



財團法人驗船中心

CR CLASSIFICATION SOCIETY

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS

CR CLASSIFICATION SOCIETY

December 2025

GUIDELINES FOR CYBER SECURITY

ONBOARD SHIPS

PART I CYBER SECURITY MANAGEMENT SYSTEM ONBOARD SHIPS

PART II CYBER RESILIENCE OF SHIPS

PART III CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT



財團法人驗船中心

CR CLASSIFICATION SOCIETY

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS

PART I – CYBER SECURITY MANAGEMENT SYSTEM

ONBOARD SHIPS

CR CLASSIFICATION SOCIETY

December 2025

REVISION HISTORY

(This version supersedes all previous ones.)

Revision No.	Editor	Date (yyyy-mm)
001	Rules Section	2020-09
002	Rules Section	2025-12

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS
PART I – CYBER SECURITY MANAGEMENT SYSTEM
ONBOARD SHIPS

CONTENTS

Chapter 1	General	1
1.1	Introduction.....	1
1.2	Application.....	2
1.3	Best Practices for Implementation of Cyber Risk Management	2
1.4	Definition.....	3
Chapter 2	Cyber Security and Safety Management.....	6
2.1	General.....	6
2.2	Plans and Procedures	6
2.3	Key Aspects of Cyber Security	7
2.4	Defence in Depth and in Breadth.....	8
Chapter 3	Identify Threats	9
3.1	Circumstances.....	9
3.2	Examples of Cyber Threats.....	9
3.3	Types of Cyber Attack	10
3.4	Stages of a Cyber Attack.....	11
Chapter 4	Identify Vulnerabilities.....	13
4.1	Assessment of Potential Threats	13
4.2	Onboard Systems	13
4.3	Ship to Shore Interface.....	14
4.4	Common Vulnerabilities	15
Chapter 5	Assess Risk Exposure	16
5.1	Overview.....	16
5.2	Risk Assessment Made by the Company	20
5.3	Third-Party Risk Assessments	21
5.4	Risk Assessment Process	21

Chapter 6	Develop Protection and Detection Measures.....	24
6.1	General.....	24
6.2	CIS Technical Protection Measures	25
6.3	ISO/IEC 27001	27
6.4	IACS Rec. No. 166	31
6.5	Procedural Protection Measures.....	31
Chapter 7	Establish Contingency Plans	35
7.1	Attention of Developing The Plan	35
Chapter 8	Respond to and Recover from Cyber Security Incidents.....	36
8.1	General.....	36
8.2	Effective Response.....	36
8.3	Recovery Plan.....	37
8.4	Investigating Cyber Incidents	37
8.5	Losses Arising From a Cyber Incident.....	37
Chapter 9	Audit.....	39
9.1	Type of Audit	39
9.2	Timing of Audits	39
9.3	Initial Audit.....	39
9.4	Renewal Audit.....	40
9.5	Annual Audit.....	41
9.6	Occasional Audits	41
Annex 1	Target Systems, Equipment and Technologies.....	42
A1.1	Communication Systems	42
A1.2	Bridge Systems	42
A1.3	Propulsion and Machinery Management and Power Control Systems	42
A1.4	Access Control Systems.....	43
A1.5	Cargo Management Systems.....	43
A1.6	Passenger Servicing and Management Systems.....	43
A1.7	Passenger-Facing Networks.....	43
A1.8	Core infrastructure systems.....	44
A1.9	Administrative and Crew Welfare Systems.....	44
Annex 2	Onboard Networks	45
A2.1	Physical Layout.....	45

A2.2 Network Management..... 45
A2.3 Network Segmentation..... 45
A2.4 Monitoring Data Activity 46
A2.5 Secure Running Environment 47

Annex 3 Cyber Risk Management and the Safety Management System 48

A3.1 Identify..... 48
A3.2 Protect..... 49
A3.3 Detect..... 51
A3.4 Respond 51
A3.5 Recovery 52

Chapter 1 General

1.1 Introduction

Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together and more frequently connected to the internet.

This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media. In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. It further encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. The same year, IMO developed guidelines¹ that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. As also highlighted in the IMO guidelines, effective cyber risk management should start at the senior management level.

Senior management should embed a culture of cyber risk awareness into all levels and departments of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

1.1.1 MSC.428(98)

Recognizing the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks.

Encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021

1.1.2 ISM (International Safety Management) Code 1.2.2

Safety management objectives of the Company should, inter alia [...] assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards.

1.1.3 ISPS (International Ship and Port Facility Security) Code Part B, 8.3

A Ship Security Assessment (SSA) should address the important elements including radio and telecommunication systems, as well as computer systems and networks, on board or within the ship.

1.1.4 MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management

- (a) Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.
- (b) Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

¹ MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management.

- (c) Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organisation and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.
- (d) Vulnerabilities created by accessing, interconnecting or networking numerous systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to systems list in 3.2.

1.1.5 More guidance on how to incorporate cyber risk management into the company's SMS can be found in Annex 3.

1.2 Application

The Guidelines for Cyber Security Onboard Ships **Part I** are intended to offer guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard the ships. In addition, **this Part** are intended to help IT and industrial automation control system professionals to join their efforts towards building and maintaining cyber security resilience of the total set of the assets and processes employed to conduct the company's business.

This Part are not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual company's and ship's approach to cyber risk management.

1.2.1 Approaches to cyber security will be company- and ship-specific, but should be guided by appropriate standards and the requirements of relevant national, international and flag state regulations. **This Part** provide a risk-based approach to identifying and responding to cyber threats. Following a risk based approach, the decisions of what is critical and high priority is then left at the discretion of the organisation. An important aspect is that relevant personnel should have training in identifying the typical modus operandi of cyber attacks.

1.2.2 Different members of the management team might have different exposure and levels of responsibility towards cyber security. Depending on different needs and organization size, the security level may differ from high level management, basic capabilities to comprehensive, very technical in depth. Assessment, protection, as well as improvement activities can be scaled accordingly.

1.2.3 Class notation

For ship complying with the requirements of **this Part**, the class notation **Cyber-S** will be assigned to the ship. Any suffix and description may be added in the curly bracket after the notation, e.g.: "**Cyber-S{...}**".

1.3 Best Practices for Implementation of Cyber Risk Management

1.3.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of **this Part** should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.3.2 Additional guidance and standards may include, but are not limited to:

(a) NIST framework

United States National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. NIST aims to help understand, manage and express cyber security risks both internally and externally, for example within a ship's organisation. It can help to identify and prioritise actions

for reducing cyber security risks. It is also a tool for aligning policy, business and technological approaches to manage the risks.

(b) CIS Controls

The Centre for Internet Security (CIS) provides guidance on measures¹¹ that can be used to address cyber security vulnerabilities. The protection measures are a list of Critical Security Controls (CSC) that are prioritised and vetted to help ensure that they provide an effective approach for companies to assess and improve their defences. The CSCs include both technical and procedural aspects.

(c) ISO/IEC 27001, CNS 27001

Standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Certification to this standard involves the revised 93 controls listed in Annex A of ISO/IEC 27001 and CNS 27001, which aim to combine secure architecture, preventive, and detective control measures. These controls are reclassified into four main themes:

- (1) Organizational Controls
- (2) People Controls
- (3) Physical Controls
- (4) Technological Controls

(d) IACS Rec. No. 166

Recommendation on Cyber Resilience, which consolidates IACS' previous 12 Recommendations related to cyber resilience (Nos. 153 to 164) and applies to the use of computer-based systems which provide control, alarm, monitoring, safety or internal communication functions, and provides:

- (1) guidance for mitigating the risk related to events affecting onboard computer-based systems, and
- (2) goals for design and construction, functional requirements, technical requirements and verification testing.

1.3.3 Reference should be made to the most current version of any guidance or standards utilized.

1.4 Definition

1.4.1 Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

1.4.2 Back door is a secret method of bypassing normal authentication and verification when accessing a system. A back door is sometimes created by hidden parts of the system itself or established by separate software.

1.4.3 Bring your own device (BYOD): allows employees to bring personally owned devices (laptops, tablets, and smart phones) to the ship and to use those devices to access privileged information and applications for business use.

1.4.4 Cyber attack is any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data.

1.4.5 Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

1.4.6 Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits of actions taken by stakeholders.

1.4.7 Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.

1.4.8 Defence in breadth is a planned, systematic set of activities that seek to identify, manage, and reduce exploitable vulnerabilities in IT and OT systems, networks and equipment at every stage of the system, network, or sub-component life cycle. Onboard ships this approach will generally focus on network design, system integration, operations and maintenance.

1.4.9 Defence in depth is an approach which uses layers of independent technical and procedural protection measures to protect IT and OT on board.

1.4.10 Executable software includes instructions for a computer to perform specified tasks according to encoded instructions.

1.4.11 Firewall is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.

1.4.12 Firmware is software imbedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems. They are normally self-contained and not accessible to user manipulation.

1.4.13 Flaw is unintended functionality in software.

1.4.14 Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

1.4.15 Intrusion Prevention Systems (IPSs), also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity.

1.4.16 Information technology (IT) is the use of computers to store, retrieve, transmit, and manipulate data, or information, including all hardware, software and peripheral equipment.

1.4.17 Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.

1.4.18 Malware is a generic term for a variety of malicious software which can infect computer systems and impact on their performance.

1.4.19 Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems.

1.4.20 Patches are software designed to update software or supporting data to improve the software or address security vulnerabilities and other bugs in operating systems or applications.

1.4.21 Phishing refers to the process of deceiving recipients into sharing sensitive information with a third-party.

1.4.22 Principle of least privilege refers to the restriction of user account privileges only to those with privileges that are essential to perform its intended function.

1.4.23 Producer is the entity that manufactures the shipboard equipment and associated software.

1.4.24 Recovery refers to the activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

1.4.25 Removable media is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs and diskettes.

1.4.26 Risk assessment is the process which collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.

1.4.27 Risk management is the process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

1.4.28 Sandbox is an isolated environment, in which a program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.

1.4.29 Service provider is a company or person who provides and performs software maintenance.

1.4.30 Social engineering is a method used to gain access to systems by tricking a human into revealing confidential information.

1.4.31 Software whitelisting means specifying the software which may be present and active on an IT or OT system.

1.4.32 Virtual Local Area Network (VLAN) is the logical grouping of network nodes. A virtual LAN allows geographically dispersed network nodes to communicate as if they were physically on the same network.

1.4.33 Virtual Private Network (VPN) enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network.

1.4.34 Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

1.4.35 Wi-Fi is all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

Chapter 2 Cyber Security and Safety Management

2.1 General

2.1.1 Both cyber security and cyber safety are important because of their potential effect on personnel, the ship, environment, company and cargo. Cyber security is concerned with the protection of IT, OT, information and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

2.1.2 Cyber safety incidents can arise as the result of:

- (a) a cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS);
- (b) a failure occurring during software maintenance and patching;
- (c) loss of or manipulation of external sensor data, critical for the operation of a ship. This includes but is not limited to Global Navigation Satellite Systems (GNSS).

2.1.3 Whilst the causes of a cyber safety incident may be different from a cyber security incident, the effective response to both is based upon training and awareness.

2.2 Plans and Procedures

2.2.1 Company plans and procedures for cyber risk management should be complementary to the existing security and safety risk management requirements contained in the ISM Code² and ISPS Code³. Cyber security should be considered at all levels of the company, from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship.

2.2.2 In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect. The assessment should address radio and telecommunication systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring “the ship to shore” path of the internet connection, which is important owing to the fast adoption of sophisticated and digitalised onboard OT systems that in many cases have not been designed to be cyber resilient.

2.2.3 The objective of the company's Safety Management System (SMS) is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. In the context of ship operations, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents.

2.2.4 The SMS should include instructions and procedures to ensure the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. These instructions and procedures should consider risks arising from the use of IT and OT on board, as appropriate, taking into account applicable codes, guidelines and recommended standards.

² International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code).

³ International Ship and Port Facility Security Code (ISPS Code).

2.2.5 When incorporating cyber risk management into the company SMS, consideration should be given to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. This should consider factors, including but not limited to the extent to which IT and OT is used on board, the complexity of system integration and the nature of operations.

2.2.6 Cyber risk management should

- (a) identify the roles and responsibilities of users, key personnel, and management both ashore and on board;
- (b) identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety;
- (c) implement technical measures to protect against a cyber incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software
- (d) implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal;
- (e) implement activities to prepare for and respond to cyber incidents.

2.2.7 In recognising that some aspects of work to include cyber risk management in safety management systems may include commercially sensitive or confidential information, companies should consider protecting this information appropriately. As far as possible, policies and procedures included in a safety management system should not include sensitive information like this.

2.3 Key Aspects of Cyber Security

The development, understanding and awareness of key aspects of cyber security and safety are list as below:

2.3.1 Identify threats

Understand the external cyber security threats to the ship. Understand the internal cyber security threat posed by inappropriate use and lack of awareness.

2.3.2 Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cyber security threat on these systems. Understand the capabilities and limitations of existing protection measures.

2.3.3 Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats. Determine the likelihood of vulnerabilities being exposed by inappropriate use. Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

2.3.4 Develop protection and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures. Reduce the potential impact of a vulnerability being exploited.

2.3.5 Establish contingency plans

Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.

2.3.6 Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents that are realised using the response plan. Assess the impact of the effectiveness of the response plan and reassess threats and vulnerabilities.

2.4 Defence in Depth and in Breadth

2.4.1 Using more than one technical or procedural protection measure is recommended. It is essential to protect critical systems and data with multiple layers of protection measures which take into account the role of personnel, procedures and technology to:

- (a) increase the probability that a cyber incident is detected;
- (b) increase the effort and resources required to protect information, data or the availability of IT and OT systems.

2.4.2 This defence in depth approach encourages a combination of:

- (a) physical security of the ship in accordance with the ship security plan (SSP);
- (b) protection of networks, including effective segmentation;
- (c) intrusion detection;
- (d) software whitelisting;
- (e) access and user controls;
- (f) appropriate procedures regarding the use of removable media and password policies;
- (g) personnel's awareness of the risk and familiarity with appropriate procedures.

2.4.3 Company policies and procedures should ensure that cyber security is considered within the overall approach to safety and security risk management. The complexity and potential persistence of cyber threats means that a “defence in depth” approach should be considered. Equipment and data protected by layers of protection measures are more resilient to cyber attacks.

2.4.4 However, onboard ships where levels of integration between cyber systems may be high, defence in depth only works if technical and procedural protection measures are applied in layers across all vulnerable and integrated systems. This is “defence in breadth” and it is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

2.4.5 Defence in depth and defence in breadth are complementary approaches which, when implemented together, provide the foundation of a holistic response to the management of cyber risks.

Chapter 3 Identify Threats

3.1 Circumstances

3.1.1 The cyber risk⁴ is specific to the company, ship, operation and/or trade. When assessing the risk, companies should be aware of any specific aspects of their operations that might increase their vulnerability to cyber incidents.

3.1.2 Unlike other areas of safety and security where historic evidence is available and reporting of incidents is required, cyber security is made more challenging by the absence of any definitive information about the incidents and their impact. Until this evidence is obtained, the scale and frequency of attacks will continue to be unknown.

3.1.3 Experiences from other business sectors such as financial institutions, public administration and air transport have shown that successful cyber attacks might result in a significant loss of services, assets and even endanger human lives. Such events argue that the shipping industry should also work proactively to understand and mitigate cyber threats.

3.2 Examples of Cyber Threats

3.2.1 There are motives for organisations and individuals to exploit cyber vulnerabilities. The following examples give some indication of the threat posed and the potential consequences for companies and the ships they operate:

Table I 3-1 Motivation and objectives

Group	Motivation	Objective
Activists (including disgruntled employees)	<ul style="list-style-type: none"> • Reputational damage • Disruption of operations 	<ul style="list-style-type: none"> • Destruction of data • Publication of sensitive data • Media attention • Denial of access to the service or system targeted
Criminals	<ul style="list-style-type: none"> • Financial gain • Commercial espionage • Industrial espionage 	<ul style="list-style-type: none"> • Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo • Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc
Opportunists	<ul style="list-style-type: none"> • The challenge 	<ul style="list-style-type: none"> • Getting through cyber security defences • Financial gain
States State sponsored organizations Terrorists	<ul style="list-style-type: none"> • Political gain • Espionage 	<ul style="list-style-type: none"> • Gaining knowledge • Disruption to economies and critical national infrastructure

3.2.2 The groups in Table I 3-1 are active and have the skills and resources to threaten the safety and security of ships, and a company's ability to conduct its business.

3.2.3 In addition, there is the possibility that company personnel, on board and ashore, could compromise cyber systems and data. In general, the company should be prepared that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures.

⁴ The text in this chapter has been summarised from CESG, Common Cyber Attacks: Reducing the Impact.

3.2.4 There is, however, the possibility that actions may be malicious and are a deliberate attempt to damage the company and the ship that is by a disgruntled employee.

3.3 Types of Cyber Attack⁵

3.3.1 Categories of cyber attacks:

In general, there are two categories of cyber attacks, which may affect companies and ships:

- (a) Untargeted attacks, where a company or a ship's systems and data are one of many potential targets;
- (b) Targeted attacks, where a company or a ship's systems and data are the intended target.

3.3.2 Untargeted attacks

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate, discover and exploit widespread vulnerabilities which may also exist in a company and onboard a ship. Examples of some tools and techniques that may be used in these circumstances include:

(a) Malware:

Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including trojans, ransomware, spyware, viruses, and worms. Ransomware encrypts data on systems until a ransom has been paid. Malware may also exploit known deficiencies and problems in outdated/unpatched business software. The term exploit usually refers to the use of a software or code, which is designed to take advantage and manipulate a problem in another computer software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction, and error in protocol implementation. These vulnerabilities may be exploited remotely or triggered locally. Locally, a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.

(b) Social engineering:

A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

(c) Phishing:

Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.

(d) Water holing:

Establishing a fake website or compromising a genuine website to exploit visitors.

(e) Scanning:

Attacking large portions of the internet at random.

3.3.3 Targeted attacks

⁵ In 2016, IHS Markit together with BIMCO carried out a cyber security survey. The respondent from the shipping industry had experienced the mentioned forms of attacks. Four percent of the attacks were directed at ship borne systems.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. Examples of tools and techniques which may be used in these circumstances include:

- (a) Brute force:
An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.
- (b) Denial of service (DoS):
DoS prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.
- (c) Spear-phishing:
Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.
- (d) Subverting the supply chain
Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

3.3.4 The above examples are not exhaustive. Other methods are evolving for example impersonating a legitimate shore based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyber attacks continue to evolve and are limited only by the ingenuity of those organisations and individuals developing them.

3.4 Stages of a Cyber Attack

Cyber attacks are conducted in stages. The length of time taken to prepare a cyber attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those onboard its ships. The four stages of an attack are:

3.4.1 Survey/reconnaissance

Open/public sources used to gain information about a company, ship or seafarer, which can be used to prepare for a cyber attack. Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring (analysing – sniffing) the actual data flowing into and from a company or a ship.

3.4.2 Delivery

Attackers may attempt to access company and ship systems and data. This may be done from either within the company or ship or remotely through connectivity with the internet. Examples of methods used to obtain access include:

- (a) company online services, including cargo or consignment tracking systems;
- (b) sending emails containing malicious files or links to malicious websites to personnel;
- (c) providing infected removable media, for example as part of a software update to an onboard system;

- (d) creating false or misleading websites which encourage the disclosure of user account information by personnel.

3.4.3 Breach

The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack. It should be noted that a breach might not result in any obvious changes to the status of the equipment. Depending on the significance of the breach, an attacker may be able to:

- (a) make changes that affect the system's operation, for example interrupt or manipulate information used by navigation equipment;
- (b) gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists;
- (c) achieve full control of a system, for example a machinery management system.

3.4.4 Effect

The motivation and objectives of the attacker will determine what effect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

- (a) access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;
- (b) manipulate crew or passenger lists, or cargo manifests. this may be used to allow the fraudulent transport of illegal cargo, or facilitate thefts;
- (c) cause complete denial of service on business systems;
- (d) enable other forms of crime for example piracy, theft and fraud;
- (e) disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.

It is crucial that users of IT systems onboard ships are aware of the potential cyber security risks, and are trained to identify and mitigate such risks.

Chapter 4 Identify Vulnerabilities

4.1 Assessment of Potential Threats

4.1.1 It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced. This should be followed by an assessment of the systems and onboard procedures to map their robustness to handle the current level of threat. These vulnerability assessments should then serve as the foundation for a senior management level discussion/workshop. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centred around the key risks. The distinction between IT and OT systems should be considered. IT systems focus on the use of data as information whilst OT systems focus on the use of data to control or monitor physical processes.

