RUSSIAN MARITIME REGISTER OF SHIPPING

Version: 01.07.2024

RULES

FOR THE CLASSIFICATION AND CONSTRUCTION OF SEA-GOING SHIPS

PART XXI

CYBER RESILIENCE

ND No. 2-020101-174-E

St. Petersburg

RULES FOR THE CLASSIFICATION AND CONSTRUCTION OF SEA-GOING SHIPS (PART XXI)

The present version of Part XXI "Cyber Resilience" of the Rules for the Classification and Construction of Sea-Going Ships of Russian Maritime Register of Shipping (RS, the Register) has been developed on the basis of IACS Unified Requirements E26 (Rev.1 Nov 2023) and E27 (Rev.1 Sep 2023), approved in accordance with the established approval procedure and comes into force on 1 July 2024.

REVISION HISTORY[1]

For this version, there are no amendments to be included in the Revision History.

[1] With the exception of amendments and additions introduced by Rule Change Notices (RCN), as well as of misprints and omissions.

1 GENERAL

1.1 SCOPE OF APPLICATION

1.1.1 The requirements of this Part apply to the following ships and offshore installations[1] contracted for construction on or after 1 July 2024:

.1 passenger ships (including passenger high-speed craft) engaged in international voyages;

.2 cargo ships of 500 gross tonnage and upwards engaged in international voyages;

.3 high-speed cargo craft of 500 gross tonnage and upwards engaged in international voyages;

.4 mobile offshore drilling units of 500 gross tonnage and upwards;

.5 self-propelled mobile offshore units.

1.1.2 Upon desire of the customer, the requirements of this Part may apply to the following:

.1 ships of war and troopships;

.2 cargo ships less than 500 gross tonnage (including high-speed craft);

.3 ships not propelled by mechanical means;

.4 wooden ships of primitive build;

.5 passenger yachts not engaged in trade;

.6 fishing vessels;

.7 other ships and offshore installations not listed in 1.1.1.

1.1.3 The requirements of this Part apply to operational technology (OT) systems onboard ships (i.e. those computer based systems (CBS) using data to control and/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 ship and/or threat to the environment.

1.1.4 In particular, the requirements apply to CBS used for the operation of the following ship functions and systems, if present onboard:

.1 control system of propulsion system;

.2 control system of steering system;

.3 anchoring and mooring;

.4 electrical power generation and distribution;

.5 fire detection and extinguishing system;

.6 cargo processing system;

.7 bilge and ballast systems;

.8 loading computer;

.9 watertight integrity and flooding detection;

.10 lighting (e.g. emergency lighting, low locations, navigation lights, etc.);

.11 any required safety system whose disruption of functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure ship safety system, gas detection system, etc.).

1.1.5 In addition, the following systems shall be included in the scope of application of this Part:

.1 navigational systems required by statutory regulations;

.2 internal and external communication systems required by the RS rules and statutory regulations.

N o t e . For navigation and radiocommunication systems, IEC 61162-460:2024 or other equivalent standards in lieu of the requirements in 3.3 may be applied, on the condition that requirements of Section 2 are complied with.

[1] Hereinafter referred to as "the ships".

1.1.6 The requirements of this Part shall also apply to any Internet Protocol (IP)-based communication interface from CBS in the scope of application of this Part, and to other systems, such as:

.1 passenger or visitor servicing and management systems;

.2 passenger-facing networks;

.3 administrative networks;

.4 crew welfare systems;

.5 any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

1.1.7 System categories are defined in 7.9.4, Part XV "Automation" on the basis of the consequences of a system failure to human safety, safety of the ship and/or threat to the environment.

1.1.8 If ships comply with the requirements specified in this Part, the distinguishing mark **CYBER** given in 2.2.64, Part I "Classification" is added to the character of classification.

1.2 DEFINITIONS AND EXPLANATIONS

Definitions and explanations relating to general terminology of the Rules for the Classification and Construction of Sea-Going Ships[1] are given in Part I "Classification".

For the purpose of this Part the following definitions have been adopted.

Attack surface is a set of all possible points where an unauthorized user can access a system, cause an effect on or extract data from. The attack surface comprises two categories: digital and physical:

digital attack surface encompasses all the hardware and software that connect to an organization's network, including applications, code, ports, servers and websites;

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.

Authentication is a provision of assurance that a claimed characteristic of an entity is correct.

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

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

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

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

Cyber resilience is 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 ship and/or threat to the environment.

Data compromise is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the protected data transferred, stored or otherwise processed.

Defence in depth is the information security strategy integrating people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

---

[1] Hereinafter referred to as "these Rules".

Essential services are services for propulsion and steering, and safety of the ship. Essential services comprise primary essential services and secondary essential services:

primary essential services are those services which need to be in continuous operation to maintain propulsion and steering;

secondary essential services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the ship's safety.

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

Firmware is a 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.

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

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

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

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

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

Network segment is a set of nodes having the same network address plan. A network segment is a broadcast domain.

Note. In the stack of TCP/IP protocols, the 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).

Network switch (Switch) is a device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

Offensive cyber manoeuvre is an action that result in denial, degradation, disruption, destruction, or manipulation of IT or OT systems.

Operational technology (OT) are 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.

OT system is a computer based system, which provide control, alarm, monitoring, safety or internal communication functions.

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

Protocol is 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 stack and various field buses.

Recovery means to develop and implement the appropriate measures and activities to maintain resilience and to restore any functional capabilities that were impaired due to a cyber incident. The recovery function supports timely return to normal CBS operations to reduce the impact from a cyber incident.

Security zone is a collection of CBS in the scope of application of this Section that meet the same security requirements. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

Shipowner/Company[1] is the owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The shipowner can be the shipyard or systems integrator (builder or shipyard) during initial construction. After ship delivery, the shipowner may delegate some responsibilities to the ship management company.

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

System is a combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes.

System categories (I, II, III): system categories are assigned based on their failure effect on occurrence of dangerous situations for human safety, safety of the ship and/or threat to the environment as defined in 7.9.4, Part XV "Automation".

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

Untrusted network is any network outside the scope of application of this Part.

Virtual private network (VPN) is a virtual network built over the existing physical networks that provides a secure communication tunnel for data transferred between the networks or devices by means of tunneling, means of security control and translation of end addresses similar to the connection in the dedicated network.

[1] Hereinafter referred to as "the shipowner".

2 CYBER RESILIENCE OF SHIPS

2.1 GOALS AND ORGANIZATION OF REQUIREMENTS

2.1.1 Primary goal.

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

Safe and secure shipping can be achieved through effective cyber risk management system.

2.1.2 Sub-goals.

To achieve the primary goal, the following sub-goals of cyber risk management are defined that shall be performed simultaneously and considered as a part of the integral comprehensive risk management system:

.1 identify: develop an organizational understanding on CBS to manage cyber security 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.

2.1.3 Organization of requirements.

The requirements are organized according to a goal-based approach. Functional/technical requirements are given for the achievement of each of the specific sub-goals. The requirements are intended to allow a uniform implementation by stakeholders and to make them applicable to all types of ships, in such a way as to enable an acceptable level of resilience.

For each requirement, a rationale is given.

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

2.2 REQUIREMENTS

This Chapter contains the requirements to be satisfied in order to achieve the primary goal defined in 2.1.1, organized according to five sub-goals identified in 2.1.2.

The requirements shall be fulfilled by the stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified (refer to definitions in 1.2):

shipowner;

systems integrator;

suppler.

Whilst the above requirements may be fulfilled by these stakeholders, for the purposes of this Section, responsibility to fulfil them shall lie with the stakeholder who has contracted with the Register.

2.2.1 Identify.

The requirements are aimed at identifying:

the CBS onboard, their interdependencies and the relevant information flows;

the key resources involved in their management, operation and governance, their roles and responsibilities.

2.2.1.1 Ship Asset Inventory.

2.2.1.1.1 Requirement.

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

2.2.1.1.2 Requirement details.

The Ship Asset Inventory shall include at least the CBS indicated in 1.1.3 — 1.1.6, if present onboard.

The Ship Asset Inventory shall be kept updated during the entire life of the ship. Software and hardware modifications potentially introducing new vulnerabilities or modifying functional dependencies or connections among systems shall be recorded in the Inventory.

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

2.2.1.1.2.1 Hardware:

.1 for all hardware devices in the scope of application of this Part, the Ship Asset Inventory shall include at least the information specified in 3.2.1.1;

.2 the Ship Asset Inventory shall specify system categories and security zones associated with CBS.

2.2.1.1.2.2 Software:

.1 for all software in the scope of application of this Part (e.g., application programs, operating systems, firmware), the Ship Asset Inventory shall include at least the information specified in 3.2.1.1;

.2 software of CBS in the scope of application of this Part shall be maintained and updated in accordance with the shipowner's process for management of the software maintenance and update policy in the Ship Cyber Security and Resilience Program (refer to 2.3.3.1).

R a t i o n a l e . The Ship Asset Inventory and relevant software used in OT systems is essential for an effective management of cyber resilience of the ship, the main reason being that every CBS becomes a potential point of vulnerability. Cybercriminals can exploit unaccounted and out-of-date hardware and software to hack systems. Moreover, managing CBS assets enables shipowners understand the criticality of each system to ship safety objectives.

2.2.1.1.3 Demonstration of compliance.

2.2.1.1.3.1 Design phase:

.1 the systems integrator shall submit the Ship Asset Inventory to the Register (refer also to 2.3.1.3);

.2 the Ship Asset Inventory shall incorporate the asset inventories of all individual CBS in the scope of application of this Part, as well as other equipment delivered by the systems integrator.

2.2.1.1.3.2 Construction phase:

.1 the systems integrator shall keep the Ship Asset Inventory updated.

2.2.1.1.3.3 Commissioning phase:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate that:

the Ship Asset Inventory is updated and completed at delivery;

all CBS in the scope of application of this Part are correctly represented by the Ship Asset Inventory;

software of CBS in the scope of application of this Part is kept regularly updated.

2.2.1.1.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the process of management of change (MoC) for all CBS in the scope of application of this Part, addressing at least the following requirements:

management of change (MoC) (refer to 2.3.3);

hardware and software modifications (refer to 2.2.1.1.2);

.2 the shipowner shall in the Ship Cyber Security and Resilience Program also describe the management of the software updates, addressing at least the following requirements:

vulnerabilities and cyber risks (refer to 2.2.1.1.2);

security patching (refer to 2.2.2.6.2.2);

.3 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

the approved MoC process is adhered to;

known vulnerabilities and functional dependencies are considered for software in CBS;

the Ship Asset Inventory is kept updated;

.4 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.1.1.3.4.3;

.5 special survey.

