To : All Surveyors and whom it may concern

No   : 2023-14-E
Date : 26 Sep 2023

Subject	9.183 Notice for Amendment to the KR Technical Rules - Guidance for Cyber Resilience
Application	(Refer to Effective date for each KR Technical Rules specified in Par.1 and the attachment)

1. Please be informed that the amendments have been made to reflect IACS Resolutions and Requests for Establishment/Revision of Classification Technical Rules. And you are kindly requested to apply the amendments on the relevant works according to effective date.

Amended KR Technical Rules	Effective Date	Reflected IACS Res.
Guidance for Cyber Resilience	1 January 2023(Date of contract for construction)	IACS UR E26, E27 (New Apr 2022)

2. Furthermore, please be informed that the establishment will be included in 2024 edition on KR Technical Rules which will be published in the first half of 2024.

Attachments: Amended KR Technical Rules (K/E) --- each 1 copy. (The End)

Guidance for Cyber Resilience

2023. 9.

- Main Amendments -

(1) Reflecting IACS UR E26, E27 <ships contracted for construction on or after 2024/01/01>

    ◉ UR E26 (New Apr 2022) : Cyber Resilience of Ships

    ◉ UR E27 (New Apr 2022) : Cyber Resilience of on-board systems and euipment

Effective Date：1 January 2024

(The contract date for ship construction)

2023

Guidance for Cyber Resilience

KR

2023

Guidance for
Cyber Resilience

KR

APPLICATION OF "GUIDANCE FOR CYBER RESILIENCE"

1. Unless expressly specified otherwise, the requirements in the Guidance apply to ships, systems and equipment for which contracts for construction are signed or for which the application for Classification Survey is submitted to the Society on or after 1 January 2024.

CONTENTS

CHAPTER 1 GENERAL

Section 1 General

101. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of com-mercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, hu-man 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 con-tinually 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.

102. Aims and purpose

1. The aim of this Guidance 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.

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

3. Minimum requirements for cyber resilience of on-board systems and equipment are given in **Ch 3** of the Guidance. Systems and equipment compliant with **Ch 3** of the Guidance will have the neces-sary security capabilities to meet **Ch 2** of the Guidance.

103. Scope of applicability

1. General application
   (1) This requirements in this Guidance apply to the ships intended to be registered and maintained as ships in according with **Pt 1** of the **Rules for the Classification of Steels sihps**.
   (2) The requirements in **Ch 3** apply to onboard systems and equipment that included in the scope of **Ch 2**.
   (3) In addition to this Guidance, **Pt 6, Ch 2** of **Rules for the Classification of Steel Ships** shall be met.
   (4) Items not specified in this Guidance are to be in accordance with each relevant requirement of **Rules for the Classification of Steel Ships.**

2. This guidance applies to:
   (1) Operational Technology (OT) systems onboard ships, i.e. those computer-based systems 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 computer based systems used for the operation of the following ship functions and systems, if present onboard, shall be considered:
   (A) Propulsion
   (B) Steering
   (C) Anchoring and mooring
   (D) Electrical power generation and distribution
   (E) Fire detection and extinguishing systems
   (F) Cargo handling system (limited to safety-related elements)
   (G) Bilge and ballast systems, loading/unloading control systems, loading computer
   (H) Boiler control system
   (I) Scrubber control system and other systems needed for compliance with class or international regulations to prevent pollution to the environment
   (J) Watertight integrity and flooding detection

(K) Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
(L) Any other OT system whose disruption or functional impairing may pose risks to ship oper-
ations (e.g. LNG monitoring and control system, relevant gas detection system etc.)
(2) In addition, the following systems shall be included in the scope of applicability of this Guidance:
(A) Navigational systems required by statutory regulations
(B) Internal and external communication systems required by class rules and statutory regulations
For navigation and radiocommunication systems, standard such as IEC 61162-460 or IEC 63154
can be used as alternatives to this Guidance, as long as the application of such standards pro-
vides equivalent or greater cyber resilience as obtained from the application of the requirements
contained in this Guidance. In any case, requirements under section 4 shall be complied with.
(3) Any Internet Protocol (IP)-based communication interface from computer based systems in scope
of this Guidance to other systems. Examples of such systems are, but not limited to, the fol-
lowing:
(A) passenger or visitor servicing and management systems,
(B) passenger-facing networks
(C) administrative networks
(D) crew welfare systems
(E) any other systems connected to OT systems, either permanently or temporarily (e.g. during
maintenance).
The cyber incidents considered in this Guidance are events resulting from any offensive ma-
noeuvre that targets OT systems onboard ships as defined in **105.**

104. Class notations

Ships complying with the Guidance will be assigned with an additional following notation

1. **Cyber Resilience**: ships having cyber resilience throughout the ships' lifecycle in accordance with the re-
lvant requirements in **Ch 2**.

105. Definitions

1. **Attack Surface:** The set of all possible points where an unauthorized user can access a system and
extract data. 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.

2. **Availability:** The property of being accessible and useable upon demand by an authorized entity.

3. **Authentication:** Provision of assurance that a claimed characteristic of an entity is correct.

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.

5. **Computer Based System:** A programmable electronic device, or interoperable set of programmable
electronic devices, organized to achieve one or more specified purposes such as collection, process-
ing, maintenance, use, sharing, dissemination, or disposition of information. computer based systems
onboard include IT and OT systems. A computer based system may be a combination of sub-
systems connected via network. Onboard computer based systems may be connected directly or via
public means of communications (e.g. Internet) to ashore computer based systems, other vessels'
computer based systems and/or other facilities.

6. **Computer Network:** A connection between two or more computers for the purpose of communicat-
ing data electronically by means of agreed communication protocols.

7. **Confidentiality:** The property that information is not disclosed to system entities (users, processes,
devices) unless they have been authorized to access the information.

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

9. **Cyber attack:** Any type of offensive cyber manoeuvre that targets IT and OT systems, computer
networks, and/or personal computer devices and attempts to compromise, destroy or access com-
pany and ship systems and data.