4.1.2 Stand-alone systems will be less vulnerable to external cyber attacks compared to those attached to uncontrolled networks or directly to the internet. Network design and network segregation will be explained in more detail in Annex 2. Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel's actions.

4.2 Onboard Systems

Onboard systems could include:

4.2.1 Cargo management systems:

Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore. Such systems may include shipment-tracking tools available to shippers via the internet. Interfaces of this kind make cargo management systems and data in cargo manifests vulnerable to cyber attacks.

4.2.2 Bridge systems:

The increasing use of digital, network navigation systems, with interfaces to shoreside networks for update and provision of services, make such systems vulnerable to cyber attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks. A cyber incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

4.2.3 Propulsion and machinery management and power control systems:

The use of digital systems to monitor and control onboard machinery, propulsion and steering make such systems vulnerable to cyber attacks. The vulnerability of these systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

4.2.4 Access control systems:

Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic "personnel-on-board" systems.

4.2.5 Passenger servicing and management systems:

Digital systems used for property management, boarding and access control may hold valuable passenger related data. Intelligent devices (tablets, handheld scanners etc.) are themselves an attack vector as ultimately the collected data is passed on to other systems.

4.2.6 Passenger facing public networks:

Fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems. These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

4.2.7 Administrative and crew welfare systems:

Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email. They can be exploited by cyber attackers to gain access to onboard systems and data. These systems should be considered uncontrolled and should not be connected to any safety critical system on board. Software provided by ship management companies or owners is also included in this category.

4.2.8 Communication systems:

Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data.

The above-mentioned onboard systems consist of potentially vulnerable equipment which should be reviewed during the assessment. More detail can be found in Annex 1.

4.3 Ship to Shore Interface

4.3.1 Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Further, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as:

- (a) engine performance monitoring;
- (b) maintenance and spare parts management;
- (c) cargo, crane and pump management;
- (d) voyage performance monitoring.

4.3.2 The above list provides examples of this interface and is not exhaustive. The above systems provide data which may be of interest to cyber criminals to exploit.

4.3.3 Modern technologies can add vulnerabilities to the ships especially if there are insecure designs of networks and uncontrolled access to the internet. Additionally, shoreside and onboard personnel may be unaware how some equipment producers maintain remote access to shipboard equipment and its network system. The risks of misunderstood, unknown, and uncoordinated remote access to an operating ship should be taken into consideration as an important part of the risk assessment.

4.3.4 It is recommended that companies should fully understand the ship's OT and IT systems and how these systems connect and integrate with the shore side. This requires an understanding of all computer based onboard systems and how safety, operations, and business can be compromised by a cyber incident.

4.3.5 The following should be considered regarding producers and third parties including contractors and service providers:

- (a) The producer's and service provider's cyber security awareness and procedures: Many of these companies lack cyber awareness training and governance in their own organisations and this may represent more sources of vulnerability, which could result in cyber incidents. The companies should have an updated cyber security company policy, which includes training and governance procedures for accessible IT and OT onboard systems.
- (b) The maturity of a third-party's cyber security procedures: The shipowner should query the internal governance for cyber network security, and seek to obtain a cyber security assurance when considering future contracts and services. This is particularly important when covering network security if the ship is to be interfaced with the third-party.

4.4 Common Vulnerabilities

4.4.1 The following are common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships:

- (a) Obsolete and unsupported operating systems.
- (b) Outdated or missing antivirus software and protection from malware.
- (c) Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege.
- (d) Shipboard computer networks, which lack boundary protection measures and segmentation of networks.
- (e) Safety critical equipment or systems always connected with the shore side.
- (f) Inadequate access controls for third parties including contractors and service providers.

Chapter 5 Assess Risk Exposure

5.1 Overview

5.1.1 Accountability and ownership for cyber security assessment should start at senior management level of a company, instead of being immediately delegated to the ship security officer or the head of the IT department. There are several reasons for this:

- (a) Initiatives to heighten cyber security may at the same time affect standard business procedures and operations, rendering them more time consuming or costly. It is therefore a senior management level strategic responsibility to evaluate and decide on risk versus reward trade-offs.
- (b) A number of initiatives which would heighten cyber security are related to business processes and training, and not to IT systems, and therefore need to be anchored organisationally outside the IT department.
- (c) Initiatives which heighten cyber security awareness may change how the company interacts with customers, suppliers and authorities, and impose new requirements on the co-operation between the parties. It is a senior management level decision whether and how to drive changes in these relationships.
- (d) Only when the above three aspects have been decided upon will it be possible to clearly outline what the IT requirements of the cyber security strategy will be, and this is the element which can be placed with the IT department.
- (e) Based on the strategic decisions in general, and the risk versus reward trade-offs, relevant contingency plans should be established in relation to handling cyber incidents if they should occur.

Senior management should realise their leadership responsibilities by delegating authority and allocating the budget needed to carry out the risk assessment and to develop solutions that are best suit for the company and the operation of their ships.

5.1.2 The level of cyber risk will reflect the circumstances of the company, ship (its operation and trade), the IT and OT systems used, and the information and/or data stored. The maritime industry possesses a range of characteristics which affect its vulnerability to cyber incidents:

- (a) the cyber controls already implemented by the company and onboard its ships;
- (b) multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure;
- (c) the ship being online and how it interfaces with other parts of the global supply chain;
- (d) ship equipment being remotely monitored eg by the producers;
- (e) business-critical, data sensitive and commercially sensitive information shared with shore-based service providers;

- (f) the availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

These elements should be considered, and relevant parts incorporated into the company security policies, safety management systems, and ship security plans. Users of **this Part** should refer to specific national legislation and flag state requirements as well as relevant international and industry standards and best practices when developing and implementing cyber risk management procedures.

IT and OT systems, software and maintenance can be outsourced to third-party service providers and the company itself may not possess a way of verifying the level of security supplied by these providers. Some companies use different providers responsible for software and cyber security checks.

The growing use of big data, smart ships and the "internet of things"⁶ will increase the amount of information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber security important both now and in the future.

5.1.3 Third-party access

Visits to ships by third parties requiring a connection to one or more computers on board can also result in connecting the ship to shore. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. Some technicians may require the use of removable media to update computers, download data and/or perform other tasks. It has also been known for customs officials and port state control officers to board a ship and request the use of a computer to "print official documents" after first inserting an unknown removable media.

Some IT and OT systems are remotely accessible and may operate with a continuous internet connection for remote monitoring, data collection, maintenance functions, safety and security. These systems can be "third-party systems", whereby the contractor monitors and maintains the systems from a remote access. These systems could include both two-way data flow and upload-only. Systems and work stations with remote control, access or configuration functions could, for example, be:

- (a) bridge and engine room computers and work stations on the ship's administrative network;
- (b) cargo such as containers with reefer temperature control systems or specialised cargo that are tracked remotely;
- (c) stability decision support systems;
- (d) hull stress monitoring systems;
- (e) navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP);
- (f) cargo handling, engine, and cargo management systems;
- (g) safety and security networks, such as CCTV (closed circuit television);

⁶ Lloyd's Register, Qinetiq and University of Southampton, Global Marine Technology Trends 2030.

- (h) specialised systems such as drilling operations, blow out preventers, subsea installation systems, Emergency Shut Down (ESD) for gas tankers, submarine cable installation and repair.

The extent and nature of connectivity of equipment should be known by the shipowner or operator and documented as part of the risk assessment.

5.1.4 Impact assessment

The confidentiality, integrity and availability (CIA) model⁷ provides a framework for assessing the impact of:

- (a) unauthorised access to and disclosure of information or data about the ship, crew, cargo and passengers;
- (b) loss of integrity, which would modify or destroy information and data relating to the safe and efficient operation and administration of the ship;
- (c) loss of availability due to the destruction of the information and data and/or the disruption to services/operation of ship systems.

The relative importance of confidentiality, integrity and availability (CIA) changes depending on the use of the information or data. For example, assessing the vulnerability of IT systems related to commercial operations may focus on confidentiality and integrity rather than availability. Conversely, assessing the vulnerability of OT systems onboard ships, particularly safety critical systems, may focus on availability and/or integrity instead of confidentiality.

⁷ Federal Information Processing Standards, Publication 199, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900.

Table I 5-1 Potential impact levels when using the CIA model

Potential impact	Definition	In practice
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organizational assets, or individuals	A limited adverse effect means that a security breach might: <ul style="list-style-type: none"> (i) cause a degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, company and ship assets, or individuals	A substantial adverse effect means that a security breach might: <ul style="list-style-type: none"> (i) cause a significant degradation in ship operation to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, company and ship assets, or individuals.	A severe or catastrophic adverse effect means that a security breach might: <ul style="list-style-type: none"> (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life- threatening injuries.

Sensitive information may include ship position, status of and readout from OT systems, cargo details, authorisations, certificates, etc. When it comes to OT systems it is important consider what impact the loss or malfunction of the system will have following a cyber incident.

5.1.5 Example

(a) Identify critical systems:

A power management system contains a supervisory control and data acquisition (SCADA) system controlling the distribution of onboard electric power. The system contains real-time sensor data which is used on board for power management. It also generates data about the power consumption, which is used by the shipping company for administrative purposes.

To determine if the information above is critical, the consequences likely to result from a compromise to the confidentiality, integrity or availability should be considered. When doing so the shipping company should determine the criticality of the information stored, processed or transmitted by the SCADA system using the most sensitive information to determine the overall impact of the system.

(b) Determine consequence:

As this OT system is using several measuring points and is integrated with other systems, the company decide to consider the effect of an operational malfunction or loss of the SCADA system due to a cyber incident. In this case, the company concludes that this will have a severe effect and thereby a high impact to the operation of the ship.

(c) Determine likelihood:

Using the confidentiality, integrity and availability (CIA) model, the shipping company can also conclude that:

- (i) losing confidentiality of the sensor data acquired by the SCADA system will have a low impact as the sensors are publicly displayed on board. However, from a safety point of view, it is important that the information transmitted by the sensors can be relied upon therefore there is a high potential impact from a loss of integrity. It will also be a safety issue if the information cannot be read, and there is therefore a high potential impact from a loss of availability.
- (ii) for the power consumption information being sent to the shipping company for statistical purposes, it is assessed that there is a low potential impact from a loss of confidentiality. The company does not want the data to be public, however the effect would be limited if it were to happen. There will also be a low potential impact from a loss of integrity as the data is only used for in-house considerations. There is therefore also a low potential impact from a loss of availability.

(d) Determine cyber security risks impact:

The following table shows the result of the assessment:

Table I 5-2 Result of CIA assessment of SCADA system

SCADA system	Confidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
Statistical data	Low	Low	Low	Low

(e) Establishing the prioritised action plan:

Risk value = Assets value (impact, consequence) x Threats likelihood x Difficulty of use of vulnerabilities
Assets value = confidentiality + integrity + availability, and the impact and consequence of loss of assets

Likelihood ↑	Medium	High	High
	Low	Medium	High
	Low	Low	Medium
	Consequence →		

5.1.6 Bring your own device (BYOD)

It is recognised that personnel may be allowed to bring their own devices (BYOD) on board to access the ships' system or network. Although this may be both beneficial and economical for ships, because these devices may be unmanaged, it significantly increases the possibility of vulnerabilities being exposed. Policies and procedures should address their control, use, and how to protect vulnerable data, such as through network segregation.

5.2 Risk Assessment Made by the Company

5.2.1 As mentioned above, the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. Elements of a ship security assessment⁸ can be used when performing the risk assessment, which should physically test and assess the IT and OT systems on board including:

⁸ The assessment described is based on regulation 8 of the ISPS Code.

- (a) identification of existing technical and procedural controls to protect the onboard IT and OT systems (more information can be found with the Critical Security Controls⁹);
- (b) identification of IT and OT systems that are vulnerable including human factors, and the policies and procedures governing the use of these systems (the identification should include searches for known vulnerabilities relevant to the equipment, the current level of patching and firmware updates)
- (c) identification and evaluation of key ship board operations that are vulnerable to cyber attacks;
- (d) identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence to establish and prioritise protection measures.

5.2.2 Companies may consult with the producers and service providers of onboard equipment and systems to understand the technical and procedural controls that may already be in place to address cyber security. Furthermore, any identified cyber vulnerability in the factory standard configuration of a critical system or component should be disclosed to facilitate better protection of the equipment in the future.

5.3 Third-Party Risk Assessments

Self-assessments can serve as a good start, but may be complemented by third-party risk assessments to drill deeper, and identify the risks and the gaps that may not be found during the self-assessment. Penetration tests of critical IT and OT infrastructure can also be performed to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. Such tests can be performed by external experts simulating attacks using both IT-systems, social engineering and, if desired, even physical penetration of a facility's security perimeter. These tests are referred to as active tests because they involve accessing and inserting software into a system. This may only be appropriate for IT systems. Where risk to OT systems during penetration testing is unacceptable, passive testing approaches should be considered. Passive methods rely on scanning data transmitted by a system to identify vulnerabilities. In general, no attempt is made to actively access or insert software into the system.

5.4 Risk Assessment Process

5.4.1 Phase 1: Pre-assessment activities

Prior to starting a cyber security assessment on board¹⁰, the following activities should be performed:

- (a) map the ship's key functions and systems and their potential impact levels, for example using the CIA model, taking into consideration the operation of OT systems;
- (b) identify main producers of critical shipboard IT and OT equipment;
- (c) review detailed documentation of critical OT and IT systems including their network architecture, interfaces and interconnections;
- (d) identify cyber security points-of-contact at each of the producers and establish working relationships with them;
- (e) review detailed documentation on the ship's maintenance and support of its IT and OT systems;

⁹ www.cisecurity.org/critical-controls.cfm.

¹⁰ Based on a third-party risk assessment method described by NCC Group.

- (f) establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment;
- (g) support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

5.4.2 Phase 2: Ship assessment

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship. These vulnerabilities and weaknesses could fall into one of the following categories:

- (a) technical such as software defects or outdated or unpatched systems;
- (b) design such as access management, unmanaged network interconnections;
- (c) implementation errors for example misconfigured firewalls;
- (d) procedural or other user errors.

The activities performed during an assessment would include reviewing the configuration of all computers, servers, routers, and cyber security technologies including firewalls. It should also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

5.4.3 Phase 3: Debrief and vulnerability review/reporting

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation. Recommended technical and/or procedural corrective actions should be identified for each vulnerability in a final report.

Ideally, the cyber security assessment report should include:

- (a) executive summary – a high-level summary of results, recommendations and the overall security profile of the assessed environment, facility or ship;
- (b) technical findings – a detailed, tabular breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and appropriate technical fix and mitigation advice;
- (c) prioritised list of actions – the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list does not represent a list of services and products the third-party risk assessor would like to sell, instead of being a complete list of options available;
- (d) supplementary data – a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing of critical or high-risk vulnerabilities;
- (e) appendices – detailed records of all activities conducted by the cyber security assessment team and the tools used during the engagement.

5.4.4 Phase 4: Producer debrief

Once the shipowner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the producers of the affected systems. Any findings, which are approved by the shipowner for disclosure

to the producers, could further be analysed with support from external experts, who should work with the producer's cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved. This supporting activity is intended to ensure that any remediation plan developed by the producer is comprehensive in nature and the correct solution to eliminate the vulnerabilities identified.

Chapter 6 Develop Protection and Detection Measures

6.1 General

6.1.1 The outcome of the senior management's risk assessment and subsequent company's cyber security strategy should be a reduction in risk, if needed. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

6.1.2 Special attention should be given when there has been no control over who has access to the onboard systems. This could, for example, happen during drydocking, layups or when taking over a new or existing ship. In such cases, it is difficult to know if malicious software has been left in the onboard systems. It is recommended that sensitive data is removed from the ship and reinstalled on returning to the ship. Where possible, systems should be scanned for malware before prior to use. OT systems should be tested to check that the functionalities are still intact.

6.1.3 It is critical to identify how to manage cyber security on board and to delegate responsibilities to the master, responsible officers and maybe the company security officer.

6.1.4 Cyber security protection measures may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls. Both technical and procedural controls should be compatible with the confidentiality, integrity and availability (CIA) model for protecting data and information.

6.1.5 It is recognised that technical cyber security controls may be more straightforward to implement on a new ship than on an existing ship. Consideration needs to be given to only implement technical controls that are practical and cost effective, particularly on existing ships.

6.1.6 Consideration should be given in

- (a) increased cost due to multiple technical controls and/or duplication;
- (b) increased complexity to manage an ever increasing technology base;
- (c) security can get in the way of the business; and
- (d) maintenance is challenging.

Implementation of cyber security controls should be prioritised, focusing first on those measures, or combinations of measures, which offer the greatest benefit. Then expanded from basic to foundational and advanced, if applicable.

6.1.7 A wide range of options to enhance the technical aspects of cyber security exists and will often be employed by or in close cooperation with the providers of the respective critical system. Below 6.2 to 6.4 respectively introduce the widely used cyber security controls related measures and standards. Organizations may choose from, but not limited to these two measures according to their need.

6.2 CIS Technical Protection Measures

6.2.1 The Centre for Internet Security (CIS) provides guidance on measures¹¹ that can be used to address cyber security vulnerabilities. The protection measures comprise of a list of Critical Security Controls (CSC) that are prioritised and vetted to ensure that they provide an effective approach for companies to assess and improve their defences. The CSCs include both technical and procedural aspects. CSC Version 7 has 20 controls and 171 subcontrols. The subcontrols were noted as being foundational or advanced.

6.2.2 The below mentioned examples of CSCs have been selected as particularly relevant to equipment and data onboard ships¹².

(a) Limitation to and control of network ports, protocols and services

Access lists to network systems can be used to implement the company's security policy. This ensures that only appropriate traffic will be allowed via a controlled network or subnet, based on the control policy of that network or subnet.

It should be a requirement that routers are secured against attacks and unused ports should be closed to prevent unauthorised access to systems or data.

(b) Configuration of network devices such as firewalls, routers and switches

It should be determined which systems should be attached to controlled or uncontrolled¹³ networks. Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, security gateways, routers and switches. Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks, as direct internet connection makes them highly prone to infiltration by malware. For example:

- (i) Networks that are critical to the operation of a ship itself, should be controlled. It is imperative that these systems - have a high level of security.
- (ii) Networks that provide suppliers with remote access to navigation and other OT system software on onboard equipment, should also be controlled. These networks may be necessary for suppliers to allow upload of system upgrades or perform remote servicing. Shoreside external access points of such connections should be secured to prevent unauthorised access.
- (iii) Other networks, such as guest access networks, may be uncontrolled, for instance those related to passenger recreational activities or private internet access for crew. Normally, any wireless network should be considered uncontrolled.

Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data are in that zone. Confidential and safety critical systems should be in the most protected zone. See Annex 2 for more information on shipboard networks and also refer to ISO/IEC 62443.

(c) Physical security

Security and safety critical equipment and cable runs should be protected from unauthorised access. Physical security is a central aspect of cyber security¹⁴.

(d) Detection, blocking and alerts

Identifying intrusions and infections is a vital part of the controls. A baseline of network operations and expected data flows for users and systems should be established and managed so that cyber incident alert

¹¹ CIS, Critical Security Controls for Effective Cyber Security, available at www.cisecurity.org/critical-controls.cfm.

¹² Stephenson Harwood (2015), Cyber Risk.

¹³ In accordance with EC 61162-460:2015: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security.

¹⁴ See also the ISPS Code.

thresholds can be established. Key to this will be the definition of roles and responsibilities for detection to ensure accountability. Additionally, a company may choose to incorporate an Intrusion Detection System (IDS) system or an Intrusion Prevention System (IPS) into the network or as part of the firewall. Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity. Further details concerning IDS and IPS can be found in annex 2. Ensure that dedicated onboard personnel can understand the alerts and their implications. Incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

(e) Satellite and radio communication

Cyber security of the radio and satellite connection should be considered in collaboration with the service provider. In this connection, the specification of the satellite link should be considered when establishing the requirements for onboard network protection.

When establishing an uplink connection for ships' navigation and control systems to shore-based service providers, consideration should be given in how to prevent illegitimate connections gaining access to the onboard systems.

The access interconnect is the distribution partner's responsibility. The final routing of user traffic from the internet access point to its ultimate destination onboard ("last mile") is the responsibility of the shipowner. User traffic is routed through the communication equipment for onward transmission on board. At the access point for this traffic, it is necessary to provide data security, firewalling and a dedicated "last-mile" connection.