The shipowner shall demonstrate to the Register implementation of the requirements of 2.2.1.1.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2 Protect.

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

2.2.2.1 Security zones and network segmentation.

2.2.2.1.1 Requirement:

.1 all CBS in the scope of application of this Part shall be grouped into security zones with well-defined security policies and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls, simplex serial links, TCP/IP diodes, dry contacts, etc.);

.2 only explicitly allowed traffic shall traverse a security zone boundary.

2.2.2.1.2 Requirement details:

.1 a security zone may contain multiple CBS and networks, all of which shall comply with applicable security requirements given in this Section and in Section 3;

.2 the network(s) of a security zone shall be logically and/or physically segmented from other zones or networks;

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

.4 navigational and communication systems shall not be in same security zone as machinery or cargo systems. If navigation and radiocommunication systems are approved in accordance with other equivalent standards (refer to 1.1.5), these systems shall be in a dedicated security zone;

.5 wireless devices shall be in dedicated security zones considering requirements of 2.2.2.5;

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

.7 it shall be possible to isolate a security zone without affecting the primary functionality of CBS in the zone.

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

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

2.2.2.1.3 Demonstration of compliance.

2.2.2.1.3.1 Design phase:

.1 the systems integrator shall submit to the Register Zones and Conduit Diagram and the Cyber Security Design Description (refer to 2.3.1.1 and 2.3.1.2);

.2 the Zones and Conduit Diagram shall illustrate CBS in the scope of application of this Part, how they are grouped into security zones, and include the following information:

clear indication of the security zones;

simplified illustration of each CBS in the scope of application of this Part, and indication of the security zone, in which CBS is allocated, and indication of physical location of the CBS/equipment;

reference to the approved version of the CBS system topology diagrams provided by the suppliers (refer to 3.2.1.2);

illustration of network communication between systems in a security zone;

illustration of any network communication between systems in different security zones (conduits);

illustration of any communication between systems in a security zone and untrusted networks (conduits);

.3 the systems integrator shall include the following information in the Cyber Security Design Description:

a short description of CBS allocated to the security zone. It shall be possible to identify each CBS in the Zones and Conduit Diagram;

network communication between CBS in the same security zone. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication;

network communication between CBS in different security zones. The description shall include purpose and characteristics (i.e. protocols and data flows) of the communication. The description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules);

any communication between CBS in security zones and untrusted networks. The description shall include discrete signals, serial communication, purpose and characteristics (protocols and data flows) of IP-based network communication. The Cyber Security Design Description shall also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

2.2.2.1.3.2 Construction phase:

.1 the systems integrator shall keep the Zones and Conduit Diagram updated.

2.2.2.1.3.3 Commissioning phase:

.1 the systems integrator shall submit the Ship Cyber Resilience Test Procedure and demonstrate to the Register that:

the security zones on board are implemented in accordance with the approved documents (Zones and Conduit Diagram, Cyber Security Design Description, Ship Asset Inventory, and relevant documents provided by the supplier). This may be done by visual inspection, network scanning or other methods confirming that the installed equipment is grouped in security zones according to the approved design;

security zone boundaries allow only the traffic that has been documented in the approved Cyber Security Design Description. This may be done by evaluation of firewall rules or port scanning.

2.2.2.1.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements:

principle of least functionality (refer to 2.2.2.2.1.3);

explicitly allowed traffic (refer to 2.2.2.1.1.2);

protection against denial of service (DoS) events (refer to 2.2.2.2.1.2);

inspection of security audit records (refer to 2.2.3.1.2);

.2 first annual survey.

The shipowner shall demonstrate to the Register that the Zones and Conduit Diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that security zone boundaries are managed in accordance with the above requirements;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.2.1.3.4.2;

.4 special survey.

The shipowner shall demonstrate to the Register fulfillment of the requirements of 2.2.2.1.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2.2 Network protection safeguards.

2.2.2.2.1 Requirement:

.1 security zones shall be protected by firewalls or equivalent means as specified in 2.2.2.1;

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

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

2.2.2.2.2 Requirement details.

When designing the network in order to minimize the risk of denial of service (DoS) and network storm/high rate of traffic, it is necessary to provide means to meet the intended data flow through the network. Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format.

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

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

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

2.2.2.2.3 Demonstration of compliance.

2.2.2.2.3.1 Design phase.

Demonstration of compliance is not required in the design phase.

2.2.2.2.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.2.2.3.3 Commissioning phase:

.1 the systems integrator shall submit Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) to the Register and demonstrate:

test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable;

test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests shall cover flooding of network (i.e. attempt to consume the available capacity on the network segment), and application layer attack (i.e. attempt to consume the processing capacity of selected endpoints in the network)[1];

test that unnecessary functions, ports, protocols and services in CBS have been removed or prohibited in accordance with hardening guidelines provided by the suppliers (refer to 3.4.7 and 3.5.3.4.7)[1].

2.2.2.2.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of the requirements of 2.2.2.2.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

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

2.2.2.3.1 Requirement.

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

[1] The commissioning tests may be omitted if performed during the CBS certification in compliance with 2.3.2.1.

2.2.2.3.2 Requirement details:

.1 malware protection shall be implemented on CBS in the scope of application of this Part. On CBS having an operating system for which industrial-standard antivirus and antimalware software is available and maintained up-to-date, antivirus and/or antimalware software shall be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for categories II and III CBS performing real-time tasks);

.2 on CBS where antivirus and antimalware software cannot be installed, malware protection shall be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

Rationale. 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.

Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off the malicious intruding viruses performing a prophylactic function. It detects potential virus and then works to remove it, mostly before the virus gets to harm the system.

Common means for malicious code to enter CBS 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.

2.2.2.3.3 Demonstration of compliance.

2.2.2.3.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

for each CBS, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software;

for CBS with antimalware software, information about how to keep the software updated;

any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.

2.2.2.3.3.2 Construction phase:

.1 the systems integrator shall ensure that malware protection is kept updated during the construction phase.

2.2.2.3.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate antimalware software or other compensating countermeasures is effective (test e.g., with a trustworthy antimalware test file).

2.2.2.3.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of malware protection, addressing at least the following requirements:

maintenance/update (refer to 2.2.2.3.2);

operational procedures, physical safeguards (refer to 2.2.2.3.2);

use of mobile, portable, removable media (refer to 2.2.2.4.2.4 and 2.2.2.7.2);

access control (refer to 2.2.2.4);

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

any antimalware software is being maintained and updated;

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

procedures for use of portable, mobile or removable devices are followed;
policies and procedures for access control are followed;
physical safeguards are maintained;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.2.3.3.4.2;

.4 special survey.

The shipowner shall demonstrate to the Register fulfillment of the requirements in 2.2.2.3.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2.4 Access control.

2.2.2.4.1 Requirement.

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

2.2.2.4.2 Requirement details.

Access to CBS and networks in the scope of application of this Part and all information stored on such systems shall only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality.

2.2.2.4.2.1 Physical access control.

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

2.2.2.4.2.2 Physical access control for visitors.

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

2.2.2.4.2.3 Physical access control of network access points:

.1 access points to onboard networks connecting category II and/or category III CBS shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance;

.2 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).

2.2.2.4.2.4 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 considering requirements of 2.2.2.7.

2.2.2.4.2.5 Management of credentials:

.1 CBS 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.

N o t e . CBS shall identify and authenticate human users in accordance with item 1, Table 3.3.1. In other words, it is not necessary to "uniquely" identify and authenticate all human users;

.2 onboard CBS shall be provided with appropriate access control that fits to the policy of their security zone but does not adversely affect their primary purpose. CBS, which require strong access control, may need to be secured using a strong encryption key or multi-factor authentication;

.3 administrator privileges shall be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to CBS, who as part of their role in the company or onboard need to log on to systems using these privileges.

2.2.2.4.2.6 Least privilege principle:

.1 any human user allowed to access CBS and networks in the scope of application of this Part shall have only the bare minimum privileges necessary to perform his/her functions;

.2 the default configuration for all new account privileges shall be set as low as possible. Wherever possible, raised privileges shall be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time shall be avoided, e.g. by regular auditing of user accounts.

R a t i o n a l e . Attackers may attempt to access the ship's systems and data from either onboard the ship and within the shipowner's 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.

Physical threats and relevant countermeasures are also considered in the International Ship and Port Facility Security Code, adopted by resolution 2 of 2002 IMO conference, as amended[1]. Similarly, the International Safety Management Code, adopted by IMO resolution A.741(18) as amended[2] contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of the 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.

2.2.2.4.3 Demonstration of compliance.

2.2.2.4.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

location and physical access controls for CBS. Devices providing human machine interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices shall be specified separately.

2.2.2.4.3.2 Construction phase.

The systems integrator shall prevent unauthorized access to CBS during the construction phase.

2.2.2.4.3.3 Commissioning phase:

.1 the systems integrator shall submit Ship Cyber Resilience Test Procedure and demonstrate the following to the Register:

components of CBS are located in areas or enclosures where physical access can be controlled by authorized crew;

user accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed[3].

---

[1] Hereinafter referred to as "the ISPS Code".

[2] Hereinafter referred to as "the ISM Code".

[3] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.2.4.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of logical and physical access, addressing at least the following requirements:

physical access control (refer to 2.2.2.4.2.1);

physical access control for visitors (refer to 2.2.2.4.2.2);

physical access control of network access points (refer to 2.2.2.4.2.3);

management of credentials (refer to 2.2.2.4.2.5);

least privilege policy (refer to 2.2.2.4.2.6);

.2 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of confidential information, addressing at least the following requirements:

confidential information (refer to 2.2.1.1.2);

information allowed to authorized personnel (refer to 2.2.2.4.2);

information transmitted on the wireless network (refer to 2.2.2.5.2);

.3 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

personnel are authorized to access CBS in accordance with their responsibilities;

only authorized devices are connected to CBS;

visitors are given access to CBS according to the relevant policies and procedures;

physical access controls are maintained and applied;

credentials, keys, secrets, certificates, relevant CBS documentation, and other sensitive information are managed and kept confidential according to the relevant policies and procedures;

.4 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.2.4.3.4.3.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2.5 Wireless communication.