10. **Cyber incident:** An event resulting from any offensive manoeuvre, either intentional or unintentional, that targets or affects one or more computer based system 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 computer based system or transported in the networks connecting such systems. Cyber incidents do not include system failures.

11. **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.

12. **Defence in depth:** Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

13. **Demilitarized zone (DMZ):** A physical or logical perimeter network segment that contains and exposes an organization's external-facing services to an external network. Its purpose is to enforce the internal network's security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

14. **Essential System:** 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.

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

16. **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.

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

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

19. **Initial Authenticator Content:** Factory default authentication credentials (e.g.: initial passwords, tokens, etc.) to allow for initial installation and configuration of system.

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

21. **Integrity:** The property whereby an entity has not been modified in an unauthorized manner.

22. **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.

23. **Logical network segment:** The same as "Network segment", but two or more logical network segments share the same physical components.

    Note on TCP/IP: Logical networks are hosted on the same physical network but segmented and managed at the data link or network layers (OSI Layer 2 and 3).

24. **Network segment:** A collection of nodes that share the same network address plan. A network segment is 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).

25. **Offensive cyber manoeuvre:** Actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems.

26. 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.

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

28. Physical network segment: The same as "Network segment". The physical components are not shared by other network segments.

> Note on TCP/IP: Segmentation breaks networks down into multiple physical segments or subnets. The incoming and outgoing packets are controlled. The connections and data exchanges are allowed or blocked at both network layer (OSI Layer 3) and application level (OSI Layer 7). Both traffic management and packet filtering can be managed by a single software or hardware equipment.

29. 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.

30. 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.

31. Security zone: A collection of connected computer based systems in the scope of applicability of this Guidnace that require the same access control policy. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

32. Ship Designer/Shipyard: The person or organization:

(1) Implementing the process of evolving the ship specifications given by the Shipowner into a complete ship project, including management of concept, contract and detail design, and/or

(2) In charge of ship construction and responsible for fulfilling during ship construction the requirements of applicable rules and regulations and implementing the specifications of ship design, and/or

(3) Responsible for the integration of systems and products provided by Suppliers into an integrated system.

33. 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 Owner could be the Shipyard or System Integrator (Builder or Shipyard) during initial construction. After vessel delivery, the owner may delegate some responsibilities to the vessel operating company.

34. 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.

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

36. System Categories (I, II, III): System categories based on their effects on system functionality, which are defined in **Pt 6, Ch 2, sec.4 of the Rules**,

37. 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. This role shall be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

38. Untrusted network: Any network outside the scope of applicability of this Guidance.

39. Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data transmitted between networks or devices utilizing tunnelling, security controls and endpoint address translation giving the impression of a dedicated line.

106. abbreviation

1. IT: Information Technology

2. Switch: Network Switch

3. OT: Operational Technology

4. VPN: Virtual Private Network

107. Reference

Refer to the following additional IACS documents and international standards for computer-based systems and cyber resilience.

1. IACS UR E22: Computer-based systems

2. IACS UR E26: Cyber resilience of ships

3. IACS UR E27: Cyber resilience of on-board systems and equipment

4. IACS Rec.166: Cyber resilience

5. IEC 62443-3-3 (2013): Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

6. IEC 62443-4-1 (2018): Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements ⚓

CHAPTER 2   REQUIREMENTS FOR CYBER RESILIENCE OF SHIPS

Section 1   Goals and organization of requirements

101. Primary goal

1. The primary goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

2. 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 **102.** below.

102. Sub-goals per functional element

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

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

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

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

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.

103. Organization of requirements

1. 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.

2. For each requirement, a rationale is given.

3. 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.

4. Criteria for performance evaluation and testing are also given.

Section 2 Requirements

201. General

1. This section contains the requirements to be satisfied in order to achieve the primary goal defined in **101**, organized according to the five functional elements identified in **102**.

2. The requirements shall be fulfilled under the responsibility of stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified:
   (1) Shipowner/Company
   (2) Ship Designer/Shipyard
   (3) System Integrator
   (4) Supplier
   (5) Classification Society

202. Identify

The requirements for the 'Identify' functional element are aimed at identifying: on one side, the computer based systems 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.

1. Inventory of computer based systems and networks onboard
   (1) Requirement:
      An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the computer based systems in the scope of applicability of this chapter and of the networks connecting such systems to each other and to other computer based systems onboard or ashore shall be provided and kept up to date during the entire life of the ship.
   (2) Rationale:
      The inventory of computer based systems 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 computer based system becomes a potential point of vulnerability. Cybercriminals can exploit unaccounted and out-of-date hardware and software to hack systems. Moreover, managing computer based system assets enables Companies understand the criticality of each system to ship safety objectives.
   (3) Requirement details
      (A) The inventory of computer based systems onboard shall include at least the computer based systems indicated in **Ch 1, 103. 2**, if present onboard.
      (B) The inventory shall be 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.
      (C) 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.
      (D) Hardware
         For hardware, theinventory shall contain at least the following information:
         (a) For each computer based system, a short description of its purpose with brief functional description and technical features (brand, manufacturer, model, main technical data);
         (b) A block diagram identifying the logical and physical connections among various computer based systems onboard and between computer based systems and external devices or networks, the topology of networks connecting computer based systems and the intended function of each node;
         (c) For network devices such as switches, routers, of the connected subnetworks, IP ranges, MAC addresses of nodes connected (or addresses/identifiers specific to the protocols used in the network)
         (d) The main features of each network (e.g. protocols used) and communication data flows (e.g. data flow diagram) in all intended operation modes;
         (e) A map describing the physical layout of each digital network connecting the computer based systems onboard, including the physical location of the computer based systems onboard and the physical location of network access points.

Based on the information above, a system category and security zone may also be associated to the computer based systems and recorded in the inventory.
(E) Software
For software, the nventory shall contain at least the following information, for each software application program, operating system, firmware etc.
(a) The computer based systems where it is installed, a short description of its purpose, technical features (brand, manufacturer, model, main technical data) and specific function;
(b) Version information, license information with initial installation and expiration dates and a log of updates;
(c). Maintenance policy (e.g. on-site vs. remote, periodic vs. occasional, etc.) and responsible persons;
(d) Access control policy (including e.g. read, write and execution rights) with roles and responsibilities.