When using a Virtual Private Network (VPN), the data traffic should be encrypted to an acceptable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or on board) should be deployed. The distribution partner should advise on the routing and type of connection most suited for specific traffic. Onshore filtering (inspection/blocking) of traffic is also a matter between a shipowner and the distribution partner. However, it is not sufficient to have either onshore filtering of traffic or firewalls/security inspection/blocking gateways on the ship, because both types are needed and supplement each other to achieve a sufficient level of protection.

Producers of satellite communication terminals and other communication equipment may provide management interfaces with security control software that are accessible over the network. This is primarily provided in the form of web-based user interfaces. Protection of such interfaces should be considered when assessing the security of a ship's installation.

(f) Wireless access control

It should be ensured that wireless access to networks on the ship is limited to appropriate authorised devices and secured using a strong encryption key, which is changed regularly.

(g) Malware detection

Scanning software that can automatically detect and address the presence of malware in systems onboard should be regularly updated.

As a general guideline, onboard computers should be protected to the same level as office computers ashore. Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard. This will reduce the risk of these computers acting as attack vectors towards servers and other computers on the ship's network. The decision on whether to rely on these defence methods should take into consideration how regularly the scanning software will be able to be updated.

(h) Secure configuration for hardware and software

Only senior officers should be given administrator profiles so that they can control the set up and disabling of normal user profiles. User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes for which they are required. User profiles should not allow the user to alter the systems or install and execute new programs.

(i) Email and web browser protection

Email communication between ship and shore is a vital part of a ship's operation. Appropriate email and web browser protection serves to:

- (i) protect shoreside and onboard personnel from potential social engineering
- (ii) prevent email being used as a method of obtaining sensitive information
- (iii) ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, for example protecting by encryption
- (iv) prevent web browsers and email clients from executing malicious scripts.

Some best practices for safe email transfer are: email as zip or encrypted file when necessary, disable hyperlinks on email system, and avoid using generic email addresses and ensure the system has configured user accounts.

(j) Data recovery capability

Data recovery capability is the ability to restore a system and/or data from a secure copy or image thereby allowing the restoration of a clean system. Essential information and software-adequate backup facilities should be available to ensure it can be recovered following a cyber incident.

Retention periods and restore scenarios should be established to prioritise which critical systems need quick restore capabilities to reduce the impact. Systems that have high data availability requirements should be made resilient. OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident. More detail on recovery can be found in chapter 7.

(k) Application software security (patch management)

Critical safety and security updates should be provided to onboard systems. These updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack.

6.3 ISO/IEC 27001

6.3.1 Many organisations find it worthwhile to establish an information security management system (ISMS) according to the international standard ISO/IEC 27001. The standard is fully aligned with recent editions of the other commonly used ISO management system standards, such as ISO 9001 and ISO 14001, allowing for easy integration of the ISMS into the wider scope of a company's integrated management system if so desired. At time of **this Part** publishing, ISO/IEC 27001:2013 is the current edition of the standard. ISO/IEC 27001 requires continuous cyber security management, through implementing an information security management system (ISMS). The ISMS shall be established, implemented, maintained and continually improved in accordance with the requirements of ISO/IEC 27001, covering the organisation, responsibilities and management of IT & OT systems. The typical PDCA management system cycle also applies to the ISMS. **This Part** deals with the operational aspects of cyber security management, focusing on the ship in operation. The ISO/IEC 27001 approach complements **this Part**' approach with an organisation-centric approach, putting much emphasis on planning, resources, and continuous improvement.

6.3.2 ISO/IEC 27001:2013 is divided into ten clauses and an annex; the management system controls (clause 4 to 10) and annexure controls (14 sections, 35 control objectives and 114 detail controls). Clauses 1 to 3 contain the scope of the standard, normative references, and a reference to ISO 27000 for terms and definitions. Clauses 4 to 10 contain the following requirements:

(a) Clause 4: Context of the organisation

- 4.1 Understanding the organisation and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system established

- (b) Clause 5: Leadership
 - 5.1 Leadership and commitment
 - 5.2 Policy
 - 5.3 Organisational roles, responsibilities and authorities

- (c) Clause 6: Planning
 - 6.1 Actions to address risks and opportunities
 - 6.2 Information security objectives and planning to achieve them

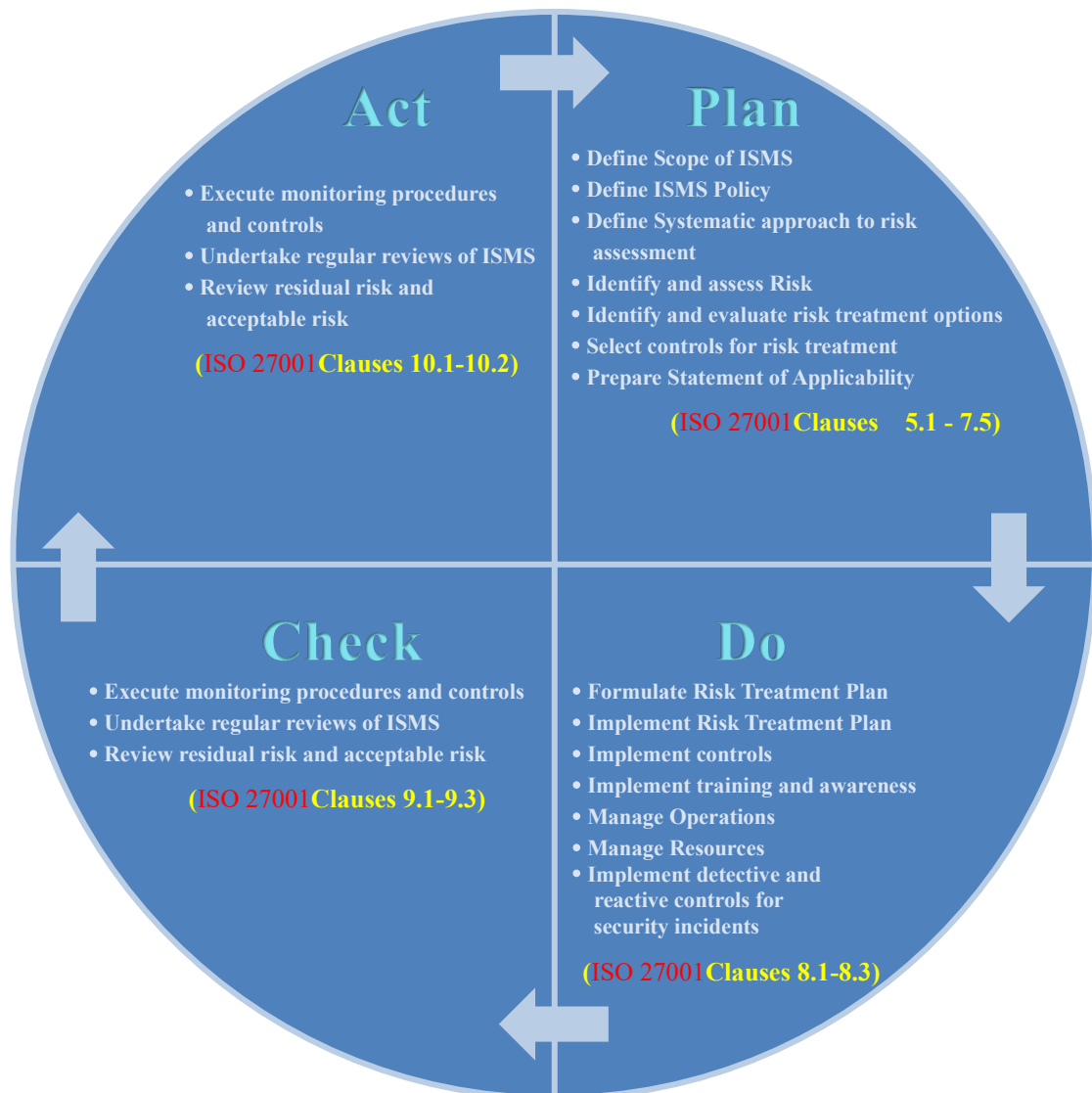
- (d) Clause 7: Support
 - 7.1 Resources
 - 7.2 Competence
 - 7.3 Awareness
 - 7.4 Communication
 - 7.5 Documented Information

- (e) Clause 8: Operation
 - 8.1 Operational planning and control
 - 8.2 Information security risk assessment
 - 8.3 Information security risk treatment

- (f) Clause 9: Performance evaluation
 - 9.1 Monitoring, measurement, analysis and evaluation
 - 9.2 Internal Audit
 - 9.3 Management Review

- (g) Clause 10: Improvement
 - 10.1 Nonconformity and corrective action
 - 10.2 Continual improvement

- (h) Annex A (normative): Reference control objectives and controls
Lists in detail controls to be used for the main clauses of the standard. The organisation's controls must be checked against this list to ensure no necessary controls are overlooked.



The typical PDCA management system cycle

6.3.3 Overview of ISO 27001:2013 Annex A

Ref.	Section	Controls	Content
A.5	Information security policies	2	Management direction
A.6	Organization of information security	7	Internal organization, Mobile devices and teleworking
A.7	Human resource security	6	Prior to, during employment, termination and change of employment
A.8	Asset management	10	Responsibility for assets, information classification, media handling
A.9	Access Control	14	Business requirements, user access management and responsibilities, system and application access control
A.10	Cryptography	2	Cryptographic controls
A.11	Physical and environmental security	15	Secure areas, equipment

A.12	Operations security	14	Procedures and responsibilities, malware protection , backup process, Logging and monitoring, operational software, technical vulnerabilities, system audits
A.13	Communications security	7	Network security, Information transfer
A.14	System acquisition, development and maintenance	13	Security requirements, development and support, test data
A.15	Supplier relationships	5	Information security in supplier relationships, service delivery
A.16	Information security incident management	7	Management of information security incidents and improvements
A.17	Information security aspects of business continuity management	4	Continuity, redundancy
A.18	Compliance	8	Legal and contractual compliance, reviews

6.3.4 Mandatory documents corresponding to ISO 27001:2013

Mandatory documents	Check
Scope of the ISMS (clause 4.3)	
Information security policy and objectives (clauses 5.2 and 6.2)	
Risk assessment and risk treatment methodology (clause 6.1.2)	
Statement of Applicability (clause 6.1.3 d)	
Risk treatment plan (clauses 6.1.3 e and 6.2)	
Risk assessment report (clause 8.2)	
Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)	
Inventory of assets (clause A.8.1.1)	
Acceptable use of assets (clause A.8.1.3)	
Access control policy (clause A.9.1.1)	
Operating procedures for IT/OT management (clause A.12.1.1)	
Secure system engineering principles (clause A.14.2.5)	
Supplier security policy (clause A.15.1.1)	
Incident management procedure (clause A.16.1.5)	
Business continuity procedures (clause A.17.1.2)	
Statutory, regulatory, and contractual requirements (clause A.18.1.1)	

6.3.5 Mandatory records corresponding to ISO 27001:2013

Mandatory records	Check
Records of training, skills, experience and qualifications (clause 7.2)	
Monitoring and measurement results (clause 9.1)	
Internal audit program (clause 9.2)	
Results of internal audits (clause 9.2)	
Results of the management review (clause 9.3)	
Results of corrective actions (clause 10.1)	
Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)	

6.3.6 Non-mandatory documents corresponding to ISO 27001:2013

Non-mandatory records	Check
Procedure for document control (clause 7.5)	
Controls for managing records (clause 7.5)	
Procedure for internal audit (clause 9.2)	
Procedure for corrective action (clause 10.1)	
Bring your own device (BYOD) policy (clause A.6.2.1)	
Mobile device and teleworking policy (clause A.6.2.1)	
Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)	

Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)	
Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)	
Procedures for working in secure areas (clause A.11.1.5)	
Clear desk and clear screen policy (clause A.11.2.9)	
Change management policy (clauses A.12.1.2 and A.14.2.4)	
Backup policy (clause A.12.3.1)	
Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)	
Business impact analysis (clause A.17.1.1)	
Exercising and testing plan (clause A.17.1.3)	
Maintenance and review plan (clause A.17.1.3)	
Business continuity strategy (clause A.17.2.1)	

6.4 IACS Rec. No. 166

Refer to IACS announced publication of its Recommendation on Cyber Resilience (No. 166) which provides technical requirements for cyber resilient ships throughout their service lives. See also 1.3.2(d).

6.5 Procedural Protection Measures

Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. Examples for procedural actions can be:

6.5.1 Training and awareness

Training and awareness is the key supporting element to an effective approach to cyber safety and security as described in **this Part** and summarised in 2.3.

The internal cyber threat is considerable and should not be underestimated. Personnel have a key role in protecting IT and OT systems but can also be careless, for example by using removable media to transfer data between systems without taking precautions against the transfer of malware. Training and awareness should be tailored to the appropriate levels for:

- onboard personnel including the master, officers and crew;
- shoreside personnel, who support the management and operation of the ship.

This Part assume that other major stakeholders in the supply chain, such as charterers, classification societies and service providers, will carry out their own best-practice cyber security protection and training. It is advised that owners and operators ascertain the status of cyber security preparedness of their third-party providers as part of their sourcing procedures for such services.

An awareness programme should be in place for all onboard personnel, covering at least the following:

- risks related to emails and how to behave in a safe manner (examples are phishing attacks where the user clicks on a link to a malicious site);
- risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;

- risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected);
- risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package);
- risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;
- safeguarding user information, passwords and digital certificates;
- cyber risks in relation to the physical presence of non-company personnel, eg, where third-party technicians are left to work on equipment without supervision;
- detecting suspicious activity or devices and how to report if a possible cyber incident is in progress (examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network);
- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;
- understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incident-response planning and testing;
- procedures for protection against risks from service providers' removable media before connecting to the ship's systems.

In addition, personnel need to be made aware that the presence of anti-malware software does not remove the requirement for robust security procedures, for example controlling the use of all removable media.

Further, applicable personnel should know the signs when a computer has been compromised. This may include the following:

- an unresponsive or slow to respond system;
- unexpected password changes or authorised users being locked out of a system;
- unexpected errors in programs, including failure to run correctly or programs running unexpectedly;
- unexpected or sudden changes in available disk space or memory;
- emails being returned unexpectedly;
- unexpected network connectivity difficulties;
- frequent system crashes;
- abnormal hard drive or processor activity;

- unexpected changes to browser, software or user settings, including permissions.

And, nominated personnel should be able to understand reports from IDS systems, if used. This list is not comprehensive and is intended to raise awareness of potential signs, which should be treated as possible cyber incidents.

6.5.2 Access for visitors

Visitors such as authorities, technicians, agents, port officials, and owner representatives should be restricted with regard to computer access whilst on board. Unauthorised access to sensitive OT network computers should be prohibited through clearly marked physical barriers. If access to a network by a visitor is required and allowed, then it should be restricted in terms of user privileges. Access to certain networks for maintenance reasons should be approved and co-ordinated following appropriate procedures as outlined by the company/ship operator.

If a visitor requires computer and printer access, an independent computer, which is air-gapped from all controlled networks, should be used. To avoid unauthorised access, removable media blockers should be used on all other physically accessible computers and network ports.

6.5.3 Upgrades and software maintenance

Hardware or software that is no longer supported by its producer or software developer will not receive updates to address potential vulnerabilities. For this reason, the use of hardware and software, which is no longer supported, should be carefully evaluated by the company as part of the cyber risk assessment.

Relevant hardware and software installations on board should be updated to maintain a sufficient security level. Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc. Software includes computer operating systems, which should also be kept up to date. Additionally, a number of routers, switches and firewalls, and various OT devices will be running their own firmware, which may require regular updates and so should be addressed in the procedural requirements.

Effective maintenance of software depends on the identification, planning and execution of measures necessary to support maintenance activities throughout the full software lifecycle. An industry standard¹⁵ to ensure safe and secure software maintenance has been developed. It specifies requirements for all stakeholders involved in software maintenance of shipboard equipment and associated integrated systems. The standard covers on board, on shore and remote software maintenance.

6.5.4 Anti-virus and anti-malware tool updates

In order for scanning software tools to detect and deal with malware, they need to be updated. Procedural requirements should be established to ensure updates are distributed to ships on a timely basis and that all relevant computers on board are updated.

6.5.5 Remote access

Policy and procedures should be established for control over remote access to onboard IT and OT systems. Clear guidelines should establish who has permission to access, when they can access, and what they can access. Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system. Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

6.5.6 Use of administrator privileges

Access to information should only be allowed to relevant authorised personnel.

Administrator privileges allow full access to system configuration settings and all data. Users logging into systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on board, to

¹⁵ See: Industry standard on software maintenance of shipboard equipment by BIMCO and CIRM (Comité International Radio-Maritime).

log into systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

User privileges should be removed when the people concerned are no longer on board. User accounts should not be passed on from one user to the next using generic usernames. Similar rules should be applied to any onshore personnel with remote access to systems on ships when they change role and no longer need access.

In a business environment, such as shipping, access to onboard systems is granted to various stakeholders. Suppliers and contractors are a risk because they often have both intimate knowledge of a ship's operations and often full access to systems.

To protect access to confidential data and safety critical systems, a robust password policy should be developed¹⁶. Passwords should be strong and changed periodically. The company policy should address the fact that over-complicated passwords, which must be changed too frequently, are at risk of being written on a piece of paper and kept near the computer.

6.5.7 Physical and removable media controls

Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware. Removable media can be used to bypass layers of defences and can be used to attack systems that are otherwise not connected to the internet. A clear policy for the use of such media devices is essential; it must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

There are, however, situations where it is unavoidable to use these media devices, for example during software maintenance. In such cases, there should be a procedure in place to require checking of removable media for malware and/or validating legitimate software by digital signatures and watermarks.

Policies and procedures relating to the use of removable media should include a requirement to scan any removable media device in a computer that is not connected to the ship's controlled networks. If it is not possible to scan the removable media on board, eg the laptop of a maintenance technician, then the scan could be done prior to boarding with the result and timing duly documented. Companies should consider notifying ports and terminals about the requirement to scan removable media prior to permitting the uploading of files onto a ship's system. This scanning should be carried out when transferring the following file types:

- (a) cargo files and loading plans eg container ship BAPLIE files;
- (b) national, customs, and port authority forms;
- (c) bunkering and lubrication oil forms;
- (d) ship's stores and provisions lists;
- (e) engineering maintenance files.

This list represents examples and should not be seen as exhaustive.

6.5.8 Equipment disposal, including data destruction

Obsolete equipment can contain data which is commercially sensitive or confidential. The company should have a procedure in place to ensure that the data held in obsolete equipment is properly destroyed prior to disposing of the equipment, ensuring that vital information cannot be retrieved.

6.5.9 Obtaining support from ashore and contingency plans

Ships should have access to technical support in the event of a cyber attack. Details of this support and associated procedures should be available on board. Please refer to Chapter 6 for more information about contingency planning.

¹⁶ More information can be found in NIST publication SP 800-63-3 Digital Identity Guidelines.

Chapter 7 Establish Contingency Plans

7.1 Attention of Developing The Plan

7.1.1 When developing contingency plans for implementation onboard ships, it is important to understand the significance of any cyber incident, particularly for IT and OT systems and prioritise response actions accordingly.

7.1.2 Any cyber incident should be assessed in accordance with the CIA model (see chapter 5) to estimate the impact on operations, assets etc. In most cases, a loss of IT systems on board, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the ship. In the event of a cyber incident affecting IT systems only, the priority may be the immediate implementation of an investigation and recovery plan.

7.1.3 The loss of OT systems may have a significant and immediate impact on the safe operation of the ship. Should a cyber incident result in the loss or malfunctioning of OT systems, it will be essential that effective actions are taken to ensure the immediate safety of the crew, ship and protection of the marine environment. In general, appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by appropriate operational and emergency procedures included in the safety management system. Some of the existing procedures in the ship's safety management system will already cover such cyber incidents.

7.1.4 The safety management system will already include procedures for reporting accidents or hazardous situations and define levels of communication and authority for decision making. Where appropriate, such procedures should be amended to reflect communication and authority in the event of a cyber incident.

7.1.5 The following is a non-exhaustive list of the actions in response to the type of cyber incidents, which should be addressed in contingency plans on board:

- (a) loss of availability of electronic navigational equipment or loss of integrity of navigation related data;
- (b) loss of availability or integrity of external data sources, including but not limited to GNSS
- (c) loss of essential connectivity with the shore, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications
- (d) loss of availability of industrial control systems, including propulsion, auxiliary systems and other critical systems, as well as loss of integrity of data management and control
- (e) the event of a ransomware or denial or service incident.