2.2.2.5.1 Requirement.

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

.1 cyber incidents will not propagate to other CBS;

.2 only authorized human users will gain access to the wireless network;

.3 only authorized processes and devices will be allowed to communicate on the wireless network;

.4 information in transit on the wireless network cannot be manipulated or disclosed.

2.2.2.5.2 Requirement details:

.1 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;

.2 devices on the wireless network shall only communicate on the wireless network (i.e. they shall not be "dual-homed");

.3 wireless networks shall be designed as separate segments in accordance with 2.2.2.1 and protected in accordance with 2.2.2.2;

.4 wireless access points and other devices in the network shall be installed and configured such that access to the network can be controlled;

.5 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.

R a t i o n a l e . Wireless networks give rise to additional cyber security risks than wired networks. This is mainly due to less physical protection of the devices and the use of the radio frequency communication.

Inadequate physical access control may lead to unauthorized personnel gaining access to the physical devices, which in turn can lead to circumventing logical access restrictions or deployment of rogue devices on the network.

Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn can cater for attacks such as piggybacking (use of wireless network for unauthorized access) or evil twin attacks (substitution of the original access point by a spoof to which the user connects, thus, providing the attacker the possibility to access the confidential information).

2.2.2.5.3 Demonstration of compliance.

2.2.2.5.3.1 Design phase.

The systems integrator shall include the following information in the Cyber Security Design Description:

description of wireless networks in the scope of application of this Part. The description shall include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

2.2.2.5.3.2 Construction phase.

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

2.2.2.5.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate that:

only authorized devices can access the wireless network;

secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyzer tool).

2.2.2.5.3.4 Operation phase:

.1 special survey.

Subject to modifications of the wireless networks in the scope of application of this Part, the shipowner shall demonstrate to the Register the fulfillment of requirements in 2.2.2.5.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2.6 Remote access control and communication with untrusted networks.

2.2.2.6.1 Requirement.

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

2.2.2.6.2 Requirement details:

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;

for CBS in the scope of application of this Part, no IP address shall be exposed to untrusted networks;

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.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.2.6.2.1 Design.

CBS in the scope of application of this Section shall:

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;

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;

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.

2.2.2.6.2.2 Additional requirements for remote maintenance.

When remote access is used for maintenance, the following requirements shall be complied with in addition to those in 2.2.2.6.2.1:

.1 documentation shall be provided to show how they connect and integrate with the shore side;

.2 security patches and software updates shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects or cyber events that cannot be tolerated. A confirmation report from the software supplier towards above shall be obtained, prior to undertaking remote update;

.3 suppliers shall provide plans for and make security updates available to the shipowner (refer to 3.4.2, 3.4.3, 3.4.4);

.4 at any time, during remote maintenance activities, authorized personnel shall have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of CBS and systems involved;

.5 multi-factor authentication is required for any access by human users to CBS in the scope from an untrusted network;

.6 after a configurable number of failed remote access attempts, the next attempt shall be blocked for a predetermined length of time;

.7 if the connection to the remote maintenance location is disrupted for some reason, access to the system shall be terminated by an automatic logout function.

R a t i o n a l e . Onboard CBS 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 CBS makes them vulnerable to cyber incidents. Attackers may attempt to access onboard CBS through connectivity with the Internet and may be able to make changes that affect a CBS's operation or even achieve full control of CBS, or attempt to download information from the ship's CBS. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects cyber resilience, special care shall 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.

2.2.2.6.3 Demonstration of compliance.

2.2.2.6.3.1 Design stage:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

list of CBS in the scope of application of this Part that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks;

for each CBS, a description of compliance with requirements in 2.2.2.6.2, as applicable.

2.2.2.6.3.2 Construction phase.

The systems integrator shall ensure that any communication with untrusted networks is only temporarily enabled and used in accordance with the requirements of 2.2.2.6.

2.2.2.6.3.3 Commissioning phase:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate that:

communication with untrusted networks is secured in accordance with 3.3.2 and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool);

remote access requires multifactor authentication of the remote user;

a limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established;

remote connections shall be explicitly accepted by responsible personnel on board;

remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity;

remote sessions are logged (refer to item 13, Table 3.3.1);

instructions or procedures are provided by the respective product suppliers (refer to 3.2.1.3).

2.2.2.6.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements:

user's manual (refer to 2.2.2.6.2);

roles and permissions (refer to 2.2.2.6.2);

patches and updates (refer to 2.2.2.6.2.2);

confirmation prior to undertaking remote software update (refer to 2.2.2.6.2.2);

interrupt, abort, roll back (refer to 2.2.2.6.2.2);

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

remote access sessions have been recorded or logged and carried out according to the relevant policies and user manuals;

installation of security patches and other software updates have been carried out in accordance with management of change procedures and in cooperation with the supplier;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.2.6.3.4.2;

.4 special survey.

The shipowner shall demonstrate to the Register fulfillment of the requirements of 2.2.2.6.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.2.7 Use of mobile and portable devices.

2.2.2.7.1 Requirement.

The use of mobile and portable devices in CBS in the scope of application of this Part shall be limited to only necessary activities and be controlled in accordance with item 10, Table 3.3.1. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked.

2.2.2.7.2 Requirement details:

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

R a t i o n a l e . CBS 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.

2.2.2.7.3 Demonstration of compliance.

2.2.2.7.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

any CBS in the scope of application of this Part that do not meet the requirements of item 10, Table 3.3.1, i.e. that shall have protection of interface ports by physical means such as port blockers.

2.2.2.7.3.2 Construction phase:

.1 the systems integrator shall ensure that use of physical interface ports in CBS is controlled in accordance with item 10, Table 3.3.1, and that any use of such devices follows procedures to prevent malware from being introduced in CBS.

2.2.2.7.3.3 Commissioning phase:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure and demonstrate that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures shall be demonstrated as relevant:

use of mobile and portable devices is restricted to authorized users;

interface ports can only be used by specific device types;

files cannot be transferred to the system from mobile and portable devices;

files on such devices will not be automatically executed (by disabling autorun);

network access is limited to specific MAC or IP addresses;

unused interface ports are disabled and/or physically blocked.

2.2.2.7.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management of mobile and portable devices, addressing at least the following requirements:

implementation of policy and procedures (refer to 2.2.2.4.2.4);

physical block of interface ports (refer to 2.2.2.7.1);

use by authorized personnel only (refer to 2.2.2.7.3.3);

connection of only authorized devices (refer to 2.2.2.7.3.3);

consideration of risks of introducing malware (refer to 2.2.2.7.3.3);

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

the use of mobile, portable or removable media is restricted to authorized personnel and follows relevant policies and procedures;

only authorized devices are connected to CBS;

means to restrict use of physical interface ports are implemented in accordance with the approved design documentation;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.2.7.3.4.2;

.4 special survey.

The shipowner shall demonstrate to the Register fulfillment of requirements of 2.2.2.7.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.3 Detect.

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

2.2.3.1 Network operation monitoring.

2.2.3.1.1 Requirement.

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

2.2.3.1.2 Requirement details:

.1 measures to monitor networks in the scope of application of this Part shall have the following capabilities:

monitoring and protection against excessive traffic;

monitoring of network connections;

monitoring and recording of device management activities;

protection against connection of unauthorized devices;

generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier (refer to 7.9.8.2.1.5, Part XV "Automation");

.2 intrusion detection systems (IDS) may be implemented, subject to the following:

the IDS shall be qualified by the supplier of the respective CBS;

the IDS shall be passive and not activate protection functions that may affect the performance of CBS;

relevant personnel shall be trained and qualified for using IDS.

Rationale. Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction can result in incidents where the ship 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.

2.2.3.1.3 Demonstration of compliance.

2.2.3.1.3.1 Design phase.

Demonstration of compliance is not required in the design phase.

2.2.3.1.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.3.1.3.3 Commissioning phase[1]:

.1 the systems integrator shall specify in the Ship Cyber Resilience Test Procedure and demonstrate to the Register the network monitoring and protection mechanisms in CBS:

test that disconnected network connections shall activate alarm and that the event is recorded;

test that abnormally high network traffic is detected, and that alarm and audit record is generated; this test may be carried on together with the test in 2.2.4.4.3.3;

demonstrate that CBS will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (refer also to 2.2.2.2.3.3);

demonstrate generation of audit records (logging of security-related events);

if intrusion detection system (IDS) is implemented, demonstrate that this is passive and does not activate protection functions that may affect intended operation of CBS;

.2 any intrusion detection system (IDS) in CBS in the scope of application of this Part shall be subject to technical supervision by the Register. Relevant documentation shall be submitted to the Register for approval with subsequent survey to be carried out on board.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.3.1.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management activities to detect anomalies in CBS and networks, addressing at least the following requirements:

reveal and recognize anomalous activity (refer to 2.2.3);

inspection of security audit records (refer to 2.2.3.1.2);

instructions or procedures to detect incidents (refer to 2.2.4.1.1);

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

CBS are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the CBS;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.3.1.3.4.2;

.4 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of the requirements of 2.2.3.1.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.3.2 Verification and diagnostic functions of CBS and networks.

2.2.3.2.1 Requirement.

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

2.2.3.2.2 Requirement details:

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

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

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

2.2.3.2.3 Demonstration of compliance.

2.2.3.2.3.1 Design phase.

Demonstration of compliance is not required in the design phase.

2.2.3.2.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.3.2.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate the effectiveness of the procedures for verification of security functions provided by the suppliers.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.3.2.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the management activities to verify correct operation of the security functions in CBS and networks, addressing at least the following requirements:

test and maintenance periods (refer to 2.2.3.2.2);

period maintenance (refer to 2.3.3.3);

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

the security functions in CBS are periodically tested or verified;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.3.2.3.4.2.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.4 Respond.

The requirements 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 CBS and networks onboard.

2.2.4.1 Incident Response Plan.

2.2.4.1.1 Requirement.

An Incident Response Plan shall be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident Response Plan shall contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBS in the scope of application of this Section.