203. 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.

1. Security Zones

(1) Requirement
(A) All computer based systems in the scope of applicability of **Ch 2** shall be grouped into security zones with well-defined security control policy 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.)
(B) Only explicitly allowed traffic shall traverse a security zone boundary.
(2) Rationale
(A) 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.
(B) 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 computer based systems into security zones allows grouping the computer based systems in accordance with their risk profile.
(3) Requirement details
(A) A security zone may contain multiple computer based systems and networks, all of which shall comply with the security requirements given in this Guidance.
(B) The network(s) of a security zone shall be logically or physically segmented from other zones or networks. See also **4.** (3).
(C) computer based systems providing required safety systems shall be grouped into separate security zones and shall be physically segmented from other security zones.
(D) Navigational and communication systems shall not be in same security zone as machinery or cargo systems.
(E) Wireless devices shall be in dedicated security zones. See also **5**.
(F) Other OT systems, or computer based systems outside the scope of applicability of **Ch 2** shall be physically segmented from security zones required by **Ch 2**. Alternatively, it is accepted that other OT systems are part of a security zone if these OT-systems meet the same requirements as demanded by the zone.
(G) It shall be possible to manually isolate a security zone without affecting the primary functionality of the computer based systems in the zone.
(H) In the definition of security control policies, the functions allowed to access or operate on the network shall be associated to technical procedures and roles.

2. Network protection safeguards

(1) Requirement
(A) Networks connecting computer based systems in the scope of applicability of **Ch 2** shall be protected by firewalls or equivalent means as specified in **1**. The networks shall also be pro-

tected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources.
- (B) The computer based systems in scope of **Ch 2** 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.

(2) Rationale
- (A) Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of computer networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities.
- (B) 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.
- (C) 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.

(3) Requirement details
The design of network shall include means for limiting data flow rate 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.

3. Antivirus, antimalware, antispam and other protections from malicious code

(1) Requirement
Computer based systems in the scope of applicability of **Ch 2** shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.

(2) Rationale
- (A) 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.
- (B) Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off all the malicious intruding viruses performing a prophylactic function. It detects any potential virus and then works to remove it, mostly before the virus gets to harm the system.
- (C) Common means for malicious code to enter computer based systems 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.

(3) Requirement details
- (A) Malware protection shall be implemented on computer based systems in the scope of applicability of this UR. On computer based systems having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs the ability of computer based system to provide the functionality and level of service required (e.g. for Cat.II and Cat.III computer based systems performing real-time tasks).
- (B) On computer based systems 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.

4. Access control

(1) Requirement

Computer based systems and networks in the scope of applicability of **Ch 2** 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 computer based system for their level of access according to the least privilege principle.

(2) Rationale

(A) 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. shall then be implemented to ensure safety of the ship and its cargo.

(B) 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. The requirements in this article may be considered as the technical foundation for instructions and procedures deriving from the application of ISPS and ISM Code.

(3) Requirement details

Access to computer based systems and networks in the scope of applicability of **Ch 2** and all information stored on such systems shall only be allowed to authorized personnel, authorized processes and devices, based on their need to access the information as a part of their responsibilities or their intended functionality.

(A) Physical access control

Computer based systems of Cat.II and Cat.III shall 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 computer based systems for installation, integration, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.

(B) Physical access control for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and owner representatives shall be restricted regarding access to computer based systems onboard whilst on board, e.g. by allowing access under supervision.

(C) Physical access control of network access points

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

 (b) 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).

(D) 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 **7**.

(E) Management of credentials

 (a) Computer based systems 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.

 (b) Onboard computer based systems shall be provided with appropriate access control that fits to the policy of their Security Zone but does not adversely affect their primary purpose. computer based systems which require strong access control may need to be secured using a strong encryption key or multi-factor authentication.

 (c) Administrator privileges allowing full access to system configuration settings and all data shall only be given to appropriately trained personnel, who as part of their role in the company or onboard, need to log onto systems using these privileges. Administrator privileges shall be removed when the person concerned is no longer onboard. In any case, use of administrator privileges shall always be limited to functions requiring such access.

(F) Least privilege policy

 (a) Any user, program, or process allowed to access computer based system and networks in the scope of applicability of **Ch 2** shall have only the bare minimum privileges necessary to perform its function. Processes having access to systems and networks onboard

shall operate at privilege levels no higher than necessary to accomplish their intended task.

(b) The default configuration for all new account or process 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 and process accounts.

5. Wireless communication

(1) Requirement

(A) Wireless communication networks in the scope of **Ch 2** shall be designed, implemented and maintained to ensure that:

(a) Cyber incidents will not propagate to other control systems

(b) Only authorised human users will gain access to the wireless network

(c) Only authorised processes and devices will be allowed to communicate on the wireless network

(d) Information in transit on the wireless network cannot be manipulated or disclosed

(2) Rationale

(A) 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.

(B) 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.

(C) 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).

(3) Requirement details

(A) 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.

(B) Devices on the wireless network shall only communicate on the wireless network (i.e. they shall not be "dual-homed")

(C) Wireless networks shall be designed as separate segments in accordance with **1.** and protected as per **2.**

(D) Wireless access points and other devices in the network shall be installed and configured such that access to the network can be controlled.

(E) 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.

6. Remote access control and communication with untrusted networks

(1) Requirement

Computer based systems in scope of **Ch 2** shall be protected against unauthorized access and other cyber threats from untrusted networks.

(2) Rationale

Onboard computer based systems 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 computer based systems makes them vulnerable to cyber incidents. Attackers may attempt to access onboard computer based systems through connectivity with the internet and may be able to make changes that affect a computer based system"s operation or even achieve full control of the computer based systems, or attempt to download information from the ship's computer based system. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects a lot 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.

(3) Requirement details

(A) 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.