7.1.6 It is important that onboard personnel understand that the loss of OT systems due to a cyber incident must be treated like any other equipment failure. Furthermore, it is important to ensure that a loss of equipment or reliable information due to a cyber incident does not make existing emergency plans and procedures redundant. It is crucial that contingency plans, and related information, are available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

7.1.7 There may be occasions when responding to a cyber incident may be beyond the competencies on board or at head office due to the complexity or severity of such incidents. In these cases, external expert assistance may be required (for example post event forensic analysis and clean-up).

Chapter 8

Respond to and Recover from Cyber Security Incidents

8.1 General

It is important to understand that cyber incidents may not disappear by themselves. If for example the ECDIS has been infected with malware, starting up the back-up ECDIS may cause another cyber incident. It is, therefore, recommended to plan how to carry out the cleaning and restoring of infected systems.

Knowledge about previous identified cyber incidents should be used to improve the response plans of all ships in the company's fleet and an information strategy for such incidents may be considered.

8.2 Effective Response

8.2.1 A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations. The team should be capable of performing all aspects of the response.

8.2.2 An effective response should at least consist of the following steps:

- (a) Initial assessment: To ensure an appropriate response, it is essential that the response team find out:
 - (i) how the incident occurred;
 - (ii) which IT and/or OT systems were affected and how;
 - (iii) the extent to which the commercial and/or operational data is affected;
 - (iv) to what extent any threat to IT and OT remains.
- (b) Recover systems and data: Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software. The content of a recovery plan is covered in 8.3.
- (c) Investigate the incident: To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence. Investigations into cyber incidents are covered in 8.4.
- (d) Prevent a re-occurrence: Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action.

8.2.3 When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to initiate the recovery plan alongside onboard contingency plans. When this is the case, the response team should be able to provide advice to the ship on:

- (a) whether IT or OT systems should be shut down or kept running to protect data

- (b) whether certain ship communication links with the shore should be shut down
- (c) the appropriate use of any advanced tools provided in pre-installed security software
- (d) the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

8.3 Recovery Plan

8.3.1 Recovery plans should be available in hard copy on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritised in the plan. The recovery plan should be understood by personnel responsible for cyber security. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

8.3.2 As explained in 6.2, a data recovery capability is a valuable technical protection measure. Data recovery capabilities are normally in the form of software backup for IT data. The availability of a software backup, either on board or ashore, should enable recovery of IT to an operational condition following a cyber incident.

8.3.3 Recovery of OT may be more complex especially if there are no backup systems available and recovery may involve assistance from ashore. Details of where this assistance is available and by whom, should be part of the recovery plan, for example by proceeding to a port to obtain assistance from a service engineer.

8.3.4 If qualified personnel are available on board, more extensive diagnostic and recovery actions may be performed. Otherwise, the recovery plan will be limited to obtaining quick access to technical support.

8.4 Investigating Cyber Incidents

8.4.1 Investigating a cyber incident can provide valuable information about the way in which a vulnerability was exploited. Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board in accordance with company procedures. A detailed investigation may require external expert support.

8.4.2 The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. It will also provide the wider maritime industry with a better understanding of maritime cyber risks. Any investigation should result in¹⁷:

- (a) a better understanding of the potential cyber risks facing the maritime industry both on board and ashore;
- (b) identification of lessons learned, including improvements in training to increase awareness;
- (c) updates to technical and procedural protection measures to prevent a recurrence.

8.5 Losses Arising From a Cyber Incident

8.5.1 Insurance issue

¹⁷ Based on CREST, Cyber Security Incident Response Guide, Version 1.

For insurers, the term “cyber” includes many different aspects and it is important to distinguish between them and their effects on insurance cover. Also, it is important to note that according to the general understanding of insurers, there is no systemic risk to ships arising from a cyber incident and the impact of an incident is expected to be most likely confined to a single ship.

Companies will be aware that specific non-marine insurance cover may be available to cover data loss and the resulting fines and penalties resulting from equipment failure.

Companies should be able to demonstrate that they are acting with reasonable care in their approach to managing cyber risk and protecting the ship from any damage that may arise from a cyber incident.

8.5.2 Cover for property damage

Generally, in many markets offering marine property insurance, the policy may cover loss or damage to the ship and its equipment caused by a shipping incident such as grounding, collision, fire or flood, even when the underlying cause of the incident is a cyber incident. It may be noted that currently in some markets exclusion clauses for cyber attacks exist. If the marine policy contains an exclusion clause for cyber attacks, the loss or damage will not be covered.

Companies are recommended to check with their insurers / brokers in advance whether their policy covers claims caused by cyber incidents and/or by cyber attacks.

Guidelines for the market have been published, in which marine insurers are recommended to ask questions about company cyber security awareness and non-technical procedures. Companies should, therefore, expect a request for non-technical information regarding their approach to cyber security from insurers.

The limited data on the frequency, severity of loss or probability of physical damage resulting from a cyber incident, represents a challenge and means that standard pricing is not available.

8.5.3 Cover for liability

It is recommended to contact the P&I (Protection and Indemnity) Club for detailed information about cover provided to shipowners and charterers in respect of liability to third parties (and related expenses) arising from the operation of ships.

An incident caused, for example by malfunction of a ship's navigation or mechanical systems because of a criminal act or accidental cyber attack, does not in itself give rise to any exclusion of normal P&I cover.

It should be noted that many losses, which could arise from a cyber incident are not in the nature of third-party liabilities arising from the operation of the ship. For example, financial loss caused by ransomware, or costs of rebuilding scrambled data would not be identified in the coverage.

Normal cover, in respect of liabilities, is subject to a war risk exclusion and cyber incidents in the context of a war or terror risk, will not normally be covered.

Chapter 9 Survey Requirements

9.1 General

Registration and maintenance of class notation "**Cyber-S**" are specified in the following 9.1.1 to 9.1.3:

- 9.1.1 Initial **Survey** (refer to 9.3)
- 9.1.2 **Special Survey** (hereinafter referred to as "Periodical **Survey**")
- 9.1.3 Annual **Survey** (hereinafter referred to as "Periodical Survey")
- 9.1.4 Occasional **Survey**

9.2 Survey Intervals

Survey are to be carried out in accordance with the following requirements given in 9.2.1 and 9.2.2.

- 9.2.1 Initial **surveys** are to be carried out at the time an application for registration of "**Cyber-S**" notation is made.
- 9.2.2 Periodical **surveys** are to be carried out in (a) through (c) below.
 - (a) **Special Surveys** are to be carried out within 3 months prior to the due date of Special Survey as specified in 1.6.4 of Part I of the Rules for Steel Ship.
 - (b) Annual **Surveys** are to be carried out at the intervals specified in 1.6.5(a) of Part I of the Rules for Steel Ships
 - (c) Occasional **Surveys** are to be carried out at a timing when any of (i) to (iii) mentioned below takes place but does not fall within the schedules of **Special Surveys** or Annual **Surveys**.
 - (i) In case where any computer-based system has been damaged, repaired or renewed.
 - (ii) In case where any computer-based system is modified or altered.
 - (iii) In case where considered necessary by the Society.

9.3 Initial Survey

An owner who intends to apply "**Cyber-S**" notation is to conduct a meeting upon building contract in which a tripartite agreement is to be made amongst owner, builder and class that the owner is to define the scope of computer-based systems to which **this Part** applies and provide information necessary for the inventory by the time of the defined date in the contract.

9.3.1 Drawing and data

Before the integrator designs detailed systems and networks, following plans and documents are to be submitted to the Society for approval, if applicable.

- (a) Inventory of onboard systems as specified in 4.2.

- (b) Onboard networks (refer to Annex 2).
- (c) Ship to shore interface as specified in 4.3.
- (d) Company plans and procedures for cyber risk management as specified in 2.2.
- (e) The results of identifying threats and vulnerabilities as specified in Chapter 3 and Chapter 4.
- (f) Risk assessment report as specified in Chapter 5.
- (g) Protection and detection measures as specified in Chapter 6.
- (h) Established contingency plans as specified in Chapter 7.
- (i) Recovery plan as specified in Chapter 8.

Upon approval of the above drawings and documents by the Society, the integrator is to develop the following plans and documents which are to be submitted for approval by the Society.

- (j) Cyber security testing plans

The timing and the method of testings on cyber security features should be planned and implemented.

- (k) Documents governing remote access (control procedures etc.), where the ship has remote access capabilities.

9.3.2 Testing after installation onboard

- (a) The **Surveyor** confirms on board the ship that the measures to control the identified risks submitted by the integrator has been fully and effectively implemented onboard.
- (b) Security tests is to be carried out with the attendance of the **Surveyor**. If it is difficult for the **Surveyor** to attend the security tests, they can be replaced by submission of test reports issued by a testing company with sufficient capabilities and experiences.

9.3.3 Documents to be maintained onboard

At the completion of an initial **survey**, the drawing and data specified in 9.3.1 should be maintained and properly managed onboard.

9.4 Special Survey

Following documents are to be submitted to the Society by the owner for **special surveys**.

9.4.1 Results of security tests specified in 9.3.1(j)

9.4.2 Documents which indicates that the documents specified in 9.3.1 are properly maintained and managed

9.5 Annual Survey

Following documents are to be submitted to the Society by the owner for annual surveys.

9.5.1 Documentation which indicates that the documents specified in 9.3.1 are properly maintained and managed.

9.6 Occasional Surveys

Where an occasional survey is found necessary, the owner or the management company is to submit documents required by the Society for the examination.

Annex 1 Target Systems, Equipment and Technologies

This annex provides a summary of potentially vulnerable systems and data onboard ships to assist companies with assessing their cyber risk exposure. Vulnerable systems, equipment and technologies may include:

A1.1 Communication Systems

- A1.1.1 Integrated communication systems
- A1.1.2 Satellite communication equipment
- A1.1.3 Voice Over Internet Protocols (VOIP) equipment
- A1.1.4 Wireless networks (WLANs)
- A1.1.5 Public address and general alarm systems.

A1.2 Bridge Systems

- A1.2.1 Integrated navigation system
- A1.2.2 Positioning systems (GPS, etc.)
- A1.2.3 Electronic Chart Display Information System (ECDIS)
- A1.2.4 Dynamic Positioning (DP) systems
- A1.2.5 Systems that interface with electronic navigation systems and propulsion/manoeuvring systems
- A1.2.6 Automatic Identification System (AIS)
- A1.2.7 Global Maritime Distress and Safety System (GMDSS)
- A1.2.8 Radar equipment
- A1.2.9 Voyage Data Recorders (VDRs)
- A1.2.10 Other monitoring and data collection systems.

A1.3 Propulsion and Machinery Management and Power Control Systems

- A1.3.1 Engine governor
- A1.3.2 Power management

A1.3.3 Integrated control system

A1.3.4 Alarm system

A1.3.5 Emergency response system.

A1.4 Access Control Systems

A1.4.1 Surveillance systems such as CCTV network

A1.4.2 Bridge Navigational Watch Alarm System (BNWAS)

A1.4.3 Shipboard Security Alarm Systems (SSAS)

A1.4.4 Electronic “personnel-on-board” systems.

A1.5 Cargo Management Systems

A1.5.1 Cargo Control Room (CCR) and its equipment

A1.5.2 Level indication system

A1.5.3 Valve remote control system

A1.5.4 Ballast water systems

A1.5.5 Water ingress alarm system.

A1.6 Passenger Servicing and Management Systems

A1.6.1 Property Management System (PMS)

A1.6.2 Electronic health records

A1.6.3 Financial related systems

A1.6.4 Ship passenger/seafarer boarding access systems

A1.6.5 Infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems.

A1.7 Passenger-Facing Networks

A1.7.1 Passenger Wi-Fi or LAN internet access

A1.7.2 Guest entertainment systems

A1.7.3 Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices¹⁸.

A1.7.4 Guest entertainment systems.

A1.8 Core infrastructure systems

A1.8.1 Security gateways

A1.8.2 Routers

A1.8.3 Switches

A1.8.4 Firewalls

A1.8.5 Virtual Private Network(s) (VPN)

A1.8.6 Virtual LAN(s) (VLAN)

A1.8.7 Intrusion prevention systems

A1.8.8 Security event logging systems.

A1.9 Administrative and Crew Welfare Systems

A1.9.1 Administrative systems

A1.9.2 Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

¹⁸ This is not considered as Bring Your Own Device (BYOD). Devices are not used to access protected information. They can only be used for an individual's personal, non-company, use.

Annex 2 Onboard Networks

A secure network depends on the IT/OT set up onboard the ship, and the effectiveness of the company policy based on the outcome of the risk assessment. Control of entry points and physical network control on an existing ship may be limited because cyber security had not been considered during the ship's construction. It is recommended that network layout and network control should be planned for all new buildings.

Direct communication between an uncontrolled and a controlled network should be prevented. Furthermore, several protection measures should be added:

- (a) implement network separation and/or traffic management
- (b) manage encryption protocols to ensure correct level of privacy and commercial communication
- (c) manage use of certificates to verify origin of digitally signed documents, software or services.

In general, only equipment or systems that need to communicate with each other over the network should be able to do so. The overriding principle should be that the networking of equipment or systems is determined by operational need.

A2.1 Physical Layout

The physical layout of the network should be carefully considered. It is important to consider the physical location of essential network devices, including servers, switches, firewalls and cabling. This will help restrict access and maintain the physical security of the network installation and control of entry points to the network.

A2.2 Network Management

Any network design will need to include an infrastructure for administering and managing the network. This may include installing network management software on dedicated workstations and servers providing file sharing, email and other services to the network.

A2.3 Network Segmentation

Onboard networks should normally accommodate the following:

- (a) necessary communication between OT equipment
- (b) configuration and monitoring of OT equipment
- (c) onboard administrative and business tasks including email and sharing business related files or folders
- (d) recreational internet access for crew and/or passengers.

Effective network segmentation is a key aspect of “defence in depth”. OT, IT and public networks should be separated or segmented by appropriate protection measures. The protection measures used may include, but are not limited to an appropriate combination of the following:

- (a) a perimeter firewall between the onboard network and the internet
- (b) network switches between each network segment
- (c) internal firewalls between each network segment
- (d) Virtual Local Area Networks (VLAN) to host separate segments.

In addition, each segment should have its own range of Internet Protocol (IP) addresses. Network segmentation does not remove the need for systems within each segment to be configured with appropriate network access controls and software firewalls and malware detection.

For example, the network was segmented using a perimeter firewall, which supports three VLANs.

- (a) The OT Network containing equipment and systems, that performs safety critical functions.
- (b) The IT network containing equipment and systems, that performs administrative or business functions.
- (c) A crew and guest network, providing uncontrolled internet access.

Considerations should be made on how to maximise the security of the switches themselves. To achieve the highest level of security, each network should use a different hardware switch. This will minimise the chance of an attacker jumping between networks due to misconfiguration or by acquiring access to the configuration of a switch.

A correctly configured and appropriate firewall is an essential element of the proper segmentation of a network installation. The onboard installation should be protected by at least a perimeter firewall to control traffic between the internet and the onboard network. To prevent any unintended communication taking place, the firewall should be configured by default to deny all communication. Based on this configuration, rules should be implemented. The rules should be designed to allow passage of data traffic that is essential for the intended operation of that network.

For example, if a specific endpoint receives updates from the internet, the rule should allow the specific endpoint to connect specifically to the server handling the specific update service. Enabling general internet access to a specified endpoint for updates is bad practice.

Uncontrolled networks like a crew or passenger network should not be allowed any communication with the controlled networks. The uncontrolled network should be considered as unsafe as the internet since the devices connecting to it are unmanaged, their security status (antivirus, updates, etc.) is unknown and their users could be acting maliciously, intentionally or unintentionally.

A2.4 Monitoring Data Activity

It is essential to monitor and manage systems to be aware of the networks' status and to detect any unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network-attached devices so that in case of a breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future.

A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any attacks to the network systems. The IDS and IPS inspect data traffic, entry points or both to identify known threats or to reject traffic, which does not comply with the security policy. An IPS should comply with the latest industry best practices and guidelines.

It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An IDS/IPS sensor could also be placed by a remote-access segment, for instance a Virtual Private Network (VPN).

A2.5 Secure Running Environment

Normally referred to as a sandbox, a secure running environment provides additional protection against cyber threats by isolating executable software from the underlying operating system. This prevents unauthorised access to the operating systems, on which the software is running. The sandbox enables software to be run under a specific set of rules and this adds control over processes and computer resources. Therefore, the sandbox prevents malicious, malfunctioning or untrusted software from affecting the rest of the system.

Annex 3 Cyber Risk Management and the Safety Management System

IMO Resolution MSC.428(98) makes clear that an approved SMS should take into account cyber risk management (CRM) when meeting the objectives and functional requirements of the ISM Code. The guidance provided in this Part on maritime cyber risk management (MSC-FAL.1/Circ.3) provides high level recommendations regarding the elements of an appropriate approach to implementing cyber risk management. The guidance in this annex is designed to provide the minimum measures that all companies should consider implementing so as to address cyber risk management in an approved SMS.

A3.1 Identify¹⁹

A3.1.1 Roles and responsibilities²⁰

Action	Remarks
<p>ISM Code: 3.2 this Part: 1.2 & Ch.2</p> <p>Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks.</p>	<p>An updated safety and environment protection policy should demonstrate:</p> <ul style="list-style-type: none"> • a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment • an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks • an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment. <p>Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company.</p>
<p>ISM Code: 3.3 this Part: 1.2 & Ch.2</p> <p>Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM).</p>	<p>In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems²¹ onboard ships and are responsible for the SMS.</p> <p>Allocation of responsibility and authority may need to be updated to enable CRM. This should include:</p> <ul style="list-style-type: none"> • allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel • incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master.
<p>ISM Code: 6.5 this Part: 6.2</p> <p>Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS.</p>	<p>Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for:</p> <ul style="list-style-type: none"> • all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures • company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority.

A3.1.2 Identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Action	Remarks
--------	---------

¹⁹ Identify, Protect, Detect, Respond and Recover as described in **this Part** on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

²⁰ Functional element from **this Part** on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

²¹ For the purpose of this annex, "critical systems" means the OT, IT, software and data the sudden operational failure or unavailability of which is identified by the company as having the potential to result in hazardous situations.

<p>ISM Code: 10.3 this Part: Ch.4 & Ch.5</p> <p>Using existing company procedures, identify equipment and technical systems (OT and IT) the sudden operational failure of which may result in hazardous situations.</p>	<p>An approved SMS will already identify the equipment and technical systems (including OT and IT), and capabilities, which may cause hazardous situations if they become unavailable or unreliable. The impacts should already have been documented in an approved SMS.</p> <p>However, an approved SMS, which incorporates CRM will also need to address data in the context of sudden operational failure. Loss of availability or integrity of data used by critical systems can have the same impact on safety and protection of the environment as the system becoming unavailable or unreliable for some other reason. Consequently, it is recommended that the list of equipment and technical systems, should be supplemented by a list of the data used by those systems and its source(s).</p>
---	---

A3.2 Protect

A3.2.1 Implement risk control measures

Action	Remarks
<p>ISM Code: 1.2.2.2 this Part: Ch.6 & Annex 1</p> <p>Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.</p>	<p>The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in this Part.</p> <p>As a baseline, the following measures should be considered before a risk assessment is undertaken. The baseline consists of the technical and procedural measures, which should be implemented in all companies to the extent appropriate. These measures are:</p> <ul style="list-style-type: none"> • Hardware inventory – Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. • Software inventory – Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for: <ul style="list-style-type: none"> • maintaining this inventory when hardware controlled by the company is replaced • maintaining this inventory when software controlled by the company is updated or changed • authorizing the installation of new or upgraded software on hardware controlled by the company • prevention of installation of unauthorized software, and deletion of such software if identified • software maintenance. • Map data flows – Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for: <ul style="list-style-type: none"> • maintaining the map of data flows to reflect changes in hardware, software and/or connectivity • identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware • reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance • controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems. • Implement secure configurations for all hardware controlled by the company – This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure

	<p>configurations are included in the SMS. This information should be retained separately and securely by the company.</p> <ul style="list-style-type: none"> ● Audit logs – Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for: <ul style="list-style-type: none"> • policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine • procedures for the collation and retention of security logs by the company, if appropriate. ● Awareness and training – See line 3 above. ● Physical security – The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard.
--	--

A3.2.2 Develop contingency plans

Action	Remarks
<p>ISM Code: 7 this Part: Ch.7</p> <p>Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT.</p>	<p>An approved SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason.</p> <p>Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated.</p> <p>Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines.</p>
<p>ISM Code: 8.1 this Part: Ch.7</p> <p>Update emergency plans to include responses to cyber incidents.</p>	<p>An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into safety management systems. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment.</p> <p>Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary.</p>

A3.3 Detect

A3.3.1 Develop and implement activities necessary to detect a cyber-event in a timely manner.

