
	Spoofing	Tampering with the location information alters the ECDIS display resulting in collision of ship (4)	Due to lack of encryption & authentication of NMEA messages, attacker may spoof it, basic technical knowledge will suffice (3)	**12**
11. Radio Detection and Ranging (RADAR)	Malware intrusion	Attacker can take control over the system through malware and tamper with RADAR information, resulting in ship collision (4)	Attacker may intend to send virus-laden emails to the captain's computer (4)	**16**
	Man-in-the-middle (MITM) attack	Unauthorised access of the system due to vulnerabilities in the SMB service running in the system (3)	The vulnerabilities can be easily exploited by an attacker with basic technical knowledge (3)	**9**
12. Automatic Identification System (AIS)	Spoofing	Creation of a non-existent ship on a collision course might force the vessel to divert from its path and actually collide with an obstruction or run aground (4)	Due to lack of built-in security or authentication in the system, basic technical knowledge is enough to initiate this attack (3)	**12**
	Replay attack (DoS)	AIS display will stop working due to network exhaustion, hence system is unavailable (4)	Attacker needs to delay the transmission time of messages and repeat this over and over, moderate technical knowledge is required to perform this attack (2)	**8**
	Frequency hopping attack	Ship will be unable to send or receive signals if attacker alters the frequency, loss of communication (3)	With moderate technical knowledge and minor changes in exploits published online, attacker can tamper with the target frequency (2)	**6**
13. Global Positioning System (GPS)	GPS Spoofing	Misleading location information leads to ship collision, loss of life (4)	Attacker needs to send fake signals to GPS receiver. Basic technical knowledge is required (3)	**12**
	GPS Jamming	Impairs the normal functionality of the system, presenting erroneous information in GPS display (2)	Attacker can cause interference of signals on GNSS frequencies by using publicly available tools and resources (3)	**6**

Navigation Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
14. Dynamic Positioning System (DPS)	Denial-of-Service (DoS) attack	Unavailability of DP system due to DoS attack (4)	Attacker can flood the target from anywhere using publicly available tools/software with basic technical knowledge (3)	**12**
	Spoofing	Misleading heading, position information will force ship to change heading (2)	Attacker needs to send false signals to GNSS receiver. Basic technical knowledge is required (3)	**6**
	Backdoor attack	Using old version of software can allow attackers to gain unauthorised access to the system and deploy malware into the system, causing unavailability of systems and data (2)	Basic technical knowledge is enough to perform this attack as exploits, vulnerabilities in old versions of software are published online (3)	**6**
15. Global Maritime Distress and Safety System (GMDSS)	Spoofing	Deliver false information during distress, misleading the communication (2)	With basic technical knowledge and publicly available resources, attacker can spoof the commands (3)	**6**
	Eavesdropping	Eavesdropping on the communication - data breach (1)	Hacker can eavesdrop with basic technical knowledge by using tools like Wireshark (3)	**3**
	Denial-of-Service (DoS) attack	Disrupting the communication between the ships and ship-shore (3)	Attacker may make use of vulnerable applications running in the system to initiate DoS attack, needs moderate technical knowledge (2)	**6**
16. Voyage Data Recorder (VDR)	Remote code execution	Attacker can gain root privileges and delete radar images & conversations, causing lack of data (2)	Due to the vulnerabilities in VDR, attacker with moderate technical knowledge can perform this attack (2)	**4**
	Malware attack (via USB ports)	Steal or destroy the data – data breach (1)	The crew may inject malware via USB ports. No technical knowledge is required (4)	**4**
17. Integrated Navigation System (INS)	Man-in-the-middle (MITM) attack	Attacker can gain unauthorised access to the system and tamper with communication	Due to low encryption level in remote desktop protocol service, with minor changes	**6**

Navigation Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
		between devices, troubling ship's navigation (3)	in exploits published online attacker can perform this attack (2)	
	Remote code execution	If an older version of terminal service (SMB) is in use, attacker can take control over the system with admin privileges and cause unavailability of systems and data (2)	With basic technical knowledge and no change in exploits published online, attacker injects the malicious code into the system (3)	**6**

Table 28 Risk score evaluation - Cargo Management Systems

Cargo Management Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
18. Cargo Control Room (CCR)	Ransomware (via phishing emails)	Ransomware will spread and infect the cargo monitoring system hence the device will be encrypted and cannot be accessed unless a ransom is paid (4)	It is easy for attacker to send malicious URLs/files and it can be done from anywhere (4)	**16**
	Malware attack (via USB ports)	Attacker can gain unauthorised access to the cargo monitoring system by injecting malware (via USB), through which attacker can view, tamper with cargo related data, troubling the cargo operations (e.g., steal data or tamper cargo delivery location) (3)	The crew may inject malware via USB ports. No technical knowledge is required (4)	**12**
19. Ballast Water System (BWS)	Malware attack (via USB ports)	If malware is injected through USB ports in the system, attacker may input wrong commands regarding the increase or decrease of the water level in the ballast compartment, causing the vessel to lose its stability and sink, also lead to loss of lives (4)	The crew may inject malware via USB ports. No technical knowledge is required (4)	**16**

Cargo Management Systems				
OT sub-system(s)	**Cyber risks**	**Severity (score)**	**Likelihood (score)**	**Risk score**
	Phishing emails	If the system is infected with malware, then attacker may compromise and tamper with the functionality of the ballast water system, causing imbalance of ship, loss of life (4)	It is easy for attacker to send malicious URLs/files and it can be done from anywhere (4)	**16**


iTrust
Centre for Research
in Cyber Security