2.2.4.1.2 Requirement details:

.1 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;

.2 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;

.3 the Incident Response Plan shall, as a minimum, include the following information:

breakpoints for the isolation of compromised systems;

a description of alarms and indicators signalling detected ongoing cyber events and/or abnormal symptoms caused by cyber events;

a description of expected consequences related to cyber incidents;

response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any;

independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable;

.4 the Incident Response Plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it.

R a t i o n a l e . An Incident Response Plan is an instrument aimed to help responsible persons respond to cyber incidents. As such, the Incident Response Plan is as effective as it is simple and carefully designed. When developing the Incident Response Plan, it is important to understand the significance of any cyber incident and prioritize response actions accordingly.

Means for maintaining as much as possible the functionality and a level of service for a safe operation of the ship, e.g. transfer active execution to a standby redundant unit, shall also be indicated. Designated personnel of the shipowner/company (refer to Section 4, ISM Code) shall be integrated with the ship in the event of a cyber incident.

2.2.4.1.3 Demonstration of compliance.

2.2.4.1.3.1 Design phase.

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

references to information provided by the suppliers (refer to 3.2.1.8) that may be applied by the shipowner to establish plans for incident response.

2.2.4.1.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.4.1.3.3 Commissioning phase.

Demonstration of compliance is not required in the commissioning phase.

2.2.4.1.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe the Incident Response Plan in case of cyber incident addressing at least the following requirements:

description of who, when and how to respond to cyber incidents in accordance with requirements of 2.2.4.1;

procedures or instructions for local/manual control in accordance with requirements in 2.2.4.2;

procedures or instructions for isolation of security zones in accordance with requirements in 2.2.4.3;

description of expected behaviour of CBS in the event of cyber incidents in accordance with requirements in 2.2.4.4;

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

the Incident Response Plan is available for the responsible personnel onboard in case of cyber incident;

instructions for local/manual controls are available for responsible personnel onboard in accordance with the requirements;

instructions for disconnection/isolation of security zones are available for responsible personnel onboard;

any cyber incidents have been responded to in accordance with the Incident Response Plan;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.4.1.3.4.2.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.4.2 Local, independent and/or manual operation.

2.2.4.2.1 Requirement.

Any CBS needed for local control as required by 2.3.4 of Part XV "Automation" shall be independent of the primary control system. This includes also necessary human machine interface (HMI) for effective local operation.

2.2.4.2.2 Requirement details:

.1 the CBS for local control and monitoring shall be self-contained and not depend on communication with other CBS for its intended operation;

.2 if communication to the remote control system or other CBS is arranged by networks, segmentation and protection safeguards as described in 2.2.2.1 and 2.2.2.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone;

.3 notwithstanding the above, special considerations can be given to CBS with different concepts on case by case basis;

.4 CBS for local control and monitoring shall otherwise comply with requirements in this Part.

R a t i o n a l e . Independent local controls of machinery and equipment needed to maintain safe operation is a fundamental principle for manned ships. The objective of this requirement is to ensure that personnel can cope with failures and other incidents by performing manual operations in close vicinity of the machinery in case of failure of the remote control caused by malicious cyber events.

2.2.4.2.3 Demonstration of compliance.

2.2.4.2.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

description of how the local controls specified in 2.3.4, Part XV "Automation" are protected from cyber incidents in any connected remote or automatic control systems.

2.2.4.2.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.4.2.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate that the required local controls in the scope of application of this Part needed for safety of the ship can be operated independently of any remote or automatic control systems.

2.2.4.2.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of requirements of 2.2.4.2.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.4.3 Network isolation.

2.2.4.3.1 Requirement.

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

2.2.4.3.2 Requirement details:

.1 where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner;

.2 individual systems' data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems shall have compensations for data or functional inputs if isolated during a contingency.

---

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

R a t i o n a l e . In the event that a security breach has occurred, the Incident Response Plan shall include actions to prevent further propagation and effects of the incident. Such actions may be to isolate network segments and control systems supporting essential functions.

2.2.4.3.3 Demonstration of compliance.

2.2.4.3.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

specification of how to isolate each security zone from other zones or networks. The effects of such isolation shall also be described, demonstrating that CBS in a security zone do not rely on data transmitted by IP-networks from other zones or networks.

2.2.4.3.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.4.3.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure and demonstrate by disconnecting all networks traversing security zone boundaries, that CBS in the security zone maintain adequate operational functionality without network communication with other security zones or networks.

2.2.4.3.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of the requirements of 2.2.4.3.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.4.4 Fallback to a minimal risk condition.

2.2.4.4.1 Requirement.

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

2.2.4.4.2 Requirement details:

.1 as soon as a cyber incident affecting CBS or network is detected, compromising the system's ability to provide the intended service as required, the system shall fall back to a condition, in which a reasonably safe state can be achieved. Fall-back actions may include:

bringing the system to a complete stop;

disengaging the system;

transferring control to another system or crew;

other compensating actions;

.2 fallback to the minimum risk condition shall occur in a time frame adequate to keep the ship in a safe condition;

.3 the ability of a system to fall back to the minimal risk condition shall be considered from the design phase by the supplier and the systems integrator.

R a t i o n a l e . The ability of CBS and integrated systems to fall back to one or more minimal risk conditions to be reached in case of unexpected or unmanageable failures or events is a safety measure aimed to keep the system in a consistent, known and safe state.

Fallback to the minimal risk condition usually implies the capability of a system to abort the current operation and signal respectively to the crew, 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.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.4.4.3 Demonstration of compliance.

2.2.4.4.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

specification of safe state for the control functions in CBS in the scope of application of this Part.

2.2.4.4.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.4.4.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure and demonstrate that CBS in the scope of application of this Part respond to cyber incidents in a safe manner (refer to 2.2.4.4.3.1), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests shall at least include denial of service (DoS) attacks and may be done together with related tests in 2.2.3.1.3.3.

2.2.4.4.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of requirements of 2.2.4.4.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.5 Recover.

The requirements are aimed at the development and implementation of appropriate means supporting the ability to restore CBS and networks onboard affected by cyber incidents.

2.2.5.1 Recovery Plan.

2.2.5.1.1 Requirement.

A Recovery Plan shall be made by the shipowner to support restoring CBS in the scope of application of this Part to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom shall be part of the Recovery Plan.

2.2.5.1.2 Requirement details:

.1 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;

.2 Recovery Plan 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;

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

.3 when developing Recovery Plan, the various systems and subsystems involved shall be specified. The following recovery objectives shall also be specified:

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;

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;

.4 once the recovery objectives are defined, a list of potential cyber incidents shall be created, and the recovery procedure developed and described;

.5 Recovery Plan shall include, or refer to the following information:

instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation;

processes and procedures for the backup and secure storage of information;

complete and up-to-date logical network diagram;

the list of personnel responsible for restoring the failed system;

communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.;

current configuration information for all components;

.6 CBS required for ship operation and navigation shall be prioritized in the Recovery Plan to ensure the safety of onboard personnel;

.7 Recovery Plan in hard copy onboard and ashore shall be available to the crew and shore-based personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

R a t i o n a l e . 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.

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

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

2.2.5.1.3 Demonstration of compliance.

2.2.5.1.3.1 Design phase:

.1 the systems integrator shall include the following information in the Cyber Security Design Description:

references to information provided by the suppliers (refer to 3.2.1.8) that may be applied by the shipowner to establish Recovery Plan in case of a cyber incident.

2.2.5.1.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.5.1.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.2.5.1.3.4 Operation phase:

.1 the shipowner shall in the Ship Cyber Security and Resilience Program describe incident recovery plans covering all CBS in the scope of application of this Part and addressing at least the following requirements:

description of who, when and how to restore and recover from cyber incidents in accordance with requirements of 2.2.5.1;

policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of CBS in accordance with requirements in 2.2.5.2;

reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in 2.2.5.2 and 2.2.5.3;

.2 first annual survey.

The shipowner shall submit to the Register records or other documented evidence demonstrating implementation of the Ship Cyber Security and Resilience Program, i.e. that:

instructions and/or procedures for incident recovery are available for the responsible crew members onboard;

equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible crew members onboard;

backups of CBS are taken in accordance with the policies and procedures;

manuals and procedures for shutdown, reset, restore and restart are available for the responsible crew members onboard;

.3 subsequent annual surveys.

The shipowner shall upon request by the Register demonstrate implementation of the Ship Cyber Security and Resilience Program by presenting records or other documented evidence as specified in 2.2.5.1.3.4.2.

General requirements for surveys in the operation phase are given in 2.3.3.

2.2.5.2 Backup and restore capability.

2.2.5.2.1 Requirement.

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

R a t i o n a l e . The purpose of a backup and restore strategy is to protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following:

planning and testing responses to different kinds of failures;

configuring the database environment for backup and recovery;

setting up a backup schedule;

monitoring the backup and recovery environment;

creating a database copy for long-term storage;

moving data from one database or one host to another, etc.

2.2.5.2.2 Requirement details.

2.2.5.2.2.1 Restore capability:

.1 CBS in the scope of application of this Part shall have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident;

.2 data shall be restorable from a secure copy or image;

.3 information and backup facilities shall be sufficient to recover from a cyber incident.

2.2.5.2.2.2 Backup:

.1 CBS and networks in the scope of application of this Part shall provide backup for data. The use of offline backups shall also be considered to improve tolerance against ransomware and worms affecting online backup appliances;

.2 backup plans shall be developed, including scope, mode and frequency, storage medium and retention period.

2.2.5.2.3 Demonstration of compliance.

2.2.5.2.3.1 Design phase.

Demonstration of compliance is not required in the design phase.

2.2.5.2.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.5.2.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate the procedures and instructions for restore provided by the suppliers for CBS in the scope of application of this Part.

2.2.5.2.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of requirements of 2.2.5.2.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

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

2.2.5.3.1 Requirement.

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

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

2.2.5.3.2 Requirement details:

.1 CBS and networks in the scope of application of this Part shall be capable of:

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;

resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state;

rolling back to a previous configuration and/or state, to restore system integrity and consistency;

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;

.2 documentation shall be available to the crew on how to execute the above-mentioned operations in case of a system affected by a cyber incident.

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

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

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

The reset operation typically kicks 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 may have different effects.

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

Restarting a system and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source appears to be an effective approach to recover from unexpected faults or cyber incidents. Restart operations 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.