Action	Remarks
<p>ISM Code: 9.1 this Part: 2.4 & Ch.6</p> <p>Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents.</p>	<p>An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Examples of such non-conformities and cyber incidents:</p> <ul style="list-style-type: none"> ● unauthorised access to network infrastructure ● unauthorised or inappropriate use of administrator privileges ● suspicious network activity ● unauthorised access to critical systems ● unauthorised use of removable media ● unauthorised connection of personal devices ● failure to comply with software maintenance procedures ● failure to apply malware and network protection updates ● loss or disruption to the availability of critical systems ● loss or disruption to the availability of data required by critical systems.

A3.4 Respond

A3.4.1 Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event.

Action	Remarks
<p>ISM Code: 3.3 this Part: 8.2</p> <p>Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems.</p>	<p>An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered:</p> <ul style="list-style-type: none"> ● company or third party technical support should be familiar with onboard IT and OT infrastructure and systems ● any internal response team or external cyber emergency response team (CERT) should be available to provide timely support to the DPA ● provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises ● internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA.
<p>ISM Code: 9.2 this Part: 8.2</p> <p>Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence.</p>	<p>An approved SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective.</p>

<p>ISM Code: 10.3 this Part: 8.2</p> <p>Update the specific measures aimed at promoting the reliability of OT.</p>	<p>An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for:</p> <ul style="list-style-type: none"> ● Software maintenance as a part of operational maintenance routines – Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person. ● Authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks – This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session. ● Preventing the application of software updates by service providers using uncontrolled or infected removable media. ● Periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state. ● Controlled use of administrator privileges to limit software maintenance tasks to competent personnel.
---	---

A3.5 Recovery

A3.5.1 Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident.

Action	Remarks
<p>ISM Code: 10.4 this Part: 2.4, Ch.6 & 8.3</p> <p>Include creation and maintenance of back-ups into the ship's operational maintenance routine.</p>	<p>An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment.</p> <p>A SMS, which incorporates CRM, should include procedures for:</p> <ul style="list-style-type: none"> ● checking back-up arrangements for critical systems, if not covered by existing procedures ● checking alternative modes of operation for critical systems, if not covered by existing procedures ● creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ● maintaining back-ups of data required for critical systems to operate safely ● offline storage of back-ups and clean images, if appropriate ● periodic testing of back-ups and back-up procedures.



財團法人驗船中心

CR CLASSIFICATION SOCIETY

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS

PART II – CYBER RESILIENCE OF SHIPS

CR CLASSIFICATION SOCIETY

December 2025

REVISION HISTORY

(This version supersedes all previous ones.)

Revision No.	Editor	Date (yyyy-mm)
001	Rules Section	2025-12

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS

PART II – CYBER RESILIENCE OF SHIPS

CONTENTS

Chapter 1	General	1
1.1	Introduction.....	1
1.2	Aim and Purpose.....	1
1.3	Scope of Applicability.....	1
1.4	Definitions	3
Chapter 2	Goals and Organization of Requirements	7
2.1	Primary Goal.....	7
2.2	Sub-goals per Functional Element	7
2.3	Organization of Requirements	7
Chapter 3	Requirements for Cyber Resilience of Ships.....	8
3.1	General.....	8
3.2	Identify.....	8
3.3	Protect.....	10
3.4	Detect.....	21
3.5	Respond	24
3.6	Recover	28
Chapter 4	Demonstration of Compliance.....	33
4.1	General.....	33
4.2	During Design and Construction Phases.....	33
4.3	Upon Ship Commissioning	34
4.4	During the Operational Life of the Ship	35
Chapter 5	Risk Assessment for Exclusion of CBS from the Application of Requirements.....	37
5.1	Requirement.....	37
5.2	Rationale	37
5.3	Requirement Details.....	37
5.4	Acceptance Criteria.....	38

Chapter 1 General

1.1 Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

The minimum requirements applied consistently to the full threat surface using a goal-based approach are necessary to make cyber-resilient ships.

1.2 Aim and Purpose

1.2.1 The aim of this Part is to provide a minimum set of requirements for cyber resilience of ships, with the purpose of providing technical means to stakeholders which would lead to cyber-resilient ships.

1.2.2 This Part targets the ship as a collective entity for cyber resilience and is intended as a base for the complementary application of other IACS URs and industry standards addressing cyber resilience of onboard systems, equipment and components.

1.2.3 Minimum requirements for cyber resilience of on-board systems and equipment are given in Part III.

1.3 Scope of Applicability

1.3.1 Ships in scope

- (a) This Part is applicable to the following Ships:
 - (i) Passenger ships (including passenger high-speed craft) engaged in international voyages
 - (ii) Cargo ships of 500 GT and upwards engaged in international voyages
 - (iii) High speed craft of 500 GT and upwards engaged in international voyages
 - (iv) Mobile offshore drilling units of 500 GT and upwards
 - (v) Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc)
- (b) This Part may be used as non-mandatory guidance to the following.
 - (i) Ships of war and troopships

- (ii) Cargo ships less than 500 GT
- (iii) Vessels not propelled by mechanical means
- (iv) Wooden ships of primitive build
- (v) Passenger yachts (passengers not more than 12)
- (vi) Pleasure yachts not engaged in trade
- (vii) Fishing vessels
- (viii) Site specific offshore installations (i.e. FPSOs, FSUs, etc.)

1.3.2 Systems in scope

This Part applies to:

- (a) Operational technology (OT) systems onboard ships, i.e. those CBSs using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

In particular, the CBSs used for the operation of the following ship functions and systems, if present onboard, shall be considered:

- (i) Propulsion
 - (ii) Steering
 - (iii) Anchoring and mooring
 - (iv) Electrical power generation and distribution
 - (v) Fire detection and extinguishing systems
 - (vi) Bilge and ballast systems, loading computer
 - (vii) Watertight integrity and flooding detection
 - (viii) Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
 - (ix) Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)
- (b) In addition, the following systems shall be included in the scope of applicability of this Part:
 - (i) Navigational systems required by statutory regulations
 - (ii) Internal and external communication systems required by class rules and statutory regulations
 - (c) For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in Chapter 4 of Part III may be accepted by the Society, on the condition that requirements in this Part are complied with.
 - (d) Any internet protocol (IP)-based communication interface from CBSs in scope of this Part to other systems. Examples of such systems are, but not limited to, the following:
 - (i) passenger or visitor servicing and management systems
 - (ii) passenger-facing networks
 - (iii) administrative networks
 - (iv) crew welfare systems
 - (v) any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

The cyber incidents considered in this Part are events resulting from any offensive manoeuvre that targets OT systems onboard ships as defined in 1.4.

1.3.3 System category

System categories are defined in IACS UR E22 on the basis of the consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.

1.3.4 IACS documents on computer-based systems and cyber resilience

Attention is made to additional IACS documents on CBSs and Cyber Resilience as follows:

- (a) IACS UR E22 computer-based systems includes requirements for design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. The requirements in E22 focus on the functionality of the software and on the hardware supporting the software which provide control, alarm, monitoring, safety or internal communication functions subject to classification requirements.
- (b) Part III (IACS UR E27 - cyber resilience of on-board systems and equipment) includes requirements for cyber resilience for on-board systems and equipment.
- (c) IACS Recommendation 166 recommendation on cyber resilience: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber-resilient ships, whose resilience can be maintained throughout their service life. IACS Recommendation 166 on cyber resilience is intended for ships contracted for construction after its publication and may be used as a reference for ships already in service prior to its publication. For ships to which this Part applies as mandatory instrument, when both this Part and Recommendation 166 are used, should any difference in requirements addressing the same topic be found between the two instruments, the requirements in this Part shall prevail.

1.3.5 Class notation

For ship complying with the requirements of this Part, the class notation **Cyber-R** will be assigned to the ship.

1.4 Definitions

In the purview of this Part, the following definitions apply:

1.4.1 Annual survey

See Part I of the Rules for Steel Ship.

1.4.2 Attack surface

The set of all possible points where an unauthorized user can access a system, cause an effect on or extract data from. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

1.4.3 Authentication

Provision of assurance that a claimed characteristic of an entity is correct.

1.4.4 Compensating countermeasure

An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

1.4.5 Computer-based system (CBS)

A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs onboard include IT and OT systems. A CBS may be a combination of subsystems connected via network. Onboard CBSs may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBSs and/or other facilities.

1.4.6 Cyber incident

An event resulting from any offensive manoeuvre, either intentional or unintentional, that targets or affects one or more CBS onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard CBS or transported in the networks connecting such systems. Cyber incidents do not include system failures.

1.4.7 Cyber resilience

The capability to reduce the occurrence and mitigating the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

1.4.8 Essential services:

Services for propulsion and steering, and safety of the ship. Essential services comprise "Primary Essential Services" and "Secondary Essential Services": Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering; Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

1.4.9 Information technology (IT)

Devices, software and associated networking focusing on the use of data as information, as opposed to operational technology (OT).

1.4.10 Integrated system

A system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes.

1.4.11 Logical network segment

The same as "network segment", but where two or more logical network segments share the same physical components.

1.4.12 Network

A connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

1.4.13 Network segment

In the context of this Part, a network segment is an OSI layer-2 Ethernet segment (a broadcast domain).

Note on TCP/IP: Network address plan is prefixed by their IP addresses and the network mask. Communication between network segments is only possible by the use of routing service at network layer (OSI Layer 3).

1.4.14 Operational technology (OT)

Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

1.4.15 Physical network segment

The same as "network segment", but where physical components are not shared by other network segments.

1.4.16 Protocol

A common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various fieldbuses.

1.4.17 Security zone

A collection of CBSs in the scope of applicability of this Part that meet the same security requirements. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

1.4.18 Shipowner/Company

The owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The shipowner could be the Shipyard or systems integrator during initial construction. After vessel delivery, the shipowner may delegate some responsibilities to the vessel management company.

1.4.19 Special survey

See Part I of the Rules for Steel Ship.

1.4.20 Supplier

A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The supplier is responsible for providing programmable devices, sub-systems or systems to the systems integrator.

1.4.21 Systems integrator

The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The systems integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role shall be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

1.4.22 Untrusted network

Any network outside the scope of applicability of this Part.

Chapter 2 Goals and Organization of Requirements

2.1 Primary Goal

The primary goal is to support safe and secure shipping, which is operationally resilient to cyber risks. Safe and secure shipping can be achieved through effective cyber risk management system. To support safe and secure shipping resilient to cyber risk, the following sub-goals for the management of cyber risk are defined in the five functional elements listed in 2.2 below.

2.2 Sub-goals per Functional Element

2.2.1 Identify

Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.

2.2.2 Protect

Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.

2.2.3 Detect

Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.

2.2.4 Respond

Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.

2.2.5 Recover

Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.

These sub-goals and relevant functional elements should be concurrent and considered as parts of a single comprehensive risk management framework.

2.3 Organization of Requirements

The requirements are organized according to a goal-based approach. Functional/technical requirements are given for the achievement of specific sub-goals of each functional element. The requirements are intended to allow a uniform implementation by stakeholders and to make them applicable to all types of vessels, in such a way as to enable an acceptable level of resilience and apply to all classed vessels/units regardless of operational risks and complexity of OT systems.

For each requirement, a rationale is given.

A summary of actions to be carried out and documentation to be made available is also given for each phase of the ship's life and relevant stakeholders participating to such phase.

Chapter 3 Requirements for Cyber Resilience of Ships

3.1 General

This Chapter contains the requirements to be satisfied in order to achieve the primary goal defined in 2.1, organized according to the five functional elements identified in 2.2.

The requirements shall be fulfilled by the stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified (see also 1.4 for definitions):

- Shipowner/Company
- Systems integrator
- Supplier
- Classification Society

Whilst the above requirements may be fulfilled by these stakeholders, for the purposes of this Part, responsibility to fulfil them will lie with the stakeholder who has contracted with the Classification Society.

3.2 Identify

The requirements for the 'Identify' functional element are aimed at identifying: on one side, the CBSs onboard, their interdependencies and the relevant information flows; on the other side, the key resources involved in their management, operation and governance, their roles and responsibilities.

3.2.1 Vessel asset inventory

(a) Requirement

An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the CBSs in the scope of applicability of this Part and of the networks connecting such systems to each other and to other CBSs onboard or ashore shall be provided and kept up to date during the entire life of the ship.

(b) Rationale

The inventory of CBSs onboard and relevant software used in OT systems, is essential for an effective management of cyber resilience of the ship, the main reason being that every CBS becomes a potential point of vulnerability. Cybercriminals can exploit unaccounted and out-of-date hardware and software to hack systems. Moreover, managing CBS assets enables companies understand the criticality of each system to ship safety objectives.

(c) Requirement details

The vessel asset inventory shall include at least the CBSs indicated in 1.3.2, if present onboard. The inventory shall be kept updated during the entire life of the ship. software and hardware modifications potentially introducing new vulnerabilities or modifying functional dependencies or connections among systems shall be recorded in the inventory.

If confidential information is included in the inventory (e.g. IP addresses, protocols, port numbers), special measures shall be adopted to limit the access to such information only to authorized people.

(i) Hardware

For all hardware devices in the scope of applicability of this Part, the vessel asset inventory shall include at least the information in 3.1.1 of Part III.

In addition, the vessel asset inventory may specify system category and security zone associated with the CBS.

(ii) Software

For all software in the scope of applicability of this Part (e.g., application program, operating system, firmware), the vessel asset inventory shall include at least the information in 3.1.1 of Part III.

The software of the CBSs in the scope of applicability of this Part shall be maintained and updated in accordance with the shipowner's process for management of software maintenance and update policy in the Ship cyber security and resilience program, see 4.4.2.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall submit vessel asset inventory to the Society (ref. 4.2.3).

The vessel asset inventory shall incorporate the asset inventories of all individual CBSs falling under the scope of this Part. Any equipment in the scope of this Part delivered by the systems integrator shall also be included in the vessel asset inventory.

(ii) Construction phase

The systems integrator shall keep the vessel asset inventory updated.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that:

- (1) Vessel asset inventory is updated and completed at delivery
- (2) CBSs in the scope of applicability of this Part are correctly represented by the vessel asset inventory
- (3) Software of the CBSs in the scope of applicability of this Part has been kept updated, e.g. by vulnerability scanning or by checking the software versions of CBSs while switched on.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) The shipowner shall in the Ship cyber security and resilience program describe the process of management of change (MoC) for the CBSs in the scope of applicability of this Part, addressing at least the following requirements in this Part:

- a) Management of change (4.4)
- b) Hardware and software modifications (3.2.1(c))

(2) The shipowner shall in the Ship cyber security and resilience program also describe the management of software updates, addressing at least the following requirements in this Part:

- a) Vulnerabilities and cyber risks (3.2.1(b) and 3.2.1(c))
- b) Security patching (3.3.6(c)(v))

(3) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- a) The approved management of change process has been adhered to.
- b) Known vulnerabilities and functional dependencies have been considered for the software in the CBSs.
- c) The Vessel asset inventory has been kept updated.

(4) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

(5) Special Survey

The shipowner shall demonstrate to the Society the activities in 3.2.1(d)(iii) as per the Ship cyber resilience test procedure.

3.3 Protect

The requirements for the Protect functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential incident.

3.3.1 Security zones and network segmentation

(a) Requirement

All CBSs in the scope of applicability of this Part shall be grouped into security zones with well-defined security policies and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.) Only explicitly allowed traffic shall traverse a security zone boundary.

(b) Rationale

While networks may be protected by firewall perimeter and include Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to monitor traffic coming in, breaching that perimeter is always possible. Network segmentation makes it more difficult for an attacker to perpetrate an attack throughout the entire network.

The main benefits of security zones and network segmentation are to reduce the extent of the attack surface, prevent attackers from achieving lateral movement through systems, and improve network performance. The concept of allocating the CBSs into security zones allows grouping the CBSs in accordance with their risk profile.

(c) Requirement details

A security zone may contain multiple CBSs and networks, all of which shall comply with applicable security requirements given in this Part and Part III.

The network(s) of a security zone shall be logically or physically segmented from other zones or networks. See also 3.3.6(c).

CBSs providing required safety functions shall be grouped into separate security zones and shall be physically segmented from other security zones.

Navigational and communication systems shall not be in same security zone as machinery or cargo systems. If navigation and/or radiocommunication systems are approved in accordance with other equivalent standard(s) (see 1.3.2), these systems should be in a dedicated security zone.

Wireless devices shall be in dedicated security zones. See also 3.3.5.

Systems, networks or CBSs outside the scope of applicability of this Part are considered untrusted networks and shall be physically segmented from security zones required by this Part. Alternatively, it is accepted that such systems are part of a security zone if these OT systems meet the same requirements as demanded by the zone.

It shall be possible to isolate a security zone without affecting the primary functionality of the CBSs in the zone, see also 3.5.3.

(d) Demonstration of compliance

(i) Design phase

- (1) The systems integrator shall submit zones and conduit diagram and the cyber security design description (see 4.2.1 and 4.2.2).
- (2) The zones and conduit diagram shall illustrate the CBSs in the scope of applicability of this Part, how they are grouped into security zones, and include the following information:
 - a) Clear indication of the security zones
 - b) Simplified illustration of each CBS in scope of applicability of this Part, and indication of the security zone in which the CBS is allocated, and indication of physical location of the CBS/equipment.
 - c) Reference to the approved version of the CBS system topology diagrams provided by the suppliers (3.1.2 of Part III)
 - d) Illustration of network communication between systems in a security zone
 - e) Illustration of any network communication between systems in different security zones (conduits).
 - f) Illustration of any communication between systems in a security zone and untrusted networks (conduits).
- (3) The systems integrator shall include the following information in the cyber security design description:
 - a) A short description of the CBSs allocated to the security zone. It shall be possible to identify each CBS in the zones and conduit diagram.
 - b) Network communication between CBSs in the same security zone. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication.
 - c) Network communication between CBSs in different security zones. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication. The description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).
 - d) Any communication between CBSs in security zones and untrusted networks. The description shall include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

(ii) Construction phase

The systems integrator shall keep the zones and conduit diagram updated.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that:

- (1) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.
- (2) Security zone boundaries allow only the traffic that has been documented in the approved cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

- (1) The shipowner shall in the Ship cyber security and resilience program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this Part:

- a) Principle of least functionality (3.3.2(a))
 - b) Explicitly allowed traffic (3.3.1(a))
 - c) Protection against denial of service (DoS) events (3.3.2(a))
 - d) Inspection of security audit records (3.4.1(c))
- (2) First annual survey
The shipowner shall demonstrate to the Society that the zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.
- (3) Subsequent annual surveys
The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
- (4) Special survey
The shipowner shall demonstrate to the Society the activities in 3.3.1(d)(iii) as per the Ship cyber resilience test procedure.

3.3.2 Network protection safeguards

(a) Requirement

Security zones shall be protected by firewalls or equivalent means as specified in 3.3.1.

The networks shall also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources.

The CBSs in scope of this Part shall be implemented in accordance with the principle of least functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.

(b) Rationale

Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities.

There are many layers to consider when addressing network protection. Attacks can happen at any layer in the network layers model, so network hardware, software and policies must be designed to address each area.

While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour.

(c) Requirement details

The design of network shall include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format.

(d) Demonstration of compliance

(i) Design phase

No requirements.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate the following to the Society:

- (1) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.
- (2) Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests shall cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network).
- (3) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the CBSs have been removed or prohibited in accordance with hardening guidelines provided by the suppliers. See 5.1.2(g) and 6.4.1(k) of Part III.

The second and third tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.3.2(d)(iii) as per the Ship cyber resilience test procedure.

3.3.3 Antivirus, antimalware, antispam and other protections from malicious code

(a) Requirement

CBSs in the scope of applicability of this Part shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.

(b) Rationale

- (i) A virus or any unwanted program that enters a user's system without his/her knowledge can self-replicate and spread, perform unwanted and malicious actions that end up affecting the system's performance, user's data/files, and/or circumvent data security measures.
- (ii) Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off the malicious intruding viruses performing a prophylactic function. It detects potential virus and then works to remove it, mostly before the virus gets to harm the system.
- (iii) Common means for malicious code to enter CBSs are electronic mail, electronic mail attachments, websites, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops.