(B) For computer based systems in the scope of application of **Ch 2**, no IP address shall be ex-

posed to untrusted networks. It shall not be possible to route packets directly to security zones from untrusted networks.

(C) 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.

(D) Design

   (a) Computer based systems in the scope of applicability of **Ch 2** shall:

      (i) 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.

      (ii) 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.

      (iii) 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.

(E) Additional requirements for remote maintenance.

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

      (i) Documentation shall be provided to show how they connect and integrate with the shore side.

      (ii) Patches and 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.

      (iii) A support plan shall be developed and made available to all stakeholders involved.

      (iv) 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 computer based system and systems involved.

      (v) Multi-factor authentication is required for any access by human users to computer based system's in scope from an untrusted network .

      (vi) When an access attempt is failed, next attempt is not to be started for a predetermined length of time. When the number of failed access attempts reached to a predetermined value, the authentication function shall be blocked.

      (vii) 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.

7. Use of Mobile and Portable Devices

(1) Requirement

  (A) The connection of mobile and portable devices to computer based systems in the scope of applicability of Ch 2 and of the networks connecting such systems shall be physically or logically blocked except when connecting for operation of the ship or maintenance.

  (B) Wireless connected mobile and portable devices shall be compliant with requirements of **5**.

(2) Rationale

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

(3) Requirement details

  (A) Mobile and portable devices for ship's operational use shall be recorded on inventory list. When mobile and portable devices are used for maintenance, it is necessary to describe the maintenance information in the inventory list. Information about connection ports for mobile and portable devices equipped in computer based systems shall be included in the inventory list, including the connection ports used for maintenance.

  (B) Blockers for removable media shall be used on physically accessible computers and network ports other than independent computers mentioned in **4.** (3) (C).

  (C) For connection ports for mobile and portable devices used for onboard operation by the ship's crew or for maintenance by the supplier, measures shall be taken to prevent connection other than the predetermined equipment. Information about the connection ports shall

be included in inventory list.
(D) Ports to which physical or logical blocks have been applied shall be clearly indicated.

204. 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 computer based systems and networks onboard and identify cyber incidents.

1. **Network operation monitoring**
   (1) Requirement
      Networks in scope of **Ch 2** shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.
   (2) 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 ill-prepared 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.
   (3) Requirement details
      (A) Measures to monitor networks in the scope of applicability of **Ch 2** shall have the following capabilities:
         (a) Monitoring and protection against excessive traffic
         (b) Monitoring of network connections
         (c) Monitoring and recording of device management activities
         (d) Monitoring or protection against connection of unauthorized devices
      (B) Intrusion detection systems (IDS) may be implemented, subject to the following:
         (a) The IDS shall be qualified by the supplier of the respective computer based system
         (b) The IDS shall be passive and not activate protection functions that may affect the performance of the computer based systems
         (c) Relevant personnel should be trained and qualified for using the IDS

2. **Diagnostic functions of computer based system and networks**
   (1) Requirement
      Computer based systems and networks in the scope of applicability of **Ch 2** shall be capable to check performance and functionality of security functions required by **Ch 2**. Diagnostic functions shall provide adequate information on computer based systems integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.
   (2) Rationale
      (A) 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.).
      (B) It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the computer based system.
   (3) Requirement details
      (A) Computer based systems and networks' diagnostics functionality shall be available to verify the intended operation of all security functions during test and maintenance phases of the ship.
      (B) Diagnostic functions continuously monitoring excessive network traffic as well as status of network connections and devices during normal operation of the computer based system and related networks shall be implemented. Diagnostic functions shall alert the responsible crew if anomalies are detected.

205. 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 computer based systems and networks onboard.

1. Incident response plan

(1) Requirement

An incident response plan shall be developed 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 computer based systems in the scope of applicability of **Ch 2**.

(2) Rationale

(A) 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.

(B) 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 shall be integrated with the ship in the event of a cyber incident.

(3) Requirement details

(A) 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.

(B) 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.

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

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

2. Local, independent and/or manual operation

(1) Requirement

Any computer based system 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.

(2) 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 shall also be considered, this principle of independent local control is no less important.

(3) Requirement details

(A) The computer based system for local control and monitoring shall be self-contained and not depend on communication with other computer based system for its intended operation.

(B) If communication to the remote control system or other computer based systems's is arranged by networks, segmentation and protection safeguards as described in **1.** and **2.** shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone.

(C) The computer based system for local control and monitoring shall otherwise comply with requirements in **Ch 2**.

3. Network isolation

(1) Requirement

It shall be possible to manually or automatically terminate network-based communication to or

from a network segment.
(2) 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.
(3) Requirement details
(A) Where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate physical network segments 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.
(B) 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.

4. Fallback to a minimal risk condition

(1) Requirement
In the event of a cyber incident impairing the ability of a computer based system or network in the scope of applicability of **Ch 2** 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.
(2) Rationale
(A) The ability of a computer based system 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.
(B) 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.
(3) Requirement details
(A) As soon as a cyber incident affecting the computer based system 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:
(a) bringing the system to a complete stop;
(b) disengaging the system;
(c) transferring control to another system or human operator;
(d) other compensating actions.
(B) Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition.
(C) 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 Shipyard / Ship Designer / System Integrator.

206. Recover

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

1. Recovery plan

(1) Requirement
A recovery plan shall be made to support restoring computer based systems under the scope of applicability of **Ch 2** 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.
(2) Rationale
(A) Incident response procedures are an essential part of system recovery. Responsible personnel shall consider carefully and be aware of the implications of recovery actions (such as wiping of drives) and execute them carefully.

(B) 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.

(C) Where appropriate, professional cyber incident response support shall be obtained to assist in preservation of evidence whilst restoring operational capability.

(3) Requirement details

(A) 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.

(B) 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.

(C) When developing recovery plans, the various systems and subsystems involved shall be specified. The following recovery objectives shall also be specified:

(a) 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.

(b) 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.

(D) 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;

(a) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.

(b) Processes and procedures for the backup and secure storage of information.