2.2.5.3.3 Demonstration of compliance.

2.2.5.3.3.1 Design phase.

The systems integrator shall include the following information in the Cyber Security Design Description:

references to user's manuals or procedures describing how to safely shut down, reset, restore and restart CBS in the scope of application of this Part.

2.2.5.3.3.2 Construction phase.

Demonstration of compliance is not required in the construction phase.

2.2.5.3.3.3 Commissioning phase[1]:

.1 the systems integrator shall submit to the Register the Ship Cyber Resilience Test Procedure (refer to 2.3.2.1) and demonstrate that user's manuals or procedures are established for shutdown, reset and restore of CBS in the scope of application of this Part. These manuals/procedures shall be provided to the shipowner.

2.2.5.3.3.4 Operation phase:

.1 special survey.

Subject to modifications of CBS, the shipowner shall demonstrate to the Register fulfillment of requirements in 2.2.5.3.3.3 in accordance with the Ship Cyber Resilience Test Procedure.

General requirements for surveys in the operation phase are given in 2.3.3.

[1] The commissioning phase tests may be omitted if performed during the certification of CBS in accordance with 2.3.2.1.

2.3 DEMONSTRATION OF COMPLIANCE

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

Documentation to be submitted by suppliers to the Register for approval is specified in Section 3. The approved documentation shall be provided by the supplier to the systems integrator as specified in 3.5.2.

Documentation to be provided by the systems integrator is specified in 2.3.1 and 2.3.2.

Documentation to be provided by the shipowner is specified in 2.2.3.

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

documentation of CBS provided by the suppliers (refer to 3.5.2);

documentation produced by the systems integrator (refer to 2.3.1 and 2.3.2);

(Refer also to Appendices 1 and 2).

2.3.1 During design and construction phases.

The supplier shall demonstrate compliance with the requirements by the CBS certification according to 3.5.

The systems integrator shall demonstrate compliance with the requirements by submitting documents specified below to the Register.

During design and construction phases, all modifications to the design shall be carried out in accordance with the management of change (MoC) requirements (refer to 7.9.6.2.1, Part XV "Automation").

2.3.1.1 Zones and Conduit Diagram.

The content of this document is specified in 2.2.2.1.3.1.

2.3.1.2 Cyber Security Design Description (CSDD).

The content of this document is specified in subsections "Design phase" for each requirement in 2.2.

2.3.1.3 Ship Asset Inventory.

The content of this document is specified in 2.2.1.1.

2.3.1.4 Risk assessment for the exclusion of CBS.

The content of this document is specified in 2.4.

2.3.1.5 Description of compensating countermeasures.

If any CBS in the scope of application of this Part has been approved with compensating countermeasures in lieu of a requirement in Section 3, this document shall specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures (refer also to 3.2.1.3) requiring that the supplier describes such compensating countermeasures in the system documentation.

2.3.2 Upon ship commissioning.

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

submit updated design documentation to the Register as specified in 2.3.1;

submit to the Register the Ship Cyber Resilience Test Procedure describing how to demonstrate compliance with the requirements of this Part;

carry out testing, witnessed by the RS surveyor, in accordance with the approved Ship Cyber Resilience Test Procedure.

2.3.2.1 Ship Cyber Resilience Test Procedure:

.1 the content of this document is specified for the commissioning phase for each requirement in 2.2;

.2 the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS (refer to Section 3). Individual testing in the commissioning phase may be omitted if explicitly specified for the commissioning phase, on the condition that these security functions have been successfully tested during the certification of CBS in accordance with Section 3. Nevertheless, all tests shall be included in the Ship Cyber Resilience Test Procedure and the decision to omit tests shall be taken by the

Register. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements are met by compensating countermeasures, or due to other reasons such as modifications of CBS after the certification process;

.3 the Ship Cyber Resilience Test Procedure shall also specify how to test any compensating countermeasures described in 2.3.1.2;

.4 the Ship Cyber Resilience Test Procedure shall include means to update status and record findings during the testing, and specify the following information:

necessary test setup (to ensure the test can be repeated with the same expected result);

test equipment;

initial condition;

detailed test steps;

expected results and acceptance criteria;

.5 before submitting the Ship Cyber Resilience Test Procedure to the Register, the systems integrator shall verify that:

all the information is updated and all the amendments are introduced in accordance with the adopted procedures for change management (refer to 7.9.7.2, Part XV "Automation");

that the Ship Cyber Resilience Test Procedure is aligned with the latest configurations of CBS and networks connecting such systems together onboard the ship and to other CBS not onboard (e.g., ashore);

and that the tests are documented in such a manner as to allow verification of measures and means adopted for the fulfilment of relevant requirements of this Section on the final configuration of CBS and networks onboard;

.6 the systems integrator shall document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Ship Cyber Resilience Test Procedure;

.7 the cyber resilience testing shall be carried out on board after other commissioning activities for CBS are completed;

.8 the Register may request execution of additional tests.

2.3.3 During the operational life of the ship.

The shipowner shall manage technical and organizational security countermeasures listed in this Section.

Modifications to CBS in the scope of application of this Part shall be carried out in accordance with the management of change (MoC) requirements (refer to 7.9.7.12.1, Part XV "Automation"). This includes keeping documentation of CBS up to date.

The shipowner, with the support of suppliers, shall keep the Ship Cyber Resilience Test Procedure up to date and aligned with CBS onboard the ship and the networks connecting such systems to each other and to other CBS not onboard (e.g. ashore). The shipowner shall update the Ship Cyber Resilience Test Procedure considering the changes occurred on CBS and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship’s operational environment.

The shipowner shall prepare and implement operational procedures, provide periodic training and carry out drills for the ship crew and other concerned personnel ashore to familiarize them with CBS onboard the ship and the networks connecting such systems to each other and to other CBS not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.

The shipowner, with the support of suppliers, shall keep the measures and means adopted for the fulfilment of requirements of this Part up to date.

The shipowner shall retain onboard a copy of results of execution of tests and the updated Ship Cyber Resilience Test Procedure and make them available to the Register.

Change of shipowner shall require a new verification of the Ship Cyber Security and Resilience Program in the scope of the first annual survey.

2.3.3.1 First annual survey:

.1 before the first annual survey of the ship, the shipowner shall submit to the Register the Ship Cyber Security and Resilience Program documenting management of cyber security and cyber resilience of CBS in the scope of application of this Part;

.2 the Ship Cyber Security and Resilience Program shall include policies, procedures, plans and/or other information documenting the processes/activities specified for demonstration of compliance in 2.2;

.3 after the Register has approved the Ship Cyber Security and Resilience Program, the shipowner shall in the first annual survey demonstrate compliance by presenting records or other documented evidence of implementation of the processes described in the approved Ship Cyber Security and Resilience Program.

2.3.3.2 Subsequent annual surveys.

In the subsequent annual surveys of the ship, the shipowner shall upon request by the Register demonstrate entries or other documented evidences confirming implementation of the Ship Cyber Security and Resilience Program.

2.3.3.3 Special survey.

Upon renewal of the ship's classification certificate, the shipowner shall carry out testing witnessed by the RS surveyor in accordance with the Ship Cyber Resilience Test Procedure. Certain security safeguards shall be demonstrated at special survey whereas other need only be carried out in case of modifications to CBS as specified for operation phase in 2.2.

2.4 RISK ASSESSMENT FOR EXCLUSION OF CBS FROM THE APPLICATION OF REQUIREMENTS

2.4.1 Requirement.

A risk assessment shall be carried out in case any of CBS in the scope of application of this Part is excluded from the application of relevant requirements in Section 2. The risk assessment shall provide evidence of the acceptable risk level associated to the excluded CBS.

2.4.2 Requirement details:

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

.2 during the operational life of the ship, the shipowner shall update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in CBS. 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 CBS under examination above the acceptable risk threshold, the shipowner shall submit the updated risk assessment to the Register for review;

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

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

asset vulnerabilities;

threats, both internal and external;

potential impacts of cyber incidents affecting the asset on human safety, safety of the ship and/or threat to the environment;

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).

2.4.3 Acceptance criteria:

.1 exclusion of CBS in the scope of application of this Part from the application of relevant requirements may be accepted by the Register only if assurance is given that cyber risks have no impact on the safe operation of CBS. The said exclusion may be accepted by the Register for CBS, which does not fully meet the criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by the Register. The Register may also require submittal of additional documents to consider the said exclusion;

.2 the following additional criteria shall be met for the evaluation of risk level acceptability:

CBS shall be isolated (i.e. have no IP-network connections to other systems or networks);

CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled. It shall not be possible to connect unauthorized devices to CBS;

CBS shall be located in areas to which physical access is controlled;

CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of application of this Part (refer to 1.1);

.3 the following additional criteria shall be considered for the evaluation of risk level acceptability:

CBS shall not serve ship functions of category III;

known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting CBS have been duly considered in the risk assessment;

the attack surface for CBS is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points.

R a t i o n a l e . Exclusion of CBS in the scope of application of this Part from the application of relevant requirements needs to be duly justified and documented. Such exclusion may be accepted by the Register only if evidence is given that the risk level associated to the operation of CBS is under an acceptable threshold by means of specific risk assessment.

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

3 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT

3.1 SECURITY PHILOSOPHY

3.1.1 Systems and equipment.

3.1.1.1 A system can consist of group of hardware and software enabling safe, secure and reliable operation of a process (e.g., engine control system, DP system, etc.).

3.1.1.2 Equipment may be one of the following:

network devices (i.e. routers, managed switches);

security devices (i.e. firewall, intrusion detection system (IDS));

computers (i.e. workstation, servers);

automation devices (i.e. programmable logic controllers);

virtual machines cloud-hosted.

3.1.2 Cyber resilience.

The cyber resilience requirements given in 3.3, are applicable for all systems in the scope of application of this Part. Additional requirements related to interface with untrusted networks apply only for systems where such connectivity is designed.

3.1.3 Essential system availability.

3.1.3.1 Security measures for essential system shall not adversely affect the system operability.

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

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

3.1.4 Compensating countermeasures.

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

Compensating countermeasures shall meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each requirement and the related items in the standards, and follow the principles specified in 3.2.1.3.