(c) Requirement details

- (i) Malware protection shall be implemented on CBSs in the scope of applicability of this Part. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for Cat.II and Cat.III CBSs performing real-time tasks).
- (ii) On CBSs where anti-virus and anti-malware software cannot be installed, malware protection shall be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the cyber security design description:

- (1) For each CBS, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.
 - (2) For CBSs with anti-malware software, information about how to keep the software updated.
 - (3) Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.
- (ii) Construction phase
- The systems integrator shall ensure that malware protection is kept updated during the construction phase.
- (iii) Commissioning phase
- The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate the following to the Society:
- (1) Approved anti-malware software or other compensating countermeasures is effective (test e.g., with a trustworthy anti-malware test file).
 - (2) The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.
- (iv) Operation phase
- For general requirements to surveys in the operation phase, see 4.4.
- (1) The shipowner shall in the Ship cyber security and resilience program describe the management of malware protection, addressing at least the following requirements in this Part:
 - a) Maintenance/update (3.3.3(c))
 - b) Operational procedures, physical safeguards (3.3.3(c))
 - c) Use of mobile, portable, removable media (3.3.4(c)(iv) and 3.3.7(c))
 - d) Access control (3.3.4)
 - (2) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

 - a) Any anti-malware software has been maintained and updated.
 - b) Procedures for use of portable, mobile or removable devices have been followed.
 - c) Policies and procedures for access control have been followed.
 - d) Physical safeguards are maintained.
 - (3) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
 - (4) Special survey

The shipowner shall demonstrate to the Society the activities in 3.3.3(d)(iii) as per the Ship cyber resilience test procedure.

3.3.4 Access control

(a) Requirement

CBSs and networks in the scope of applicability of this Part shall provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures shall be such as not to hamper the ability of authorized personnel to access CBS for their level of access according to the least privilege principle.

(b) Rationale

- (i) Attackers may attempt to access the ship's systems and data from either onboard the ship, within the company, or remotely through connectivity with the internet. Physical and logical access controls to cyber assets, networks etc. should then be implemented to ensure safety of the ship and its cargo.
 - (ii) Physical threats and relevant countermeasures are also considered in the ISPS Code. Similarly, the ISM Code contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of ISPS and ISM Codes may imply inclusion in the Ship Security Plan (SSP) and Safety Management System (SMS) of instructions and procedures for access control to safety critical assets.
- (c) Requirement details
- Access to CBSs and networks in the scope of applicability of this Part and all information stored on such systems shall only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality.
- (i) Physical access control

CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.
 - (ii) Physical access control for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.
 - (iii) Physical access control of network access points

Access points to onboard networks connecting Cat.II and/or Cat.III CBSs shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance.

Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, shall be used in case of occasional connection requested by a visitor (e.g. for printing documents).
 - (iv) Removable media controls

A policy for the use of removable media devices shall be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. See also 3.3.7.
 - (v) Management of credentials
 - (1) CBSs and relevant information shall be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel shall be left active only for a limited period according to the role and responsibility of the account holder and shall be removed when no longer needed.

Note: CBSs shall identify and authenticate human users as per item No.1 in Table III 4-1 of Part III. In other words, it is not necessary to "uniquely" identify and authenticate all human users.
 - (2) Onboard CBSs shall be provided with appropriate access control that fits to the policy of their security zone but does not adversely affect their primary purpose. CBSs which require strong access control may need to be secured using a strong encryption key or multi-factor authentication.
 - (3) Administrator privileges shall be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the CBS, who as part of their role in the company or onboard need to log on to systems using these privileges.

- (vi) Least privilege principle
 - (1) Any human user allowed to access CBS and networks in the scope of applicability of this Part shall have only the bare minimum privileges necessary to perform its function.
 - (2) The default configuration for all new account privileges shall be set as low as possible. Wherever possible, raised privileges shall be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time shall be avoided, e.g. by regular auditing of user accounts.

- (d) Demonstration of compliance
 - (i) Design phase

The systems integrator shall include the following information in the cyber security design description: Location and physical access controls for the CBSs. Devices providing Human Machine Interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices shall be specified.
 - (ii) Construction phase

The systems integrator shall prevent unauthorised access to the CBSs during the construction phase.
 - (iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate the following to the Society:

 - (1) Components of the CBSs are located in areas or enclosures where physical access can be controlled to authorised personnel.
 - (2) User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of CBSs as per 4.3.2).
 - (iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

 - (1) The shipowner shall in the Ship cyber security and resilience program describe the management of logical and physical access, addressing at least the following requirements in this Part:
 - a) Physical access control (3.3.4(c)(i))
 - b) Physical access control for visitors (3.3.3(d)(ii))
 - c) Physical access control of network access points (3.3.4(c)(iii))
 - d) Management of credentials (3.3.4(c)(v))
 - e) Least privilege policy (3.3.4(c)(vi))
 - (2) The shipowner shall in the Ship cyber security and resilience program describe the management of confidential information, addressing at least the following requirements in this Part:
 - a) Confidential information (3.2.1(c))
 - b) Information allowed to authorized personnel (3.3.4(c))
 - c) Information transmitted on the wireless network (3.3.5(c))
 - (3) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

 - a) Any anti-malware software has been maintained and updated.
 - b) Personnel are authorized to access the CBSs in accordance with their responsibilities.
 - c) Only authorised devices are connected to the CBSs.
 - d) Visitors are given access to the CBSs according to relevant policies and procedures.
 - e) Physical access controls are maintained and applied.
 - f) Credentials, keys, secrets, certificates, relevant CBS documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures.

(4) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

3.3.5 Wireless communication

(a) Requirement

Wireless communication networks in the scope of this Part shall be designed, implemented and maintained to ensure that:

- (i) Cyber incidents will not propagate to other control systems
- (ii) Only authorised human users will gain access to the wireless network
- (iii) Only authorised processes and devices will be allowed to communicate on the wireless network
- (iv) Information in transit on the wireless network cannot be manipulated or disclosed

(b) Rationale

- (i) Wireless networks give rise to additional or different cybersecurity risks than wired networks. This is mainly due to less physical protection of the devices and the use of the radio frequency communication.
- (ii) Inadequate physical access control may lead to unauthorised personnel gaining access to the physical devices, which in turn could lead to circumventing logical access restrictions or deployment of rogue devices on the network.
- (iii) Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn could cater for attacks such as Piggybacking or Evil twin attacks (see <https://us-cert.cisa.gov/ncas/tips/ST05-003>).

(c) Requirement details

- (i) Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices shall be applied to ensure integrity and confidentiality of the information transmitted on the wireless network.
- (ii) Devices on the wireless network shall only communicate on the wireless network (i.e. they shall not be "dual-homed")
- (iii) Wireless networks shall be designed as separate segments in accordance with 3.3.1 and protected as per 3.3.2.
- (iv) Wireless access points and other devices in the network shall be installed and configured such that access to the network can be controlled.
- (v) The network device or system utilizing wireless communication shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the cyber security design description: Description of wireless networks in the scope of applicability of this Part and how these are implemented as separate security zones. The description shall include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules)

(ii) Construction phase

The systems integrator shall prevent unauthorised access to the wireless networks during the construction phase.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate the following to the Society:

- (1) Only authorised devices can access the wireless network.
- (2) Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the wireless networks in the scope of applicability of this Part, the shipowner shall demonstrate to the Society the activities in 3.3.5(d)(iii) as per the Ship cyber resilience test procedure.

3.3.6 Remote access control and communication with untrusted networks

(a) Requirement

CBSs in scope of this Part shall be protected against unauthorized access and other cyber threats from untrusted networks.

(b) Rationale

Onboard CBSs have become increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions. The use of digital systems to monitor and control onboard CBSs makes them vulnerable to cyber incidents. Attackers may attempt to access onboard CBSs through connectivity with the internet and may be able to make changes that affect a CBS's operation or even achieve full control of the CBS, or attempt to download information from the ship's CBS. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects cyber resilience, special care should be put to relevant hardware and software installations on board to help maintain a sufficient level of cyber resilience when such systems can be remotely accessed, also keeping in mind that not all cyber incidents are a result of a deliberate attack.

(c) Requirement details

- (i) User's manual shall be delivered for control of remote access to onboard IT and OT systems. Clear guidelines shall identify roles and permissions with functions.
- (ii) For CBSs in the scope of applicability of this Part, no IP address shall be exposed to untrusted Networks.
- (iii) Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality shall be ensured for information that is subject to read authorization.
- (iv) Design phase
CBSs in the scope of applicability of this Part shall:
 - (1) have the capability to terminate a connection from the onboard connection endpoint. Any remote access shall not be possible until explicitly accepted by a responsible role on board.
 - (2) be capable of managing interruptions during remote sessions so as not to compromise the safe functionality of OT systems or the integrity and availability of data used by OT systems.
 - (3) provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident.

(v) Additional requirements for remote maintenance

When remote access is used for maintenance, the following requirements shall be complied with in addition to those in 3.3.6(c)(iv):

- (1) Documentation shall be provided to show how they connect and integrate with the shore side.
- (2) Security patches and software updates shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects or cyber events that cannot be tolerated. A confirmation report from the software supplier towards above shall be obtained, prior to undertaking remote update.
- (3) Suppliers shall provide plans for- and make security updates available to the shipowner, see 5.1.2(b), 5.1.2(c) and 5.1.2(d) of Part III.
- (4) At any time, during remote maintenance activities, authorized personnel shall have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of the CBS and systems involved.
- (5) Multi-factor authentication is required for any access by human users to CBS's in scope from an untrusted network.
- (6) After a configurable number of failed remote access attempts, the next attempt shall be blocked for a predetermined length of time.
- (7) If the connection to the remote maintenance location is disrupted for some reason, access to the system shall be terminated by an automatic logout function.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the cyber security design description:

- (1) Identification of each CBS in the scope of applicability of this Part that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.
- (2) For each CBS, a description of compliance with requirements in 3.3.6(c), as applicable.

(ii) Construction phase

The systems integrator shall ensure that any communication with untrusted networks is only temporarily enabled and used in accordance with the requirements of this Chapter.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate the following to the Society:

- (1) Communication with untrusted networks is secured in accordance with 4.3 of Part III and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).
- (2) Remote access requires multifactor authentication of the remote user.
- (3) A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.
- (4) Remote connections must be explicitly accepted by responsible personnel on board.
- (5) Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.
- (6) Remote sessions are logged (see item 13 of Table III 4-1 of Part III).
- (7) Instructions or procedures are provided by the respective product suppliers (see 3.1.3 of Part III).

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

- (1) The shipowner shall in the Ship cyber security and resilience program describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements in this Part:

- a) User's manual (3.3.6(c))
 - b) Roles and permissions (3.3.6(c))
 - c) Patches and updates (3.3.6(c)(v))
 - d) Confirmation prior to undertaking remote software update (3.3.6(c)(v))
 - e) Interrupt, abort, roll back (3.3.6(c)(v))
- (2) First annual survey
- The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
- a) Remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals.
 - b) Installation of security patches and other software updates have been carried out in accordance with management of change procedures and in cooperation with the supplier.
- (3) Annual survey
- The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
- (4) Special survey
- The shipowner shall demonstrate to the Society the activities in 3.3.6(d)(iii) as per the Ship cyber resilience test procedure.

3.3.7 Use of Mobile and Portable Devices

(a) Requirement

The use of mobile and portable devices in CBSs in the scope of applicability of this Part shall be limited to only necessary activities and be controlled in accordance with item 10 of Table III 4-1 of Part III. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked.

(b) Rationale

It is generally known that CBSs can be impaired due to malware infection via a mobile or a portable device. Therefore, connection of mobile and portable devices should be carefully considered. In addition, mobile equipment that is required to be used for the operation and maintenance of the ship should be under the control of the shipowner.

(c) Requirement details

Mobile and portable devices shall only be used by authorised personnel. Only authorised devices may be connected to the CBSs. All use of such devices shall be in accordance with the shipowner's policy for use of mobile and portable devices, taking into account the risk of introducing malware in the CBS.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the Cyber security design description: Any CBSs in the scope of applicability that do not meet the requirements in item 10 of Table III 4-1 of Part III, i.e., that shall have protection of interface ports by physical means such as port blockers.

(ii) Construction phase

The systems integrator shall ensure that use of physical interface ports in the CBSs is controlled in accordance with item 10 of Table III 4-1 of Part III, and that any use of such devices follows procedures to prevent malware from being introduced in the CBS.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures shall be demonstrated as relevant:

- (1) Use of mobile and portable devices is restricted to authorised users
- (2) Interface ports can only be used by specific device types
- (3) Files cannot be transferred to the system from such devices
- (4) Files on such devices will not be automatically executed (by disabling autorun)
- (5) Network access is limited to specific MAC or IP addresses
- (6) Unused interface ports are disabled
- (7) Unused interface ports are physically blocked

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) The shipowner shall in the Ship cyber security and resilience program describe the management of mobile and portable devices, addressing at least the following requirements in this Part:

- a) Policy and procedures (3.3.4(c)(iv))
- b) Physical block of interface ports (3.3.7(a))
- c) Use by authorized personnel (3.3.7(c))
- d) Connect only authorized devices (3.3.7(c))
- e) Consider risk of introducing malware (3.3.7(c))

(2) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- a) The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures.
- b) Only authorised devices are connected to the CBSs.
- c) Means to restrict use of physical interface ports are implemented as per approved design documentation.

(3) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

(4) Special survey

The shipowner shall demonstrate to the Society the activities in 3.3.7(d)(iii) as per the Ship cyber resilience test procedure.

3.4 Detect

The requirements for the Detect functional element are aimed at the development and implementation of appropriate means supporting the ability to reveal and recognize anomalous activity on CBSs and networks onboard and identify cyber incidents.

3.4.1 Network operation monitoring

(a) Requirement

Networks in scope of this Part shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.

(b) Rationale

Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction could result in incidents where the vessel is illprepared for the threat. To enable an early response to attacks targeting these types of unknown vulnerabilities, technology capable of detecting unusual events is required. A monitoring system that can detect anomalies in networks and that can use post-incident analysis provides the ability to appropriately respond and further recover from a cyber event.

(c) Requirement details

(i) Measures to monitor networks in the scope of applicability of this Part shall have the following capabilities:

- (1) Monitoring and protection against excessive traffic
- (2) Monitoring of network connections
- (3) Monitoring and recording of device management activities
- (4) Protection against connection of unauthorized devices
- (5) Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See UR E22 section 7.2.1.

(ii) Intrusion detection systems (IDS) may be implemented, subject to the following:

- (1) The IDS shall be qualified by the supplier of the respective CBS
- (2) The IDS shall be passive and not activate protection functions that may affect the performance of the CBS
- (3) Relevant personnel should be trained and qualified for using the IDS

(d) Demonstration of compliance

(i) Design phase

No requirements.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall specify in the Ship cyber resilience test procedure and demonstrate to the Society the network monitoring and protection mechanisms in the CBSs.

- (1) Test that disconnected network connections will activate alarm and that the event is recorded.
- (2) Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test in 3.5.4(d)(iii).
- (3) Demonstrate that the CBS will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also 3.3.2(d)(iii))
- (4) Demonstrate generation of audit records (logging of security-related events)
- (5) If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the CBSs.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2. Any Intrusion detection systems in the CBSs in scope of applicability to be implemented shall be subject to verification by the Society. Relevant documentation shall be submitted for approval, and survey/tests shall be carried out on board.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

- (1) The shipowner shall in the Ship cyber security and resilience program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this Part:
 - a) Reveal and recognize anomalous activity (3.4)
 - b) Inspection of security audit records (3.4.1(c))
 - c) Instructions or procedures to detect incidents (3.5.1(a))The above activities may be addressed together with incident response in 3.5.1.
- (2) First annual survey
The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
The CBSs are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the CBSs.
- (3) Subsequent annual surveys
The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
- (4) Special survey
Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.4.1(d)(iii) as per the Ship cyber resilience test procedure.

3.4.2 Verification and diagnostic functions of CBS and networks

(a) Requirement

CBSs and networks in the scope of applicability of this Part shall be capable to check performance and functionality of security functions required by this Part. Diagnostic functions shall provide adequate information on CBSs integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.

(b) Rationale

The ability to verify intended operation of the security functions is important to support management of cyber resilience in the lifetime of the ship. Tools for diagnostic functions may comprise automatic or manual functions such as self-diagnostics capabilities of each device, or tools for network monitoring (such as ping, traceroute, ipconfig, netstat, nslookup, wireshark, nmap, etc.).

It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the CBS.

(c) Requirement details

CBSs and networks' diagnostics functionality shall be available to verify the intended operation of all required security functions during test and maintenance phases of the ship.

(d) Demonstration of compliance

(i) Design phase

No requirements.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society the effectiveness of the procedures for verification of security functions provided by the

suppliers.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) The shipowner shall in the Ship cyber security and resilience program describe the management activities to verify correct operation of the security functions in the CBSs and networks, addressing at least the following requirements in this Part:

- a) Test and maintenance periods (3.4.2(c))
- b) Periodic maintenance (4.4.4)

(2) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

The security functions in the CBSs are periodically tested or verified.

(3) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

3.5 Respond

The requirements for the Respond functional element are aimed at the development and implementation of appropriate means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of CBSs and networks onboard.

3.5.1 Incident response plan

(a) Requirement

An incident response plan shall be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan shall contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBSs in the scope of applicability of this Part.

(b) Rationale

An incident response plan is an instrument aimed to help responsible persons respond to cyber incidents. As such, the Incident response plan is as effective as it is simple and carefully designed. When developing the Incident response plan, it is important to understand the significance of any cyber incident and prioritize response actions accordingly.

Means for maintaining as much as possible the functionality and a level of service for a safe operation of the ship, e.g. transfer active execution to a standby redundant unit, should also be indicated. Designated personnel ashore should be integrated with the ship in the event of a cyber incident.

(c) Requirement details

- (i) The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the Incident Response Plan to be placed onboard at the first annual Survey. The Incident Response Plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.
- (ii) The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.

- (iii) The incident response plan shall, as a minimum, include the following information:
 - (1) Breakpoints for the isolation of compromised systems;
 - (2) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events;
 - (3) A description of expected major consequences related to cyber incidents;
 - (4) Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any.
 - (5) Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable;

The Incident response plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the Cyber security design description: References to information provided by the suppliers (see 3.1.8 of Part III) that may be applied by the shipowner to establish plans for incident response.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

No requirements.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

- (1) The shipowner shall in the Ship cyber security and resilience program describe incident response plans. The plans shall cover the CBSs in scope of applicability of this Part and shall address at least the following requirements in this Part:

- a) Description of who, when and how to respond to cyber incidents in accordance with requirements of 3.5.1.
- b) Procedures or instructions for local/manual control in accordance with requirements in 3.5.2.
- c) Procedures or instructions for isolation of security zones in accordance with requirements in 3.5.3.
- d) Description of expected behaviour of the CBSs in the event of cyber incidents in accordance with requirements in 3.5.4.

- (2) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- a) The incident response plans are available for the responsible personnel onboard.
- b) Procedures or instructions for local/manual controls are available for responsible personnel onboard.
- c) Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.
- d) Any cyber incidents have been responded to in accordance with the incident response plans.

- (3) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

3.5.2 Local, independent and/or manual operation

(a) Requirement

Any CBS needed for local backup control as required by SOLAS II-1 Regulation 31 shall be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation.

(b) Rationale

Independent local controls of machinery and equipment needed to maintain safe operation is a fundamental principle for manned vessels. The objective of this requirement has traditionally been to ensure that personnel can cope with failures and other incidents by performing manual operations in close vicinity of the machinery. Since incidents caused by malicious cyber events should also be considered, this principle of independent local control is no less important.

(c) Requirement details

- (i) The CBS for local control and monitoring shall be self-contained and not depend on communication with other CBS for its intended operation.
- (ii) If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in 3.3.1 and 3.3.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone. Notwithstanding the above, special considerations can be given to CBSs with different concepts on case by case basis
- (iii) The CBS for local control and monitoring shall otherwise comply with requirements in this Part.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the Cyber security design description: Description of how the local controls specified in SOLAS II-1 Reg.31 are protected from cyber incidents in any connected remote or automatic control systems.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that the required local controls in the scope of applicability of this Part needed for safety of the ship can be operated independently of any remote or automatic control systems. The tests shall be carried out by disconnecting all networks from the local control system to other systems/devices.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.5.2(d)(iii) as per the Ship cyber resilience test procedure.

3.5.3 Network isolation

(a) Requirement

It shall be possible to terminate network-based communication to or from a security zone.

(b) Rationale

In the event that a security breach has occurred and is detected, it is likely that the incident response plan includes actions to prevent further propagation and effects of the incident. Such actions could be to isolate network segments and control systems supporting essential functions.