(c) Complete and up-to-date logical network diagram.

(d) The list of personnel responsible for restoring the failed system.

(e) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.

(f) Current configuration information for all components.

(E) The operation and navigation of the ship shall be prioritized in the plan in order to help ensure the safety of onboard personnel.

(F) 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.

2. Backup and restore capability

(1) Requirement

Computer based systems and networks in the scope of applicability of **Ch 2** shall have the capability to support back-up and restore in a timely, complete and safe manner. Backups shall be regularly maintained and tested.

(2) Rationale

(A) In general, the purpose of a backup and restore strategy shall protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following:

(a) Planning and testing responses to different kinds of failures;

(b) Configuring the database environment for backup and recovery;

(c) Setting up a backup schedule;

(d) Monitoring the backup and recovery environment;

(e) Creating a database copy for long-term storage;

(f) Moving data from one database or one host to another, etc.

(3) Requirement details

(A) Restore capability

(a) Computer based systems in the scope of applicability of **Ch 2** shall have backup and restore capabilities to enable the ship to quickly and safely regain navigational and operational state after a cyber incident.

(b) Data shall be restorable from a secure copy or image.

(c) Information and backup facilities shall be sufficient to recover from a cyber incident.

(B) Backup

(a) Computer based systems and networks in the scope of applicability of **Ch 2** 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.
(b) Backup plans shall be developed, including scope, mode and frequency, storage medium and retention period.

3. Controlled shutdown, reset, roll-back and restart

(1) Requirement
  (A) Computer based systems and networks in the scope of applicability of **Ch 2** 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.
  (B) Suitable documentation on how to execute the above-mentioned operations shall be available to onboard personnel.

(2) Rationale
  (A) Controlled shutdown consists in turning a computer based system 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.
  (B) 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.
  (C) 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.
  (D) 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 ad cyber incidents, restoring the system to a consistent state.
  (E) 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 shall be however controlled in particular for integrated systems, where unexpected restart of a single component can result in inconsistent system state or unpredictable behaviour.

(3) Requirement details
  (A) Computer based system and networks in the scope of applicability of **Ch 2** shall be capable of:
    (a) 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.
    (b) resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state.
    (c) rolling back to a previous configuration and/or state, to restore system integrity and consistency.
    (d) 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.
  (B) Documentation shall be available to onboard personnel on how to execute the above-mentioned operations in case of a system affected by a cyber incident.

Section 3 Plan for performance evaluation and testing

301. General

1. Performance evaluation and testing are aimed to verify the effective implementation of measures adopted for the fulfilment of requirements in **Ch 2**.

2. Performance evaluation and testing are mainly based on the design, development, maintenance and implementation of a Test Plan, which is the essential instrument intended to support and ground testing and verification activities. It evolves during different phases of the ship's life and involves different stakeholders.

3. The Test Plan shall be used as an instrument and a reference for the verification of the actual and effective implementation of measures adopted for the fulfilment of requirements in **Ch 2**. Additional or alternative tests may also be executed. Simulated cyber incidents can be intentionally induced for testing purposes.

4. This section indicates how the Test Plan shall be designed, implemented and maintained in the different phases of the ship's life in order to include all necessary information. Responsibilities related to these actions are also indicated.

5. This section does not contain requirements on how to conduct surveys. Survey requirements will be developed separately.

6. The following information shall be produced during the different phases of the ship's life for the design, development, maintenance and implementation of a Test Plan:

302. During design and construction phases

1. The Supplier shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan), for what pertains the systems or equipment supplied to the Shipyard or System Integrator for integration in the computer based system in the scope of applicability of **Ch 2** and networks connecting such systems to each other and to other computer based system onboard or ashore.

2. The Supplier shall maintain a test report where results of execution of the tests described in the Test Plan, following the relevant testing procedures, are recorded, to be provided to the Shipyard, where test results are recorded.

3. The Shipyard or System Integrator shall incorporate the documentation provided by the Supplier into an overall Test Plan for the computer based systems in the scope of applicability of **Ch 2** and networks connecting such systems to each other and to other computer based systems onboard or ashore.

4. The Shipyard or System Integrator shall design and document testing procedures suitable to verify the performance of measures adopted to fulfil relevant requirements (Test Plan), for what pertains the whole integrated computer based systems in the scope of applicability of **Ch 2** and networks connecting such systems to each other and to other computer based systems onboard or ashore. Testing procedures shall include functional tests, failure tests and a description of alarms and other monitoring means used to signal normal conditions, warnings and alerts.

5. The Shipyard or System Integrator shall maintain a test report where results of execution of tests described in the Test Plan, following the relevant testing procedure, are recorded, to be provided to the incoming Shipowner and to the Class Society upon ship commissioning, where test results are recorded. The Classification Society shall witness the execution of tests and may request execution of additional tests.

6. Testing procedures shall be described in the Test Plans in such a way as to make it possible for a third party, upon commissioning of the ship and during its service, to reproduce onboard the intended test conditions, execute the tests and verify test results, and make it possible a comparison between the results obtained and those obtained by the Supplier and/or the Shipyard/System Integrator.

7. The Supplier and the Shipyard shall keep Test Plans up to date and aligned with the actual implementation and installation of computer based systems onboard.

303. Upon ship commissioning

1. The Shipyard and the incoming Shipowner shall together verify that the information contained in the final version of the Test Plan is updated and placed under change management; that it is aligned with the latest configurations of computer based systems and networks connecting such systems together onboard the ship and to other computer based systems not onboard (e.g., ashore); and that the tests documented in the Test Plan 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 computer based systems and networks onboard.

2. The Shipyard 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 Test Plan.

3. The final Test Plans updated according to the actual computer based systems configuration and implementation onboard shall be made available to the Classification Society. The Classification Society may request execution of additional tests.

304. During the operational life of the ship

1. The Shipowner, with the support of Systems Integrator and Suppliers, shall keep the Test Plan up to date and aligned with the computer based systems onboard the ship and the networks connecting such systems to each other and to other computer based systems not onboard (e.g. ashore). The Shipowner shall update the Test Plan considering the changes occurred on computer based systems and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment.