3.2 DOCUMENTATION

3.2.1 CBS documentation.

The following documents shall be submitted for review and approval in accordance with the requirements in this Section (refer also to 3.5.2):

3.2.1.1 CBS Asset Inventory.

The CBS Asset Inventory shall include the following information:

.1 list of hardware components (e.g., host devices, embedded devices, network devices) indicating the following:

name;
brand/manufacturer;
model/type;
short description of functionality/purpose;
physical interfaces (e.g., network, serial);
name/type of system software (e.g., operating system, firmware);
version and patch level of system software;
supported communication protocols;

.2 list of software components (e.g., application software, utility software):

the hardware component where it is installed;
brand/manufacturer;
model/type;
short description of functionality/purpose;
version of software.

3.2.1.2 Topology diagrams:

.1 the physical topology diagram shall illustrate the physical architecture of the system. It shall be possible to identify the hardware components in the CBS Asset Inventory. The diagram shall illustrate:

all endpoints and network devices, including identification of redundant units;
communication cables (networks, serial links), including communication with I/O units;
communication cables to other networks or systems;

.2 the logical topology diagram shall illustrate the data flow between components in the system. The diagram shall illustrate the following:

communication endpoints (e.g. workstations, controllers, servers);
network devices (switches, routers, firewalls);
physical and virtual computers;
physical and virtual communication paths;
communication protocols;

.3 one combined topology diagram may be acceptable if all requested information can be clearly illustrated.

3.2.1.3 Description of security capabilities:

.1 this document shall describe how CBS with its hardware and software components meets the required security capabilities specified in 3.3.1;

.2 any network interfaces to other CBS in the scope of application of this Part shall be described. The description shall include destination CBS, data flows, and communication protocols. If the systems integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (refer to 2.2.2.1) shall be described in detail if delivered as part of CBS;

.3 any network interfaces to other systems or networks outside the scope of application of this Part (untrusted networks) shall be described. The description shall specify compliance with the additional security capabilities listed in 3.3.2, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (refer to 2.2.2.1) shall be described in detail if delivered as part of CBS;

.4 a separate chapter shall be designated for each requirement. All hardware and software components in the system shall be addressed in the description, as relevant;

.5 if any requirement is not fully met, this shall be specified in the description, and compensating countermeasures shall be proposed. The compensating countermeasures shall:

protect against the same threats as the original requirement;

provide an equal level of protection as the original requirement;

not be a security control that is required by other requirements in this Section;

not introduce higher security risks;

.6 any supporting documents (e.g. information about manufacturer) necessary to verify compliance with the requirements shall be referenced in the description.

3.2.1.4 Test Procedure of Security Capabilities:

.1 this document shall describe how to demonstrate by testing that the system complies with the requirements of 3.3.1 and 3.3.2, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be considered (where applicable);

.2 the Test Procedure of Security Capabilities shall include a separate chapter for each applicable requirement and contain the following information:

necessary test setup (to ensure the test can be repeated with the same expected result);

test equipment;

initial condition;

test methodology, detailed test steps;

expected results and acceptance criteria;

.3 the Test Procedure of Security Capabilities shall also include means to update test results and record findings during the testing.

3.2.1.5 Security Configuration Guidelines.

This document shall describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with the requirements of Section 2 and any specifications by the systems integrator (e.g. user accounts, authorization, password policies, safe state of machinery, firewall rules, etc.).

The document shall serve as basis for verification of item 29, Table 3.3.1.

3.2.1.6 Secure development lifecycle documents.

This documentation shall be submitted to the Register upon request and shall describe the supplier's processes and controls in accordance with requirements for secure development lifecycle specified in 3.4. Software updates and patching shall be described. The document shall prepare for survey in accordance with 3.5.3.4.

3.2.1.7 Plans for maintenance and verification of the CBS.

These documents shall be submitted to the Register upon request and shall include procedures for security-related maintenance and testing of the system. The documents shall include instructions for how the user can verify correct operation of the system's security functions as required by item 19, Table 3.3.1.

3.2.1.8 Information supporting the owner’s Incident Response Plan and Recovery Plan.

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

local independent control (refer to 2.2.4.2);

network isolation (refer to 2.2.4.3);

forensics by use of audit records (refer to item 13, Table 3.3.1);

deterministic output (refer to 2.2.4.4 and item 20, Table 3.3.1);

backup (refer to item 26, Table 3.3.1);

restore (refer to item 27, Table 3.3.1)**;**

controlled shutdown, reset, roll-back and restart (refer to 2.2.5.3).

3.2.1.9 Management of changes.

This document shall be submitted to the Register upon request. This document is not specific for cyber security and is also required in accordance with 7.9, Part XV "Automation".

3.2.1.10 Test reports.

CBS with the RS Type Approval Certificate covering the security capabilities of this Section may be exempted from survey. However, test reports signed by the supplier shall be submitted to the Register, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as shall otherwise be verified by the Register in survey (refer to 3.5.3).

3.3 SYSTEM REQUIREMENTS

The requirements in this Chapter are based on the requirements in IEC 62443-3-3 to be guided during design and manufacture of CBS.

3.3.1 Required security capabilities.

The following required security capabilities are given in Table 3.3.1.

Table 3.3.1

No.	Objective	Requirements
Protect against casual or coincidental access by unauthenticated entities		
1	Human user identification and authentication	CBS shall provide the capability to identify and authenticate all human users who can access the system directly or through interfaces. (Refer to IEC 62443-3-3:2013/SR 1.1)
2	Account management	CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts. (Refer to IEC 62443-3-3:2013/SR 1.3)
3	Identifier management	CBS shall provide the capability to support the management of identifiers by user, group and role. (Refer to IEC 62443-3-3:2013/SR 1.4)
4	Authenticator management	CBS shall provide the capability to: initialize authenticator content; change all default authenticators upon control system installation; change/refresh all authenticators; and protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (Refer to IEC 62443-3-3:2013/SR 1.5)
5	Wireless access management	CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. (Refer to IEC 62443-3-3:2013/SR 1.6)
6	Strength of password-based authentication	CBS shall provide the capability to enforce configurable password strength based on the minimum length and variety of character types. (Refer to IEC 62443-3-3:2013/SR 1.7)
7	Authenticator feedback	CBS shall obscure feedback during the authentication process. (Refer to IEC 62443-3-3:2013/SR 1.10)
Protect against casual or coincidental misuse		
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege. (Refer to IEC 62443-3-3:2013/SR 2.1)
9	Wireless use control	CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices. (Refer to IEC 62443-3-3:2013/SR 2.2)

No.	Objective	Requirements
10	Use control for portable and mobile devices	When CBS 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. N o t e . Port limits/blockers (including silicone) can be accepted for specific systems. (Refer to IEC 62443-3-3:2013/SR 2.3)
11	Mobile code	CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (Refer to IEC 62443-3-3:2013/SR 2.4)
12	Session lock	CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (Refer to IEC 62443-3-3:2013/SR 2.5)
13	Auditable events	CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (Refer to IEC 62443-3-3:2013/SR 2.8)
14	Audit storage capacity	CBS shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. Control system shall implement such auditing mechanisms as to reduce the likelihood of such capacity being exceeded. (Refer to IEC 62443-3-3:2013/SR 2.9)
15	Response to audit processing failures	CBS shall prevent loss of essential services and functions in the event of an audit processing failure. (Refer to IEC 62443-3-3:2013/SR 2.10)
16	Timestamps	CBS shall timestamp audit records. (Refer to IEC 62443-3-3:2013/SR 2.11)
Protect the integrity of CBS against casual or coincidental manipulation		
17	Communication integrity	CBS shall protect the integrity of transmitted information. N o t e . Cryptographic mechanisms shall be employed for wireless networks. (Refer to IEC 62443-3-3:2013/SR 3.1)
18	Malicious code protection	CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms. (Refer to IEC 62443-3-3:2013/SR 3.2)
19	Security functionality verification	CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance. (Refer to IEC 62443-3-3:2013/SR 3.3)

No.	Objective	Requirements
20	Deterministic output	CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state may be: unpowered state; last-known value; fixed value. (Refer to IEC 62443-3-3:2013/SR 3.6)
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure		
21	Information confidentiality	CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. N o t e . For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (Refer to IEC 62443-3-3:2013/SR 4.1)
22	Use of cryptography	If cryptography is used, CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (Refer to IEC 62443-3-3:2013/SR 4.3)
Monitor the operation of CBS and respond to incidents		
23	Audit log accessibility	CBS shall provide the capability for accessing audit log on read only basis by authorized humans and/or tools. (Refer to IEC 62443-3-3:2013/SR 6.1)
Ensure that the control system operates reliably under normal production conditions		
24	Denial of service protection	CBS shall provide the minimum capability to maintain essential functions during DoS events. N o t e . It is acceptable that CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner, which may cause hazardous situations. Overload-based DoS events shall be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed. (Refer to IEC 62443-3-3:2013/SR 7.1)
25	Resource management	CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (Refer to IEC 62443-3-3:2013/SR 7.2)
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by CBS without affecting normal operation. (Refer to IEC 62443-3-3:2013/SR 7.3)
27	System recovery and reconstitution	CBS shall provide the capability to be recovered and reconstructed to a known secure state after a disruption or failure. (Refer to IEC 62443-3-3:2013/SR 7.4)
28	Alternative power source	CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (Refer to IEC 62443-3-3:2013/SR 7.5)

No.	Objective	Requirements
29	Network and security configuration settings	CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. CBS shall provide an interface to the currently deployed network and security configuration settings. (Refer to IEC 62443-3-3:2013/SR 7.6)
30	Least functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by CBS: operating systems software components, processes and services; network services, ports, protocols, routes and hosts accesses and any software. (Refer to IEC 62443-3-3:2013/SR 7.7)

3.3.2 Additional security capabilities.

The following additional security capabilities are required for CBS with network communication to untrusted networks (i.e. interface to any networks outside the scope of this Part) according to Table 3.3.2.

CBS with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection specified in 2.2.2.1 and 2.2.2.2.