(c) Requirement details

- (i) Where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner.
- (ii) Individual system's data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the Cyber security design description: Specification of how to isolate each security zone from other zones or networks. The effects of such isolation shall also be described, demonstrating that the CBSs in a security zone do not rely on data transmitted by IP-networks from other zones or networks.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society by disconnecting all networks traversing security zone boundaries, that the CBSs in the security zone will maintain adequate operational functionality without network communication with other security zones or networks.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.5.3(d)(iii) as per the Ship cyber resilience test procedure.

3.5.4 Fallback to a minimal risk condition

(a) Requirement

In the event of a cyber incident impairing the ability of a CBS or network in the scope of applicability of this Part to provide its intended service, the affected system or network shall fall back to a minimal risk condition, i.e. bring itself in a stable, stopped condition to reduce the risk of possible safety issues.

(b) Rationale

The ability of a CBS and integrated systems to fallback to one or more minimal risk conditions to be reached in case of unexpected or unmanageable failures or events is a safety measure aimed to keep the system in a consistent, known and safe state.

Fallback to a minimal risk condition usually implies the capability of a system to abort the current operation and signal the need for assistance, and may be different depending on the environmental conditions, the voyage phase of the ship (e.g. port depart/arrival vs. open sea passage) and the events occurred.

(c) Requirement details

- (i) As soon as a cyber incident affecting the CBS or network is detected, compromising the system's ability to provide the intended service as required, the system shall fall back to a condition in which a reasonably safe state can be achieved. Fall-back actions may include:
 - (1) bringing the system to a complete stop or other safe state;
 - (2) disengaging the system;
 - (3) transferring control to another system or human operator;
 - (4) other compensating actions.
- (ii) Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition.
- (iii) The ability of a system to fall back to a minimal risk condition shall be considered from the design phase by the supplier and the systems integrator.

(d) Demonstration of compliance

- (i) Design phase
The systems integrator shall include the following information in the Cyber security design description: Specification of safe state for the control functions in the CBSs in the scope of applicability of this Part.
- (ii) Construction phase
No requirements.
- (iii) Commissioning phase
The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that CBSs in the scope of applicability of this Part respond to cyber incidents in a safe manner (as per 3.5.4(d)(i)), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests shall at least include denial of service (DoS) attacks and may be done together with related test in 3.4.1(d)(iii).
The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.
- (iv) Operation phase
For general requirements to surveys in the operation phase, see 4.4.
 - (1) Special survey
Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.5.4(d)(iii) as per the Ship cyber resilience test procedure.

3.6 Recover

The requirements for the Recover functional element are aimed at the development and implementation of appropriate means supporting the ability to restore CBSs and networks onboard affected by cyber incidents.

3.6.1 Recovery plan

(a) Requirement

A recovery plan shall be made by the shipowner to support restoring CBSs under the scope of applicability of this Part to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom shall be part of the recovery plan.

(b) Rationale

Incident response procedures are an essential part of system recovery. Responsible personnel should consider carefully and be aware of the implications of recovery actions (such as wiping of drives) and execute them carefully.

It should be noted, however, that some recovery actions may result in the destruction of evidence that could provide valuable information on the causes of an incident.

Where appropriate, external cyber incident response support should be obtained to assist in preservation of evidence whilst restoring operational capability.

(c) Requirement details

- (i) The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the recovery plan to be placed onboard at the first annual Survey. The recovery plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.
- (ii) Recovery plans shall be easily understandable by the crew and external personnel and include essential instructions and procedures to ensure the recovery of a failed system and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board shall be available.
- (iii) When developing recovery plans, the various systems and subsystems involved shall be specified. The following recovery objectives shall also be specified:
 - (1) System recovery: methods and procedures to recover communication capabilities shall be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.
 - (2) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation shall be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.
- (iv) Once the recovery objectives are defined, a list of potential cyber incidents shall be created, and the recovery procedure developed and described. Recovery plans shall include, or refer to the following information:
 - (1) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.
 - (2) Processes and procedures for the backup and secure storage of information.
 - (3) Complete and up-to-date logical network diagram.
 - (4) The list of personnel responsible for restoring the failed system.
 - (5) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.
 - (6) Current configuration information for all components.The operation and navigation of the ship shall be prioritized in the plan in order to help ensure the safety of onboard personnel.
- (v) Recovery plans in hard copy onboard and ashore shall be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

(d) Demonstration of compliance

- (i) Design phase
The systems integrator shall include the following information in the Cyber security design description: references to information provided by the suppliers (see 3.1.8 of Part III) that may be applied by the shipowner to establish plans to recover from cyber incidents.
- (ii) Construction phase
No requirements.
- (iii) Commissioning phase
The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to

cyber incidents as specified in 3.6.2 and 3.6.3.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) The shipowner shall in the Ship cyber security and resilience program describe incident recovery plans. The plans shall cover the CBSs in scope of applicability of this Part and shall address at least the following requirements in this Part:

- a) Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in 3.6.1.
- b) Policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of the CBSs in accordance with requirements in 3.6.2.
- c) Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in 3.6.2 and 3.6.3.

(2) First annual survey

The shipowner shall present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

- a) Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.
- b) Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.
- c) Backup of the CBSs have been taken in accordance with the policies and procedures.
- d) Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.

(3) Subsequent annual surveys

The shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

3.6.2 Backup and restore capability

(a) Requirement

CBSs and networks in the scope of applicability of this Part shall have the capability to support back-up and restore in a timely, complete and safe manner. Backups shall be regularly maintained and tested.

(b) Rationale

In general, the purpose of a backup and restore strategy should protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following: Planning and testing responses to different kinds of failures; Configuring the database environment for backup and recovery; Setting up a backup schedule; Monitoring the backup and recovery environment; Creating a database copy for long-term storage; Moving data from one database or one host to another, etc.

(c) Requirement details

(i) Restore capability

- (1) CBSs in the scope of applicability of this Part shall have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident.
- (2) Data shall be restorable from a secure copy or image.
- (3) Information and backup facilities shall be sufficient to recover from a cyber incident.

(ii) Backup

- (1) CBSs and networks in the scope of applicability of this Part shall provide backup for data. The use of offline backups shall also be considered to improve tolerance against ransomware and worms affecting online backup appliances.
- (2) Backup plans shall be developed, including scope, mode and frequency, storage medium and retention period.

(d) Demonstration of compliance

(i) Design phase

No requirements.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society the procedures and instructions for backup and restore provided by the suppliers for CBSs in the scope of applicability of this Part.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.6.2(d)(iii) as per the Ship cyber resilience test procedure.

3.6.3 Controlled shutdown, reset, roll-back and restart

(a) Requirement

CBS and networks in the scope of applicability of this Part shall be capable of controlled shutdown, reset to an initial state, roll-back to a safe state and restart from a power-off condition in such state, in order to allow fast and safe recovery from a possible impairment due to a cyber incident.

Suitable documentation on how to execute the above-mentioned operations shall be available to onboard personnel.

(b) Rationale

Controlled shutdown consists in turning a CBS or network off by software function allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe and known state. Controlled shutdown is opposed to hard shutdown, which occurs for example when the computer is forcibly shut down by interruption of power.

While in the case of some cyber incidents hard shutdowns may be considered as a safety precaution, controlled shutdown is preferable in case of integrated systems to keep them in a consistent and known state with predictable behaviour. When standard shutdown procedures are not done, data or program and operating system files corruption may occur. In case of OT systems, the result of corruption can be instability, incorrect functioning or failure to provide the intended service.

The reset operation would typically kick off a soft boot, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state. Depending on system considered, the reset operation might have different effects.

Rollback is an operation which returns the system to some previous state. Rollbacks are important for data and system integrity, because they mean that the system data and programs can be restored to a clean copy even after erroneous operations are performed. They are crucial for recovering from crashes and cyber incidents, restoring the system to a consistent state.

Restarting a system and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source appears to be an effective approach to recover from unexpected faults or cyber incidents. Restart operations should be however controlled in particular for integrated systems, where unexpected restart of a single component can result in inconsistent system state or unpredictable behaviour.

(c) Requirement details

CBS and networks in the scope of applicability of this Part shall be capable of:

- (i) controlled shutdown allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe, consistent and known state.
- (ii) resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state.
- (iii) rolling back to a previous configuration and/or state, to restore system integrity and consistency.
- (iv) restarting and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source. Restart time shall be compatible with the system's intended service and shall not bring other connected systems, or the integrated system it is part of, to an inconsistent or unsafe state.

Documentation shall be available to onboard personnel on how to execute the abovementioned operations in case of a system affected by a cyber incident.

(d) Demonstration of compliance

(i) Design phase

The systems integrator shall include the following information in the Cyber security design description: References to product manuals or procedures describing how to safely shut down, reset, restore and restart the CBSs in the scope of applicability of this Part.

(ii) Construction phase

No requirements.

(iii) Commissioning phase

The systems integrator shall submit Ship cyber resilience test procedure (ref. 4.3.2) and demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the CBSs in the scope of applicability of this Part. These manuals/procedures shall be provided to the shipowner.

The above tests may be omitted if performed during the certification of CBSs as per 4.3.2.

(iv) Operation phase

For general requirements to surveys in the operation phase, see 4.4.

(1) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to the Society the activities in 3.6.3(d)(iii) as per the Ship cyber resilience test procedure.

Chapter 4 Demonstration of Compliance

4.1 General

Evaluation of compliance with requirements in this Part shall be carried out by the Society by assessment of documentation and survey in the relevant phases as specified in the following .

4.1.1 Documentation to be submitted by suppliers to the Society is specified in Part III. The approved versions of this documentation shall also be provided by the suppliers to the systems integrator as specified in 6.2 of Part III.

4.1.2 Documents to be provided by the systems integrator are listed in 4.2 and 4.3.

4.1.3 Documents to be provided by the shipowner are listed in 4.4.

4.1.4 Upon delivery of the ship, the systems integrator shall provide below documentation to the shipowner:

- (a) Documentation of the CBSs provided by the suppliers (see 6.2 of Part III)
- (b) Documentation produced by the systems integrator (see 4.2 and 4.3)

4.2 During Design and Construction Phases

The supplier shall demonstrate compliance to the Society by following the certification process specified in Chapter 6 of Part III. The systems integrator shall demonstrate compliance by submitting documents as specified in the following to the Society for assessment. During the design and construction phases, modifications to the design shall be carried out in accordance with the management of change (MoC) requirements in UR E22.

4.2.1 Zones and conduit diagram

The content of this document is specified in 3.3.1(d)(i).

4.2.2 Cyber security design description (CSDD)

The content of this document is specified in the "Design phase" for each requirement in Chapter 3.

4.2.3 Vessel asset inventory

The content of this document is specified in 3.2.1.

4.2.4 Risk assessment for the exclusion of CBSs

The content of this document is specified in Chapter 5.

4.2.5 Description of compensating countermeasures

If any CBS in the scope of applicability of this Part has been approved with compensating countermeasures in lieu of a requirement in Part III, this document shall specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also 3.1.3 of Part III requiring that the supplier describes such compensating countermeasures in the system documentation.

4.3 Upon Ship Commissioning

4.3.1 Before final commissioning of the ship, the systems integrator shall:

- (a) Submit updated design documentation to the Society (as-built versions of the documents in 4.2).
- (b) Submit Ship cyber resilience test procedure to the Society describing how to demonstrate compliance with this Part by testing and/or analytic evaluation.
- (c) Carry out testing, witnessed by the Society, in accordance with the approved Ship cyber resilience test procedure.

4.3.2 Ship cyber resilience test procedure

- (a) The content of this document is specified for the Commissioning phase in each "Demonstration of compliance" in Chapter 3.
- (b) For each CBS, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS (see Part III). Testing of such security functions may be omitted if specified in the respective "Commissioning phase", on the condition that these security functions have been successfully tested during the certification of the CBS as per Part III. Nevertheless, all tests shall be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the CBS after the certification process.
- (c) The Ship cyber resilience test procedure shall also specify how to test any compensating countermeasures described in 4.2.2.
- (d) The Ship cyber resilience test procedure shall include means to update status and record findings during the testing, and specify the following information:
 - (i) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
 - (ii) Test equipment
 - (iii) Initial condition(s)
 - (iv) Test methodology, detailed test steps
 - (v) Expected results and acceptance criteria
- (e) Before submitting the Ship cyber resilience test procedure to the Society, the systems integrator shall verify that the information is updated and placed under change management; that it is aligned with the latest configurations of CBSs and networks connecting such systems together onboard the ship and to other CBSs not onboard (e.g., ashore); and that the tests documented are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of CBSs and networks onboard.
- (f) The systems integrator shall document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Ship cyber resilience test procedure.

- (g) The testing shall be carried out on board in accordance with the approved Ship cyber resilience test procedure after other commissioning activities for the CBSs are completed. The Society may request execution of additional tests.

4.4 During the Operational Life of the Ship

4.4.1 General

- (a) After the ship has been delivered to the shipowner, the shipowner shall manage technical and organisational security countermeasures by establishing and implementing processes as specified in this Part.
- (b) Modifications to the CBSs in scope of applicability of this Part shall be carried out in accordance with the management of change (MoC) requirements in IACS UR E22. This includes keeping documentation of the CBSs up to date.
- (c) The shipowner, with the support of suppliers, shall keep the Ship cyber resilience test procedure up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore). The shipowner shall update the Ship cyber resilience test procedure considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment.
- (d) The shipowner shall prepare and implement operational procedures, provide periodic training and carry out drills for the onboard personnel and other concerned personnel ashore to familiarize them with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.
- (e) The shipowner, with the support of supplier, shall keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of CBSs onboard the ship and the networks connecting such systems.
- (f) The shipowner shall retain onboard a copy of results of execution of tests and an updated Ship cyber resilience test procedure and make them available to the Classification Society.

4.4.2 First annual survey

- (a) In due time before the first annual survey of the ship, the shipowner shall submit to the Society a Ship cyber security and resilience program documenting management of cyber security and cyber resilience of the CBSs in the scope of applicability of this Part.
- (b) The Ship cyber security and resilience program shall include policies, procedures, plans and/or other information documenting the processes/activities specified in the "Demonstration of compliance" in Chapter 3.
- (c) After the Society has approved the Ship cyber security and resilience program, the shipowner shall in the first annual survey demonstrate compliance by presenting records or other documented evidence of implementation of the processes described in the approved Ship cyber security and resilience program.
- (d) Change of vessel management company will require a new verification of the Ship cyber security and resilience program.

4.4.3 Subsequent annual surveys

In the subsequent annual surveys of the ship, the shipowner shall upon request by the Society demonstrate implementation of the Ship cyber security and resilience program.

4.4.4 Special survey

Upon renewal of the ship's classification certificate, the shipowner shall carry out testing witnessed by the Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards shall be demonstrated at Special survey whereas other need only be carried out upon request by the Society based on modifications to the CBSs as specified in the "Operation phase" in Chapter 3.

Chapter 5 Risk Assessment for Exclusion of CBS from the Application of Requirements

5.1 Requirement

A risk assessment shall be carried out in case any of the CBSs falling under the scope of applicability of this Part is excluded from the application of relevant requirements. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded CBSs.

5.2 Rationale

Exclusion of a CBS falling under the scope of applicability of this Part from the application of relevant requirements needs to be duly justified and documented. Such exclusion can be accepted by the Classification Society only if evidence is given that the risk level associated to the operation of the CBS is under an acceptable threshold by means of specific risk assessment.

The risk assessment shall be based on available knowledge bases and experience on similar designs, if any, considering the CBS category, connectivity and the functional requirements and specifications of the ship and of the CBS. Cyber threat information from internal and external sources may be used to gain a better understanding of the likelihood and impact of cybersecurity events.

5.3 Requirement Details

5.3.1 Risk assessment shall be made and kept up to date by the System integrator during the design and building phase considering possible variations of the original design and newly discovered threats and/or vulnerabilities not known from the beginning.

5.3.2 During the operational life of the ship, the shipowner shall update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in CBS onboard in a process of continuous improvement. Should new risks be identified, the shipowner shall update existing, or implement new risk mitigation measures.

5.3.3 Should the changes in the cyber scenario be such as to elevate the risk level associated to the CBS under examination above the acceptable risk threshold, the shipowner shall inform the Classification Society and submit the updated risk assessment for evaluation.

5.3.4 The envisaged operational environments for the CBS under examination shall be analyzed in the risk assessment to discern the likelihood of cyber incidents and the impact they could have on the human safety, the safety of the vessel or the marine environment, taking into account the category of the CBS. The attack surface shall be analyzed, taking into account the connectivity of the CBS, possible interfaces for portable devices, logical access restrictions, etc.

5.3.5 Emerging risks related to the specific configuration of the CBS under examination shall be also identified. In the risk assessment, the following elements shall be considered:

- (a) Asset vulnerabilities;
- (b) Threats, both internal and external;

- (c) Potential impacts of cyber incidents affecting the asset on human safety, safety of the vessel and/or threat to the environment;
- (d) Possible effects related to integration of systems, or interfaces among systems, including systems not onboard (e.g. if remote access to onboard systems is provided).

5.4 Acceptance Criteria

5.4.1 Exclusion of a CBS falling under the scope of applicability of this Part from the application of relevant requirements can be accepted by the Classification Society only if assurance is given that the operation of the CBS has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a CBS which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by the Classification Society. The Classification Society may also require submittal of additional documents to consider the said exclusion.

5.4.2 The following criteria shall be met to exclude a system from the scope of applicability of this Part:

- (a) The CBS shall be isolated (i.e, have no IP-network connections to other systems or networks)
- (b) The CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled. It shall not be possible to connect unauthorised devices to the CBS
- (c) The CBS must be located in areas to which physical access is controlled
- (d) The CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Part (see 1.3)

5.4.3 The following additional criteria should be considered for the evaluation of risk level acceptability:

- (a) The CBS should not serve ship functions of category III ;
- (b) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the CBS have been duly considered in the risk assessment;
- (c) The attack surface for the CBS is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points;



GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS
PART III – CYBER RESILIENCE OF ON-BOARD SYSTEMS
AND EQUIPMENT

CR CLASSIFICATION SOCIETY

December 2025

REVISION HISTORY

(This version supersedes all previous ones.)

Revision No.	Editor	Date (yyyy-mm)
001	Rules Section	2025-12

GUIDELINES FOR CYBER SECURITY ONBOARD SHIPS PART III – CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT

CONTENTS

Chapter 1	General	1
1.1	Introduction.....	1
1.2	Limitations	1
1.3	Scope of Applicability.....	1
1.4	Definitions and Abbreviations	1
Chapter 2	Security Philosophy	5
2.1	Systems and Equipment.....	5
2.2	Cyber Resilience	5
2.3	Essential Systems Availability	5
2.4	Compensating Countermeasures	5
Chapter 3	Documentation.....	6
3.1	CBS Documentation	6
Chapter 4	System Requirements.....	9
4.1	General.....	9
4.2	Required Security Capabilities.....	9
4.3	Additional Security Capabilities	13
Chapter 5	Secure Development Lifecycle Requirements	15
5.1	General.....	15
Chapter 6	Demonstration of Compliance.....	17
6.1	Introduction.....	17
6.2	Plan Approval	18
6.3	Survey and Factory Acceptance Test	18

Chapter 1 General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient. This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

This Part does not cover environmental performance for the system hardware and the functionality of the software. In addition to this Part, following IACS URs shall be applied:

1.2.1 IACS UR E10 for environmental performance for the system hardware

1.2.2 IACS UR E22 for safety of equipment for the functionality of the software

1.3 Scope of Applicability

1.3.1 For the scope of applicability, the requirements specified in 1.3.1~1.3.3 of Part II shall apply.

1.3.2 Class notation

For ship complying with the requirements of this Part, the class notation **Cyber-SnE** will be assigned to the ship.

1.4 Definitions and Abbreviations

1.4.1 Attack surface

The set of all possible points where an unauthorized user can access a system, cause an effect on or extract data from. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

1.4.2 Authentication

Provision of assurance that a claimed characteristic of an identity is correct.

1.4.3 Compensating countermeasure

An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

1.4.4 Computer-based system (CBS)

A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. On-board CBS may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.

1.4.5 Computer network

A connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

1.4.6 Control

Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

1.4.7 Cyber incident

An event resulting from any offensive cyber manoeuvre, either intentional or unintentional, that targets or affects one or more CBS onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard CBS or transported in the networks connecting such systems. Cyber incidents do not include system failures.