2. 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 computer based systems onboard the ship and the networks connecting such systems to each other and to other computer based systems not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.

3. The Shipowner, with the support of System Integrator and Supplier, shall keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of computer based systems onboard the ship and the networks connecting such systems.

4. The Shipowner shall retain onboard a copy of results of execution of tests and an updated Test Plan and make them available to the Classification Society.

Section 4   Risk assessment for exclusion of computer based system from the application of requirements

401. Requirement

A risk assessment shall be carried out in case any of the computer based systems falling under the scope of applicability of **Ch 2** is excluded from the application of relevant requirements. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded computer based systems. A concise list of excluded applications of relevant requirements is to be generated and maintained with the computer based system documents onboard the ship (e.g. the execution of test plans and any relevant updated test plans).

402. Rationale

1. Exclusion of a computer based system falling under the scope of applicability of **Ch 2** 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 computer based system is under an acceptable threshold by means of specific risk assessment.

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

403. Requirement details

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

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 computer based system onboard in a process of continuous improvement. Should new risks be identified, the Shipowner shall update existing, or implement new risk mitigation measures.

3. Should the changes in the cyber scenario be such as to elevate the risk level associated to the computer based system under examination above the acceptable risk threshold, the Shipowner shall inform the Classification Society and submit the updated risk assessment for evaluation.

4. A concise list of excluded applications of relevant requirements is to be generated and maintained with the computer based system documents onboard the ship (e.g. the execution of test plans and any relevant updated test plans). The Class Society may accept or reject the exclusion of the computer based system from the application of the requirements in **Ch 2**.

5. The envisaged operational environments for the computer based system 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 computer based system. The attack surface shall be analyzed, taking into account the connectivity grade of the computer based system, possible interfaces for portable devices, logical access restrictions, etc.

6. Emerging risks related to the specific configuration of the computer based system under examination shall be also identified. In the risk assessment, the following elements shall be considered:
   (1) Asset vulnerabilities;
   (2) Threats, both internal and external;
   (3) Potential impacts of cyber incidents affecting the asset on human safety, safety of the vessel and/or threat to the environment;
   (4) 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).

404. Acceptance criteria

1. Exclusion of a computer based system falling under the scope of applicability of **Ch 2** from the application of relevant requirements can be accepted by the Classification Society only if evidence is given that the operation of the computer based system has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a computer based system which does not fully meet the criteria as per **2.** 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 to submit additional documents to consider the said exclusion.

2. The following criteria shall be considered for the evaluation of risk level acceptability:
   (1) Foreseeable vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the computer based system have been duly considered in the risk assessment;
   (2) The attack surface for the computer based system is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points;
   (3) The computer based system, considered in its function and role in the integrated system it is part of, cannot be affected by cyber incidents vectored by other computer based system or network devices, nor it can propagate the effect of a cyber incident to other computer based systems or network devices;
   (4) The computer based system must not serve essential services or multiple ship services;
   (5) The computer based system must be located in areas using controlled access;
   (6) The connections of computer based system to other computer based systems have been duly investigated, understood and documented. In particular, the computer based system shall not be connected to other computer based systems or devices by IP-based networks;
   (7) The computer based system shall not have available physical interfaces that can be used by uncontrolled/unsecure removable devices;
   (8) The software installed on the computer based system has been duly identified and evidence is given of the purpose, name, version, provider and maintainer of each software application, operating system and firmware (as applicable);
   (9) The computer based system is subject to a maintenance policy and such policy does not imply any permanent or temporary connection to untrusted networks, or use of uncontrolled/unsecure removable devices;
   (10) The computer based system provides means for checking at any time its functional integrity and the quality of service provided, including checks on hardware and software integrity;
   (11) The computer based system provides suitable interfaces allowing a human operator to take local manual control, and such interfaces do not widen its attack surface (see also point (2)).
   (12) The Incident Response Plan and Recovery Plan contain indications on how to treat the computer based system in case of cyber incidents occurring on the ship. ⚓

CHAPTER 3   REQUIREMENTS FOR CYBER RESILIENCE OF ONBOARD SYSTEMS AND EQUIPMENT

Section 1   General

101. Introduction

1. 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.

2. This document specifies unified requirements for cyber resilience of on-board systems and equipment

102. Limitations

1. **Ch 3** does not cover environmental performance for the system hardware and the functionality of the software. In addition to this chapter, following Rule and guidance shall be applied:
   (1) "Automatic and Remote Control SYstems" **Ch 3, Sec 23** of the **Guidance for Approval of Manufacturing Process and Type Approval, etc.**
   (2) "Computer based systems" **Pt 6**, **Ch 4**, **Sec 4** of **Rules for the Classification of Steel ships**

103. Scope

1. The requirements specified in **Ch 3** are applicable to computer based systems as defined in **Ch 2**.

2. Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in **Ch 3**. See **Ch 1, 103**.

Section 2   Security Philosophy

201. Systems and Equipment

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. An equipment may be one of the following:
   (1) Network devices (i.e. routers, managed switches)
   (2) Security devices (i.e. firewall, Intrusion Detection System)
   (3) Computers (i.e. workstation, servers)
   (4) Automation devices (i.e. Programmable Logic Controllers)
   (5) Virtual machine cloud-hosted

202. System Requirements

The cyber resilience requirements in **Sec 4** will be applicable for all systems in scope of **Ch 2** as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

203. Compensating Countermeasures

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

2. Compensating countermeasures should follow these principles:
   (1) Compensating countermeasure(s) should meet the intent and rigor of the original stated requirement. They should also be "above and beyond" other requirements (not simply in compliance with other requirements).
   (2) For type approval of a system, the compensating countermeasure(s) should be implemented in the computer based system, i.e., not rely on barriers related to installation on board or operational procedures.

204. Essential Systems Availability

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

2. Implementation of security measures shall not cause loss of protection, loss of control, loss of view or loss of other essential functions which could result in health, safety and environmental consequences.