Table 3.3.2

No.	Objective	Requirements
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing CBS from or via untrusted network. (refer to IEC 62443-3-3:2013/SR 1.1, RE 2)
32	Software process and device identification and authentication	CBS shall identify and authenticate software processes and devices. (refer to IEC 62443-3-3:2013/SR 1.2)
33	Unsuccessful login attempts	CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (refer to IEC 62443-3-3:2013/SR 1.11)
34	System use notification	CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (refer to IEC 62443-3-3:2013/SR 1.12)
35	Access via untrusted networks	Any access to CBS from or via untrusted networks shall be monitored and controlled. (refer to IEC 62443-3-3:2013/SR 1.13)
36	Explicit access request approval	CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (refer to IEC 62443-3-3:2013/SR 1.13, RE1)
37	Remote session termination	CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (refer to IEC 62443-3-3:2013/SR 2.6)
38	Cryptographic integrity protection	CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (refer to IEC 62443-3-3:2013/SR 3.1, RE1)

No.	Objective	Requirements
39	Input validation	CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of CBS. (refer to IEC 62443-3-3:2013/SR 3.5)
40	Session integrity	CBS shall protect the integrity of sessions. Invalid session ID shall be rejected. (refer to IEC 62443-3-3:2013/SR 3.8)
41	Invalidation of session ID after session termination	The system shall invalidate session ID upon user logout or other session termination (including browser sessions). (refer to IEC 62443-3-3:2013/SR 3.8, RE1)

3.4 SECURE DEVELOPMENT LIFECYCLE REQUIREMENTS

A secure development lifecycle (SDLC) broadly addressing security aspects in following stages shall be followed for the development of systems or equipment:

requirement analysis phase;
design phase;
implementation phase;
verification phase;
release phase;
maintenance phase;
end of life phase.

A document that records how the security aspects have been addressed in above phases and at least that contains the description of the controlled processes as set out in 3.4.1 — 3.4.7 shall be produced and submitted to the Register for review and approval.

3.4.1 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 (refer to IEC 62443-4-1:2018/SM-8).

3.4.2 A process shall be employed to ensure that documentation about product security updates is made available to users (which can be through establishing a cyber security point of contact or periodic publications which can be accessed by the user) that includes but is not limited to (refer to IEC 62443-4-1:2018/SUM-2):

.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 instruction 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.

3.4.3 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 (refer to IEC 62443-4-1:2018/SUM-3):

.1 stating whether the product is compatible with the dependent component or operating system security update.

3.4.4 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 (refer to IEC 62443-4-1:2018/SUM-4).

The manufacturer shall have quality assurance (QA) process to test the updates before releasing.

3.4.5 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 (refer to IEC 62443-4-1:2018/SG-1):

.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.

3.4.6 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 shall be used (refer to IEC 62443-4-1:2018/SG-2).

3.4.7 A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product (refer to IEC 62443-4-1:2018/SG-3). 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 parameters in support of local security policies, and for each security parameter:

its contribution to the product's defence in depth strategy;

descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and

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.

3.5 DEMONSTRATION OF COMPLIANCE

3.5.1 Introduction.

Suppliers shall in cooperation with the systems integrator determine if the requirements of Section 3 are mandatory for CBS (refer to Fig. 3.5.1-1).

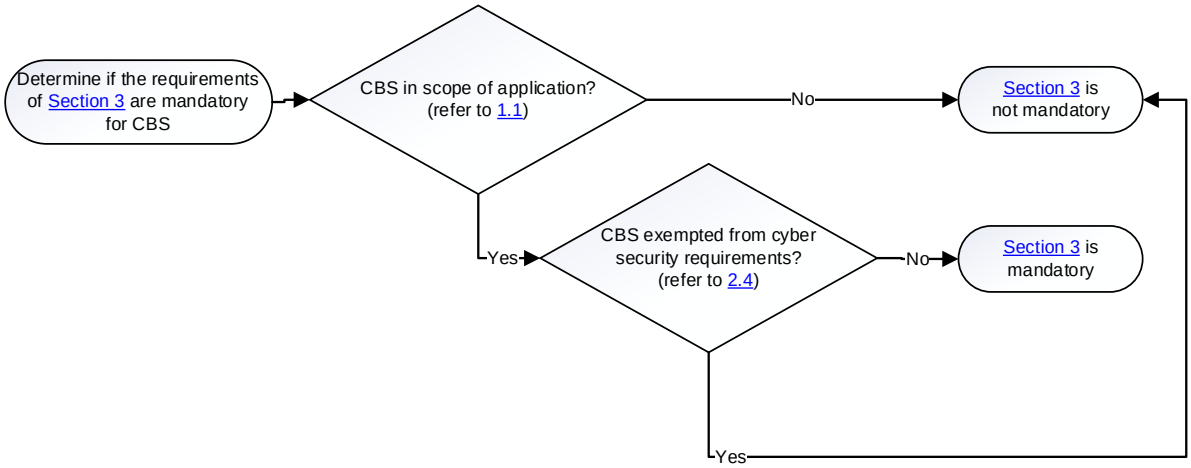

Fig. 3.5.1-1

Compliance with security requirements shall be demonstrated as indicated in Fig. 3.5.1-2. This classification process is ship-specific and shall result in the RS system certificate.

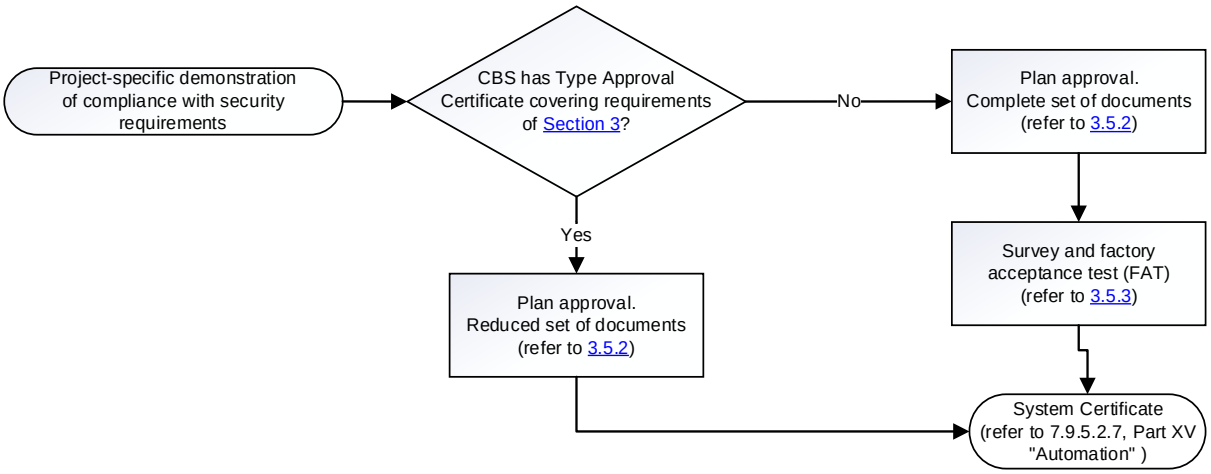

Fig. 3.5.1-2

Type approval is voluntary and applies for CBS that are standard and routinely manufactured. The requirements for the CBS certification and type approval are given in 7.9.5.2.4, Part XV "Automation".

The processes in Figs. 3.5.1-1 and 3.5.1-2 apply also if other equivalent standards are applied for navigation and radiocommunication equipment (refer to 1.1.5). In such case:

the process in Fig. 3.5.1-1 illustrates if the equivalent standard is mandatory (in lieu of Section 3);

the process in Fig. 3.5.1-2 illustrates that the certification process is lessened if CBS has been type approved in accordance with the equivalent standard.

3.5.2 Plan approval.

Plan approval is assessment of documents of CBS intended for a specific ship. The documents specified in 3.2 are required to be submitted by the supplier in order to verify compliance with requirements in this Section.

If CBS holds a valid RS Type Approval Certificate covering the requirements of this Section, the supplier may submit a reduced set of ship-specific documents to the Register (refer to Appendix 3).

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

3.5.3 Survey and factory acceptance test.

Survey and factory acceptance testing (FAT) is a ship-specific verification activity required for CBS that do not hold a valid RS Type Approval Certificate covering the requirements of this Section.

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

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

3.5.3.1 General survey items.

The supplier shall demonstrate that design, construction, and internal testing have been completed. It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with the CBS Asset Inventory (refer to 3.2.1.1) and the topology diagrams (refer to 3.2.1.2).

3.5.3.2 Test of security capabilities.

The supplier shall test the required security capabilities on the system to be delivered. The tests shall be carried out in accordance with the approved test procedure specified in 3.2.1.4 and be witnessed by the RS surveyor.

The tests shall demonstrate to the RS surveyor that all requirements are met. Testing of identical components is normally not required.

3.5.3.3 Correct configuration of security capabilities.

The supplier shall demonstrate for the RS surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines given in 3.2.1.5. This demonstration may be carried out in conjunction with testing of the security capabilities.

The security settings shall be documented in a report, e.g. a ship-specific instance of the configuration guidelines.

3.5.3.4 Secure development lifecycle.

The supplier shall, in accordance with documentation specified in 3.2.1.6, demonstrate compliance with requirements for secure development lifecycle given in 3.4.

3.5.3.4.1 Controls for private keys (refer to IEC 62443-4-1:2018/SM-8).

This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity.

The supplier shall present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access.

The policies and procedures shall address roles, responsibilities and work processes. The technical controls shall include e.g. physical access restrictions and cryptographic hardware (e.g. hardware security module) for storage of the private key.

3.5.3.4.2 Security update documentation (refer to IEC 62443-4-1:2018/SUM-2).

The supplier shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in 3.4.2.

3.5.3.4.3 Dependent component security update documentation (refer to IEC 62443-4-1:2018/SUM-3).

The supplier shall present management system documentation in compliance with the requirements of 3.4.3, substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information shall address how to manage risks related to not applying the updated acquired software.

3.5.3.4.4 Security update delivery (refer to IEC 62443-4-1:2018/SUM-4).

The supplier shall present management system documentation in compliance with the requirements of 3.4.4, substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.

3.5.3.4.5 Product defence in depth (refer to IEC 62443-4-1:2018/SG-1).

The supplier shall present management system documentation in compliance with the requirements of 3.4.5, substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in CBS during installation, maintenance and operation.

Examples of threats can be installation of unauthorized software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

3.5.3.4.6 Defence in depth measures expected in the environment (refer to IEC 62443-4-1:2018/SG-2).

The supplier shall present management system documentation in compliance with the requirements of 3.4.6, substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

3.5.3.4.7 Security hardening guidelines (refer to IEC 62443-4-1:2018/SG-3).

The supplier shall present management system documentation in compliance with the requirements of 3.4.7, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system. The guidelines shall specify how to reduce vulnerabilities in the system by removal/prohibiting/disabling of unnecessary software, accounts, services, etc.