1.4.8 Cyber resilience

The capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

1.4.9 Defence in depth

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

1.4.10 Essential systems

Computer-based system contributing to the provision of services essential for propulsion and steering, and safety of the ship. Essential services comprise "Primary Essential Services" and "Secondary Essential Services": Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering; Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

1.4.11 Firewall

A logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules.

1.4.12 Firmware

Software embedded in electronic devices that provide control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not accessible to user manipulation.

1.4.13 Hardening

Hardening is the practice of reducing a system's vulnerability by reducing its attack surface.

1.4.14 Information technology (IT)

Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

1.4.15 Integrated system

A system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes.

1.4.16 Network switch (Switch)

A device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

1.4.17 Offensive cyber manoeuvre

Actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems.

1.4.18 Operational technology (OT)

Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

1.4.19 OT system

Computer-based systems, which provide control, alarm, monitoring, safety or internal communication functions.

1.4.20 Patches

Software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications.

1.4.21 Protocols

A common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various field buses.

1.4.22 Recovery

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recovery function support s timely return to normal operations to reduce the impact from a cyber security event.

1.4.23 Supplier

A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.

1.4.24 System

Combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes.

1.4.25 System categories (I, II, III)

System categories based on their effects on system functionality, which are defined in IACS UR E22.

1.4.26 System integrator

The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The system integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role shall be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

1.4.27 Untrusted network

Any network outside the scope of applicability of this Part.

Chapter 2 Security Philosophy

2.1 Systems and Equipment

2.1.1 A System can consist of group of hardware and software enabling safe, secure and reliable operation of a process. Typical example could be Engine control system, DP system, etc.

2.1.2 Equipment may be one of the following:

- (a) Network devices (i.e. routers, managed switches)
- (b) Security devices (i.e. firewall, Intrusion Detection System)
- (c) Computers (i.e. workstation, servers)
- (d) Automation devices (i.e. Programmable Logic Controllers)
- (e) Virtual machine cloud-hosted

2.2 Cyber Resilience

The cyber resilience requirements in Chapter 4 will be applicable for all systems in scope of Part II as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

2.3 Essential Systems Availability

2.3.1 Security measures for Essential system shall not adversely affect the systems availability.

2.3.2 Implementation of security measures shall not cause loss of safety functions , loss of control functions, loss of monitoring functions or loss of other functions which could result in health, safety and environmental consequences.

2.3.3 The system shall be adequately designed to allow the ship to continue its mission critical operations in a manner that ensures the confidentiality, integrity, and availability of the data necessary for safety of the vessel, its systems, personnel and cargo.

2.4 Compensating Countermeasures

2.4.1 Compensating countermeasure may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

Compensating countermeasure(s) shall meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each requirement and the related items in the standards, and follow the principles specified in 3.1.3.

Chapter 3 Documentation

3.1 CBS Documentation

The following documents shall be submitted to Classification society for review and approval in accordance with the requirements in this Part. See also 6.2.

3.1.1 CBS asset inventory

- (a) The CBS asset inventory shall include the information below.
 - (i) List of hardware components (e.g., host devices, embedded devices, network devices)Name
 - (ii) Brand/manufacturer
 - (iii) Model/type
 - (iv) Short description of functionality/purpose
 - (v) Physical interfaces (e.g., network, serial)
 - (vi) Name/type of system software (e.g., operating system, firmware)
 - (vii) Version and patch level of system software
 - (viii) Supported communication protocols
- (b) List of software components (e.g., application software, utility software)
 - (i) The hardware component where it is installed
 - (ii) Brand/manufacturer
 - (iii) Model/type
 - (iv) Short description of functionality/purpose
 - (v) Version of software

3.1.2 Topology diagrams

- (a) The physical topology diagram shall illustrate the physical architecture of the system. It shall be possible to identify the hardware components in the CBS asset inventory. The diagram shall illustrate the following:
 - (i) All endpoints and network devices, including identification of redundant units
 - (ii) Communication cables (networks, serial links), including communication with I/O units
 - (iii) Communication cables to other networks or systems
- (b) The logical topology diagram shall illustrate the data flow between components in the system. The diagram shall illustrate the following:
 - (i) Communication endpoints (e.g. workstations, controllers, servers)
 - (ii) Network devices (switches, routers, firewalls)
 - (iii) Physical and virtual computers
 - (iv) Physical and virtual communication paths
 - (v) Communication protocols
- (c) One combined topology diagram may be acceptable if all requested information can be clearly illustrated.

3.1.3 Description of security capabilities

- (a) This document shall describe how the CBS with its hardware and software components meets the required security capabilities in 4.2.
- (b) Any network interfaces to other CBSs in the scope of applicability of Part II shall be described. The description shall include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (see 3.3.2(a) of Part III) shall be described in detail if delivered as part of the CBS.
- (c) Any network interfaces to other systems or networks outside the scope of applicability of Part II (untrusted networks) shall be described. The description shall specify compliance with the additional security capabilities in 4.3, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see 3.3.2(a) of Part II) shall be described in detail if delivered as part of the CBS.
- (d) A separate chapter shall be designated for each requirement. All hardware and software components in the system shall be addressed in the description, as relevant.
- (e) If any requirement is not fully met, this shall be specified in the description, and compensating countermeasures shall be proposed. The compensating countermeasures should:
 - (i) Protect against the same threats as the original requirement
 - (ii) Provide an equal level of protection as the original requirement
 - (iii) Not be a security control that is required by other requirements in this Part
 - (iv) Not introduce higher security risk
- (f) Any supporting documents (e.g. OEM information) necessary to verify compliance with the requirements shall be referenced in the description and submitted.

3.1.4 Test procedure of security capabilities

- (a) This document shall describe how to demonstrate by testing that the system complies with the requirements in 4.2 and 4.3, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure shall include a separate chapter for each applicable requirement and describe:
 - (i) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
 - (ii) Test equipment
 - (iii) Initial condition(s)
 - (iv) Test methodology, detailed test steps
 - (v) Expected results and acceptance criteria
- (b) The procedure shall also include means to update test results and record findings during the testing.

3.1.5 Security configuration guidelines

- (a) This document shall describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with Part II and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)
- (b) The document shall serve as basis for verification of item no. 29 of Table III 4-1.

3.1.6 Secure development lifecycle documents

This documentation shall be submitted to the Society upon request and shall describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in Chapter 5. Software updates and patching shall be described. The document shall prepare the Society for survey as per 6.4.1(d).

3.1.7 Plans for maintenance and verification of the CBS

This document shall be submitted to the Society upon request and shall include procedures for security-related maintenance and testing of the system. The document shall include instructions for how the user can verify correct operation of the system's security functions as required by item no.19 of Table III 4-1.

3.1.8 Information supporting the owner's incident response and recovery plan

This document shall be submitted to the Society upon request and shall include procedures or instructions allowing the user to accomplish the following:

- (a) Local independent control (see 3.5.2 of Part II)
- (b) Network isolation (see 3.5.3 of Part II)
- (c) Forensics by use of audit records (see item no.13 of Table III 4-1)
- (d) Deterministic output (see 3.5.4 of Part II and item no. 20 of Table III 4-1)
- (e) Backup (see item no. 26 of Table III 4-1)
- (f) Restore (see item no. 27 of Table III 4-1)
- (g) Controlled shutdown, reset, roll-back and restart (see 3.6.3 of Part II)

3.1.9 Management of change plan

This document shall be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by IACS UR E22.

3.1.10 Test reports

CBSs with Type approval certificate covering the security capabilities of this Part may be exempted from survey by the Society. However, test reports signed by the supplier shall be submitted to the Society, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the Society in survey (see 6.3).

Chapter 4 System Requirements

4.1 General

This Chapter specifies the required security capabilities for CBSs in the scope specified in 1.3.

The requirements in this Chapter are based on the selected requirements in IEC 62443-3-3. To determine the full content, rationale and relevant guidance for each requirement, the reader should consult the referenced standard.

4.2 Required Security Capabilities

The following security capabilities are required for all CBSs in the scope specified in 1.3.

Table III 4-1

Item No	Objective	Requirements
Protect against casual or coincidental access by unauthenticated entities		
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces. (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role. (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS shall provide the capability to: (1) Initialize authenticator content (2) Change all default authenticators upon control system installation (3) Change/refresh all authenticators (4) Protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. (IEC 62443-3-3/SR 1.6)

Item No	Objective	Requirements
6	Strength of password-based authentication	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. (IEC 62443-3-3/SR 1.7)
7	Authenticator feedback	The CBS shall obscure feedback during the authentication process. (IEC 62443-3-3/SR 1.10)
Protect against casual or coincidental misuse		
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege. (IEC 62443-3-3/SR 2.1)
9	Wireless use control	The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices. (IEC 62443-3-3/SR 2.2)
10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system shall include the capability to (1) Limit the use of portable and mobile devices only to those permitted by design (2) Restrict code and data transfer to/from portable and mobile devices Note: Port limits / blockers (and silicone) could be accepted for a specific system. (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)

Item No	Objective	Requirements
Protect the integrity of the CBS against casual or coincidental manipulation		
16	Timestamps	The CBS shall timestamp audit records. (IEC 62443-3-3/SR 2.11)
17	Communication integrity	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks. (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms. (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance. (IEC 62443-3-3/SR 3.3)
20	Deterministic output	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: (1) Unpowered state, (2) Last-known value, or (3) Fixed value (IEC 62443-3-3/SR 3.6)
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure		
21	Information confidentiality	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
22	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (IEC 62443-3-3/SR 4.3)
Monitor the operation of the CBS and respond to incidents		
23	Audit log accessibility	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools. (IEC 62443-3-3/SR 6.1)

Item No	Objective	Requirements
Ensure that the control system operates reliably under normal production conditions		
24	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload-based DoS events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed. (IEC 62443-3-3/SR 7.1)
25	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations. (IEC 62443-3-3/SR 7.3)
27	System recovery and reconstitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
28	Alternative power source	The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)
29	Network and security configuration settings	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)
30	Least functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the CBS: (1) Operating systems software components, processes and services (2) Network services, ports, protocols, routes and hosts accesses and any software. (IEC 62443-3-3/SR 7.7)

4.3 Additional Security Capabilities

The following additional security capabilities are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of Part II).

CBSs with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection in 3.3.1 and 3.3.2 of Part II.

Table III 4-2

Item No	Objective	Requirements
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
32	Software process and device identification and authentication	The CBS shall identify and authenticate software processes and devices. (IEC 62443-3-3/SR 1.2)
33	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
34	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
35	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
36	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
37	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (IEC 62443-3-3/SR 2.6)
38	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
39	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS. (IEC 62443-3-3/SR 3.5)

Item No	Objective	Requirements
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)

Chapter 5 Secure Development Lifecycle Requirements

5.1 General

5.1.1 A Secure Development Lifecycle (SDLC) broadly addressing security aspects in following stages shall be followed for the development of systems or equipment

- (a) Requirement analysis phase
- (b) Design phase
- (c) Implementation phase
- (d) Verification phase
- (e) Release phase
- (f) Maintenance Phase
- (g) End of life phase

5.1.2 A document, shall be produced that records how the security aspects have been addressed in above phases and shall at minimum integrate controlled processes as set out in below 5.1.2(a) to 5.1.2(g). The said document is required to be submitted to class for review and approval.

- (a) (IEC 62443-4-1/SM-8) The manufacturer shall have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.
- (b) (IEC 62443-4-1/SUM-2) A process shall be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to:
 - (i) The product version number(s) to which the security patch applies;
 - (ii) Instructions on how to apply approved patches manually and via an automated process;
 - (iii) Description of any impacts that applying the patch to the product can have, including reboot;
 - (iv) Instructions on how to verify that an approved patch has been applied; and
 - (v) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.
- (c) (IEC 62443-4-1/SUM-3) A process shall be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to:
Stating whether the product is compatible with the dependent component or operating system security update;
- (d) (IEC 62443-4-1/SUM-4) A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.

Note: The manufacturer shall have QA process to test the updates before releasing.

- (e) (IEC 62443-4-1/SG-1) A process shall exist to create product documentation that describes the security defence in depth strategy for the product to support installation, operation and maintenance that includes:
 - (i) Security capabilities implemented by the product and their role in the defence in depth strategy;
 - (ii) Threats addressed by the defence in depth strategy; and
 - (iii) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code.

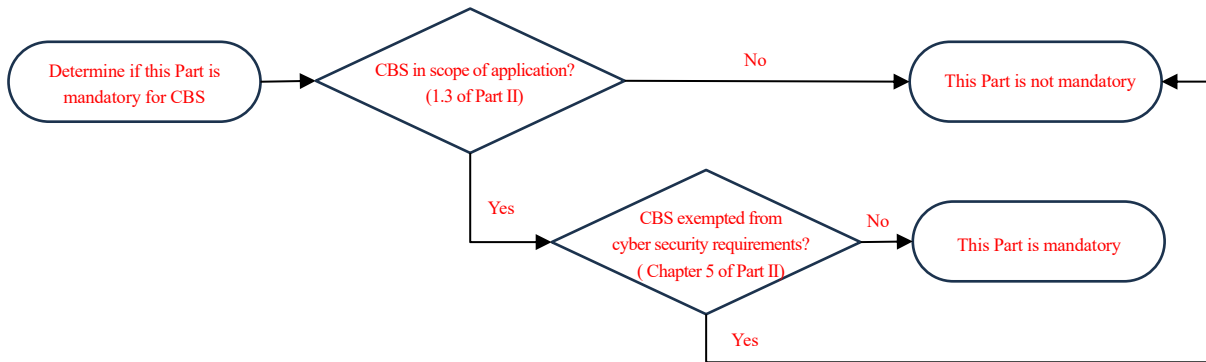
- (f) (IEC 62443-4-1/SG-2) A process shall be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used.

- (g) (IEC 62443-4-1/SG-3) A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines shall include, but are not limited to, instructions, rationale and recommendations for the following:
 - (i) Integration of the product, including third-party components, with its product security context
 - (ii) Integration of the product's application programming interfaces/protocols with user applications;
 - (iii) Applying and maintaining the product's defence in depth strategy
 - (iv) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
 - (1) Its contribution to the product's defence in depth strategy
 - (2) Descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
 - (3) Setting/changing/deleting its value;
 - (v) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product;
 - (vi) Instructions and recommendations for periodic security maintenance activities;
 - (vii) Instructions for reporting security incidents for the product to the supplier;
 - (viii) Description of the security best practices for maintenance and administration of the product.

Chapter 6 Demonstration of Compliance

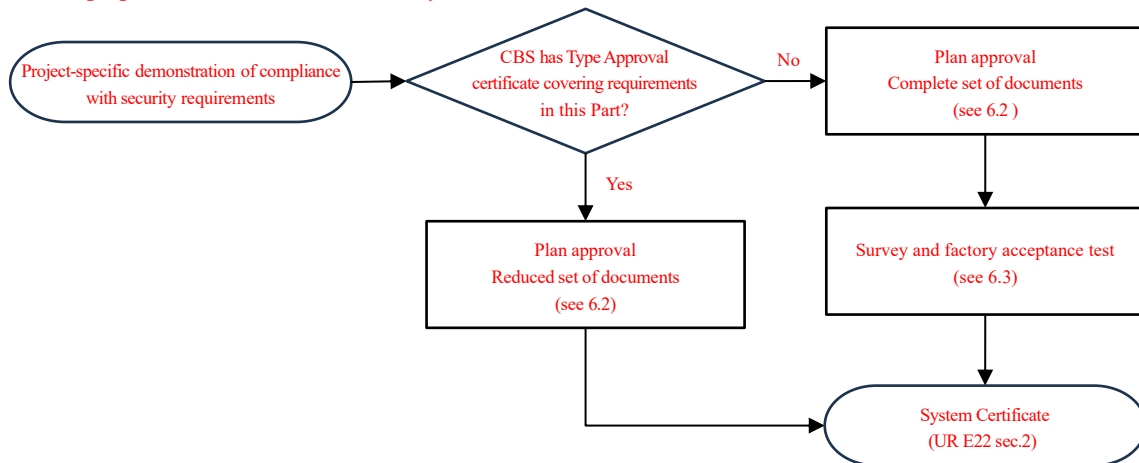
6.1 Introduction

6.1.1 Suppliers shall in cooperation with the System integrator determine if this Part is mandatory for the CBS, see Fig. III 6-1.



**Fig. III 6-1
 Determination of Application**

6.1.2 Compliance with security requirements shall be demonstrated as indicated in Fig. III 6-2. This classification process is ship-specific and shall result in a System certificate.



**Fig. III 6-2
 Compliance with Security Requirements**

6.1.3 Type approval is voluntary and applies for CBSs that are standard and routinely manufactured. See IACS UR E22 for definition of System certification and Type approval.

6.1.4 The process in Fig. III 6-1 and Fig. III 6-2 applies also if other equivalent standards are applied for navigation and radiocommunication equipment (see 1.3). In such case:

- (a) The process in Fig. III 6-1 illustrates if the equivalent standard is mandatory (in lieu of this Part)
- (b) The process in Fig. III 6-2 illustrates that the certification process is lessened if the CBS has been type approved in accordance with the equivalent standard.

6.2 Plan Approval

6.2.1 Plan approval is assessment of documents of a CBS intended for a specific vessel. The documents in Chapter 3 are required to be submitted by the supplier. The documents shall enable the Society to verify compliance with requirements in this Part.

6.2.2 If the CBS holds a valid Type approval certificate covering the requirements of this Part, subject to approval by the Society, the supplier may submit a reduced set of vessel-specific documents to the Society.

6.2.3 The approved version of the documents shall be included in the delivery of the CBS to the system integrator.

6.3 Survey and Factory Acceptance Test

6.3.1 Survey and factory acceptance testing (FAT) is a vessel-specific verification activity required for CBSs that do not hold a valid Type approval certificate covering the requirements of this Part.

6.3.2 The objective of the survey and FAT is to demonstrate by testing and/or analytic evaluation that the CBS complies with applicable requirements in this Part. The survey and FAT shall be carried out at the supplier's premises or at other works having the adequate apparatus for testing and inspection.

6.3.3 After completed plan approval and survey/FAT, the Society will issue a System certificate that shall accompany the CBS upon delivery to the system integrator.

6.3.4 The survey and FAT activities are specified as follows.

- (a) General survey items
 - (i) The supplier shall demonstrate that design, construction, and internal testing has been completed.
 - (ii) It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (3.1.1) and the topology diagrams (3.1.2).
- (b) Test of security capabilities
 - (i) The supplier shall test the required security capabilities on the system to be delivered. The tests shall be carried out in accordance with the approved test procedure in 3.1.4 and be witnessed/accepted by the class surveyor.
 - (ii) The tests shall provide the class surveyor with reasonable assurance that all requirements are met. This implies that testing of identical components is normally not required.
- (c) Correct configuration of security capabilities

- (i) The supplier shall test/demonstrate for the class surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in 3.1.5. This demonstration may be carried out in conjunction with testing of the security capabilities.
 - (ii) The security settings shall be documented in a report, e.g. a ship-specific instance of the configuration guidelines.
- (d) Secure development lifecycle
- The supplier shall, in accordance with documentation in 3.1.6, demonstrate compliance with requirements for secure development lifecycle in Chapter 5.
- (e) Controls for private keys (IEC 62443-4-1/SM-8)
- (i) This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity.
 - (ii) The supplier shall present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access.
 - (iii) The policies and procedures shall address roles, responsibilities and work processes. The technical controls shall include e.g. physical access restrictions and cryptographic hardware (e.g. Hardware security module) for storage of the private key.
- (f) Security update documentation (IEC 62443-4-1/SUM-2)
- The supplier shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in 5.1.2(b).
- (g) Dependent component security update documentation (IEC 62443-4-1/SUM-3)
- The supplier shall present management system documentation, as required by 5.1.2(c), substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information shall address how to manage risks related to not applying the updated acquired software.
- (h) Security update delivery (IEC 62443-4-1/SUM-4)
- The supplier shall present management system documentation, as required by 5.1.2(d), substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.
- (i) Product defence in depth (IEC 62443-4-1/SG-1)
- (i) The supplier shall present management system documentation, as required by 5.1.2(e), substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in the CBS during installation, maintenance and operation.
 - (ii) Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

(j) Defence in depth measures expected in the environment (IEC 62443-4-1/SG-2)

The supplier shall present management system documentation, as required by 5.1.2(f), substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

(k) Security hardening guidelines (IEC 62443-4-1/SG-3)

- (i) The supplier shall present management system documentation, as required by 5.1.2(g), substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.
- (ii) The guidelines shall specify how to reduce vulnerabilities in the system by removal/prohibiting/disabling of unnecessary software, accounts, services, etc.