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.

Section 3 Documentation

301. Computer based system documentation

Following documents shall be submitted to Classification society for review and approval in accordance with the requirements in this chapter:

1. Detailed list of equipment included in the system (see **302.**)

2. For each equipment, the involved hardware shall be detailed (i.e. motherboard, storage, interfaces (network, serial) and any connectivity)

3. A list of the following software including :
(1) Operating system/firmware
(2) Network services provided and managed by the operating systems
(3) Application Software (see **303.**)
(4) Databases
(5) Configuration files

4. Network or serial flows (source, destination, protocols, protocols details, physical implementation)

5. Network security equipment (which are to be considered and detailed as any other equipment). E.g. traffic management (firewalls, routers, etc) and packet management (IDS, etc)

6. Secure Development Lifecycle Document (see **Sec 5**)

7. Plans for maintenance of system

8. Recovery Plan

9. System Test Plan

10. Description of how the system meets the applicable requirements in **Ch 3** (i.e. Operation Manual or User Manual, etc.)

11. Change Management Plan

302. Inventories

1. The following details shall be documented:
(1) Name
(2) Brand/Manufacturer (supplier)
(3) Model or reference, some devices contain several references
(4) Current Version of the operating system and embedded firmware (software version)and date implemented

303. Software Inventory

For software, the inventory shall contain at least the following information, for each software application program, operating system, firmware etc.:

1. The computer based system where it is installed, a short description of its purpose with brief functional description and technical features (brand, manufacturer, model, main technical data);

2. Version information, license information with expiration dates and a log of updates;

3. Maintenance policy (e.g. on-site vs. remote, periodic vs. occasional, etc.) and responsible persons;

4. Access control policy (e.g. read, write and execution rights)with roles and responsibilities

Section 4 System Requirements

401. General

1. This section specifies the required security capabilities for computer based systems in the scope specified in **103**.

2. The requirements in this section 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.

402. Required security capabilities

The following security capabilities are required for all computer based systems in the scope specified in section **103**.

Table 1

No.	Objective	Requirements	Standard
Protect against casual or coincidental access by unauthenticated entities			
1	Human user identification and authentication	The computer based system shall identify and authenticate all human users who can access the system directly or through interfaces	IEC 62443-3-3/SR1.1
2	Account management	The computer based system 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/SR1.3
3	Identifier management	The computer based system shall provide the capability to support the management of identifiers by user, group and role.	IEC 62443-3-3/SR1.4
4	Authenticator management	The computer based system shall provide the capability to: - Initialize authenticator content - Change all default authenticators upon control system installation - Change/refresh all authenticators - Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	IEC 62443-3-3/SR1.5
5	Wireless access management	The computer based system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication	IEC 62443-3-3/SR1.6
6	Strength of password-based authentication	The computer based system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	IEC 62443-3-3/SR1.7
7	Authenticator feedback	The computer based system shall obscure feedback during the authentication process.	IEC 62443-3-3/SR1.10
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/SR2.1
9	Wireless use control	The computer based system 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/SR2.2

Table 1 (Continued)

No.	Objective	Requirements	Standard
10	Use control for portable and mobile devices	When the computer based system supports use of portable and mobile devices, the system shall include the capability to Limit the use of portable and mobile devices only to those permitted by design 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/SR2.3
11	Mobile code	The computer based system shall control the use of mobile code such as java scripts, ActiveX and PDF.	IEC 62443-3-3/SR2.4
12	Session lock	The computer based system shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock.	IEC 62443-3-3/SR2.5
13	Auditable events	The computer based system 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/SR2.8
14	Audit storage capacity	The computer based system 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/SR2.9
15	Response to audit processing failures	The computer based system shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure.	IEC 62443-3-3/SR2.10
16	Timestamps	The computer based system shall timestamp audit records.	IEC 62443-3-3/SR2.11
Protect the integrity of the computer based system against casual or coincidental manipulation			
17	Communication integrity	The computer based system shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks.	IEC 62443-3-3/SR3.1
18	Malicious code protection	The computer based system 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/SR3.2
19	Security functionality verification	The computer based system 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/SR3.3
20	Deterministic output	The computer based system 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: - Unpowered state, - Last-known value, or - Fixed value	IEC 62443-3-3/SR3.6
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure			
21	Information confidentiality	The computer based system 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/SR4.1

Table 1 (Continued)

No.	Objective	Requirements	Standard
22	Use of cryptography	If cryptography is used, the computer based system shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations.	IEC 62443-3-3/SR4.3
Monitor the operation of the computer based system and respond to incidents			
23	Audit log accessibility	The computer based system shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools.	IEC 62443-3-3/SR6.1
Ensure that the control system operates reliably under normal production conditions			
24	Denial of service protection	The computer based system shall provide the minimum capability to maintain essential functions during DoS events.	IEC 62443-3-3/SR7.1
25	Resource management	The computer based system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	IEC 62443-3-3/SR7.2
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 computer based system without affecting normal operations	IEC 62443-3-3/SR7.3
27	System recovery and reconstitution	The computer based system shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.	IEC 62443-3-3/SR7.4
28	Emergency power	The computer based systems shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	IEC 62443-3-3/SR7.5
29	Network and security configuration settings	The computer based system traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the computer based system supplier. The computer based system shall provide an interface to the currently deployed network and security configuration settings.	IEC 62443-3-3/SR7.6
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 system: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software	IEC 62443-3-3/SR7.7

403. Additional security capabilities

1. The following additional security capabilities are required for computer based systems with network communication to untrusted networks (i.e. interface to any networks outside the scope of **Ch 2**).

Table 2

No.	Objective	Requirements	Standard
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the computer based system from or via an untrusted network.	IEC 62443-3-3/SR1.1, RE2
32	Software process and device identification and authentication	The computer based system shall identify and authenticate software processes and devices	IEC 62443-3-3/SR1.2
33	Unsuccessful login attempts	The computer based system shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period.	IEC 62443-3-3/SR1.11
34	System use notification	The computer based system 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/SR1.12
35	Access via untrusted networks	Any access to the computer based system from or via untrusted networks shall be monitored and controlled.	IEC 62443-3-3/SR1.13
36	Explicit access request approval	The computer based system shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board.	IEC 62443-3-3/SR1.13, RE1
37	Remote session termination	The computer based system 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/SR2.6
38	Cryptographic integrity protection	The computer based system shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks.	IEC 62443-3-3/SR3.1, RE1
39	Input validation	The computer based system 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 computer based system.	IEC 62443-3-3/SR3.5
40	Session integrity	The computer based system shall protect the integrity of sessions. Invalid session IDs shall be rejected.	IEC 62443-3-3/SR3.8
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/SR3.8, RE1

Section 5 Secure Product Development Lifecycle Requirements

501. General

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

(1) Requirement analysis phase
(2) Design phase
(3) Implementation phase
(4) Verification phase
(5) Release phase
(6) Maintenance Phase
(7) End of life phase

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 **502. 1.** to **7.** The said document is required to be submitted to class for review and approval.

502. Controlled process

1. (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. The manufacturer shall have QA process to test the updates before releasing.

2. (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:

(1) The product version number(s) to which the security patch applies;
(2) Instructions on how to apply approved patches manually and via an automated process;
(3) Description of any impacts that applying the patch to the product can have, including reboot;
(4) Instructions on how to verify that an approved patch has been applied; and
(5) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.

3. (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:

(1) Stating whether the product is compatible with the dependent component or operating system security update;

4. (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.

5. (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:

(1) Security capabilities implemented by the product and their role in the defence in depth strategy;
(2) Threats addressed by the defence in depth strategy; and
(3) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code.

6. (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.

7. (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:

(1) Integration of the product, including third-party components, with its product security context;
(2) Integration of the product's application programming interfaces/protocols with user applications;

(3) Applying and maintaining the product's defence in depth strategy;
(4) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
    (A) its contribution to the product's defence in depth strategy
    (B) descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
    (C) setting/changing/deleting its value;
(5) 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;
(6) Instructions and recommendations for periodic security maintenance activities;
(7) Instructions for reporting security incidents for the product to the supplier;
(8) Description of the security best practices for maintenance and administration of the product. ⚓

ANNEX

Annex 1 Summary of actions and documents

1. Legend

(1) Approve: The document shall be submitted to Class Society for approval.
(2) Check: The Surveyor shall verify the availability and update status of the document.
(3) Info: The document shall be submitted to Class Society for information.
(4) Maintain: The indicated stakeholder shall keep the document up to date and aligned with the ac-tual implementation of computer based systems, networks and risk mitigation measures.
(5) Make avail: The indicated stakeholder shall make documentation available to the Surveyor.
(6) Provide: The indicated stakeholder shall provide the documentation and make it available to other concerned stakeholders.

Table 3 Summary of actions and documents

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Identify						
Inventory of hardware and software of the computer based systems in the scope of applicability of Ch 2 and of the networks connecting such systems to each other and to other computer based systems onboard or ashore	Inventory of computer based systems and software onboard	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Protect						
Documentation of the product, equipment or component supplied to construct network segregation, including a diagram of zones and conduits and the configuration of traffic filtering/shaping rules	Network segmentation / segregation	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Documentation on network protection measures including a test plan to verify the implemented control	Network protection sefaguards	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Antivirus, antimalware and antispam software installed or other security measures applied	Antivirus, antimalware, antispam and other protections from malicious code	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

Table 3 Summary of actions and documents (Continued)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Installation locations, physical access restrictions, credential management policy, removable media access points	Physical and logical access control	Design	Provide			Info
		Construction		Maintain		Approve
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Wireless networks diagrams, security capabilities, connection with other networks	Wireless communication	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Remote connection policies and procedures, roles and responsibilities	Remote access control and remote maintenance	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Policies and procedures on use of mobile and portable devices, roles and responsibilities	Use of Mobile and Portable Devices	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Detect						
Description on how to monitor networks, test plan; plans for training and drills	Network operation monitoring	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Monitoring, alarm and diagnostic functions of computer based system and network devices	Diagnostic functions of computer based system and networks	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

Table 3   Summary of actions and documents (Continued)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Respond						
Alarms and other means used to signal cyber incidents and procedures to respond to such incidents; plans for training and drills	Incident response plan	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Instructions on how to activate local independent and/or manual operation (part of the Incident response plan)	Local, independent and/or manual operation	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Instructions to allow personnel to isolate the network in an efficient manner (part of the Incident response plan)	Network isolation	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Minimal risk conditions to be reached in case of unexpected or unmanageable failures or cyber events including procedures to be followed in case of request for human operator's takeover	Fallback to a minimal risk condition	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Recover						
Instructions and procedures for the recovery of a failed system; how to get external assistance and support from ashore; plans for training and drills	Recovery plan	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check

Table 3   Summary of actions and documents (Continued)

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Procedures and operations for backup and restoration of data and software; plans for training and drills	Backup and restore capability	Design	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Documentation on how to execute controlled shutdown, reset to an initial state, roll-back to a safe state and restart from scratch to allow fast and safe recovery	Controlled shutdown, reset, roll-back and restart	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Performance evaluation and testing						
Test Plans describing testing procedures in such a way as to make it possible for the Surveyor or other third party to reproduce onboard the intended test conditions, execute the tests and verify test results, and make it possible a comparison between the results obtained and those obtained by the Supplier and/or the Shipyard/System Integrator. Testing procedures shall include a description of functional tests, failure tests, alarms and other monitoring means used to signal normal conditions, warnings and alerts	Performance evaluation and testing	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Risk Assessment						
Risk assessment for supplied products, equipment or components aimed at identification of cyber risks and relevant mitigation measures, including a concise list of excluded applications of relevant requirements.	Risk assessment for exclusion of computer based system from the application of requirements	Design	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check

⚓

GUIDANCE FOR CYBER RESILIENCE