APPENDIX 1

SUMMARY OF ACTIONS AND DOCUMENTS

Legend	
Submit	The stakeholder shall submit the document to the Register for verification and approval of compliance with requirements in Section 2.
Maintain	The stakeholder shall keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records shall by submitted to the Register in accordance with the requirements of 7.9, Part XV "Automation".
Demonstrate	The stakeholder shall demonstrate to the Register compliance with the requirements in accordance with the approved documents.

Document	Systems integrator			Shipowner			
	Design	Construction	Commissioning	Operation	1st annual survey	Annual survey	Special survey
Approved supplier documentation (refer to 2.3)		Maintain	Maintain	Maintain			
Zones and Conduit Diagram (refer to 2.3.1.1)	Submit	Maintain	Maintain	Maintain			
Cyber Security Design Description (refer to 2.3.1.2)	Submit	Maintain	Maintain	Maintain			
Ship Asset Inventory (refer to 2.3.1.3)	Submit	Maintain	Maintain	Maintain			
Risk assessment for the exclusion of CBS (refer to 2.3.1.4)[1]	Submit	Maintain	Maintain	Maintain			
Description of compensating countermeasures (refer to 2.3.1.5)[1]	Submit	Maintain	Maintain	Maintain			
Ship Cyber Resilience Test Procedure (refer to 2.3.2.1)		Submit	Demonstrate	Maintain			Demonstrate
Ship Cyber Security and Resilience Program (refer to 2.3.3.1): management of change (MoC) (refer to 2.2.1.1.3.4); management of software updates (refer to 2.2.1.1.3.4); management of firewalls (refer to 2.2.2.1.3.4); management of malware protection (refer to 2.2.2.3.3.4); management of access control (refer to 2.2.2.4.3.4); management of confidential information (refer to 2.2.2.4.3.4); management of remote access (refer to 2.2.2.6.3.4); management of mobile and portable devices (refer to 2.2.2.7.3.4); detection of security anomalies (refer to 2.2.3.1.3.4); verification of security functions (refer to 2.2.3.2.3.4); Incident Response Plan (refer to 2.2.4.1.3.4); Recovery Plan (refer to 2.2.5.1.3.4)				Maintain	Submit	Demonstrate	

[1] If applicable.

APPENDIX 2

SUMMARY OF REQUIREMENTS AND DOCUMENTS

Ship Asset Inventory (refer to 2.2.1.1)		
CBS security capabilities	Documentation of product security updates	Refer to 3.4.2
	Documentation of dependent component security updates	Refer to 3.4.3
	Provision of security updates	Refer to 3.5.3.4.4
CBS documentation	CBS Asset Inventory	Refer to 3.2.1.1
	Management of change plan	Refer to 3.2.1.9
Ship design documentation	Ship Asset Inventory	Refer to 2.2.1.1.3.1
Ship Cyber Security and Resilience Program	Management of change	Refer to 2.2.1.1.3.4
	Management of software updates	Refer to 2.2.1.1.3.4

Security zones and network segmentation (refer to 2.2.2.1)		
CBS security capabilities		
CBS documentation	Topology diagrams	Refer to 3.2.1.2
Ship design documentation	Zones and Conduit Diagram	Refer to 2.2.2.1.3.1
	Description of cyber resilience activities	Refer to 2.2.2.1.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.1.3.3
Ship Cyber Security and Resilience Program	Management of security zone boundary devices (e.g., firewalls)	Refer to 2.2.2.1.3.4

Network protection safeguards (refer to 2.2.2.2)		
CBS security capabilities	Denial of service (DoS) protection	Refer to item 29, Table 3.3.1
	Deterministic output	Refer to item 20, Table 3.3.1
CBS documentation	Description of security facilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Ship Cyber Resilience Test Procedures	Refer to 2.2.2.2.3.3
Ship Cyber Security and Resilience Program		

Antivirus, antimalware, antispam and other protections from malicious code (refer to 2.2.2.3)		
CBS security capabilities	Malicious code protection	Refer to item 18, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Cyber Security Design Description	Refer to 2.2.2.3.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.3.3.3
Ship Cyber Security and Resilience Program	Management of malware protection	Refer to 2.2.2.3.3.4

Access control (refer to 2.2.2.4)		
CBS security capabilities	Human user identification and authorization	Refer to item 1, Table 3.3.1
	Account management	Refer to item 2, Table 3.3.1
	Identifier management	Refer to item 3, Table 3.3.1
	Authenticator management	Refer to item 4, Table 3.3.1
	Authorization enforcement	Refer to item 8, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Cyber Security Design Description	Refer to 2.2.2.4.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.4.3.3
Ship Cyber Security and Resilience Program	Management of confidential information	Refer to 2.2.2.4.3.4
	Management of logical and physical access	Refer to 2.2.2.4.3.4

Wireless communication (refer to 2.2.2.5)		
CBS security capabilities	Wireless access management	Refer to item 5, Table 3.3.1
	Wireless use control	Refer to item 9, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Cyber Security Design Description	Refer to 2.2.2.5.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.5.3.3
Ship Cyber Security and Resilience Program		

Remote access control and communication with untrusted networks (refer to 2.2.2.6)		
CBS security capabilities	Multifactor authentication	Refer to item 31, Table 3.3.2
	Process/device identification and authorization	Refer to item 32, Table 3.3.2
	Unsuccessful login attempts	Refer to item 33, Table 3.3.2
	System use notification	Refer to item 34, Table 3.3.2
	Access via untrusted networks	Refer to item 35, Table 3.3.2
	Explicit access request approval	Refer to item 36, Table 3.3.2
	Remote session termination	Refer to item 37, Table 3.3.2
	Cryptographic integrity protection	Refer to item 38, Table 3.3.2
	Input validation	Refer to item 39, Table 3.3.2
	Session integrity	Refer to item 40, Table 3.3.2
	Invalidation of session ID	Refer to item 41, Table 3.3.2
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Cyber Security Design Description	Refer to 2.2.2.6.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.6.3.3
Ship Cyber Security and Resilience Program	Management of remote access and communication with/via untrusted networks	Refer to 2.2.2.6.3.4

Use of mobile and portable devices (refer to 2.2.2.7)		
CBS security capabilities	Use control for portable devices	Refer to item 10, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Cyber Security Design Description	Refer to 2.2.2.7.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.2.7.3.3
Ship Cyber Security and Resilience Program	Management of mobile and portable devices	Refer to 2.2.2.7.3.4

Network operation monitoring (refer to 2.2.3.1)		
CBS security capabilities	Use control for mobile and portable devices	Refer to item 10, Table 3.3.1
	Auditable events	Refer to item 13, Table 3.3.1
	Denial of service (DoS) protection	Refer to item 24, Table 3.3.1
	Alarm excessive bandwidth use	Refer to 7.9.8.2.1.5, Part XV "Automation"
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
Ship design documentation	Ship Cyber Resilience Test Procedure	Refer to 2.2.3.1.3.3
Ship Cyber Security and Resilience Program	Incident Response Plan	Refer to 2.2.3.1.3.4

Verification and diagnostic functions of CBS and networks (refer to 2.2.3.2)		
CBS security capabilities	Security function verification	Refer to item 19, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Plans for CBS maintenance and verification	Refer to 3.2.1.7
Ship design documentation	Ship cyber resilience and verification	Refer to 2.2.3.2.3.3
Ship Cyber Security and Resilience Program	Verification of security functions	Refer to 2.2.3.2.3.4

Incident response plan (refer to 2.2.4.1)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.4.1.3.1
Ship Cyber Security and Resilience Program	Incident Response Plan	Refer to 2.2.4.1.3.4

Local independent and/or manual operation (refer to 2.2.4.2)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting incident response and recovery plans	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.4.2.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.4.2.3.3
Ship Cyber Security and Resilience Program	Incident Response Plan	Refer to 2.2.4.1.3.4

Network isolation (refer to 2.2.4.3)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.4.3.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.4.3.3.3
Ship Cyber Security and Resilience Program	Incident Response Plan	Refer to 2.2.4.1.3.4

Fallback to a minimal risk condition (refer to 2.2.4.4)		
CBS security capabilities	Deterministic output	Refer to item 20, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.4.4.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.4.4.3.3
Ship Cyber Security and Resilience Program	Incident Response Plan	Refer to 2.2.4.1.3.4

Recovery Plan (refer to 2.2.5.1)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.5.1.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.5.1.3.3
Ship Cyber Security and Resilience Program	Recovery Plan	Refer to 2.2.5.1.3.4

Backup and restore capability (refer to 2.2.5.2)		
CBS security capabilities	System backup	Refer to item 26, Table 3.3.1
	System recovery and reconstitution	Refer to item 27, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Ship Cyber Resilience Procedure	Refer to 2.2.5.2.3.3
Ship Cyber Security and Resilience Program	Recovery Plan	Refer to 2.2.5.1.3.4

Controlled shutdown, reset, restore and restart (refer to 2.2.5.3)		
CBS security capabilities	System recovery and reconstitution	Refer to item 27, Table 3.3.1
CBS documentation	Description of security capabilities	Refer to 3.2.1.3
	Test procedure for security capabilities	Refer to 3.2.1.4
	Information supporting Incident Response Plan and Recovery Plan	Refer to 3.2.1.8
Ship design documentation	Cyber Security Design Description	Refer to 2.2.5.3.3.1
	Ship Cyber Resilience Test Procedure	Refer to 2.2.5.3.3.3
Ship Cyber Security and Resilience Program	Recovery Plan	Refer to 2.2.5.1.3.4

Risk assessment for exclusion of CBS from the application of requirements (refer to 2.4)		
CBS security capabilities		
CBS documentation		
Ship design documentation	Risk assessment for the exclusion of CBS	Refer to 2.3.1.4
Ship Cyber Security and Resilience Program		

APPENDIX 3

SUMMARY ON DOCUMENTS THAT THE SUPPLIER SHALL SUBMIT TO THE REGISTER

Document	Requirements	Register
CBS Asset Inventory (refer to 3.2.1.1)	To be incorporated in Ship Asset Inventory (refer to 2.2.1.1)	Approval[1, 2]
Topology diagrams (refer to 3.2.1.2)	Enabling systems integrator to design security zones and conduits (refer to 2.2.2.1)	Approval[1, 2]
Description of security capabilities (refer to 3.2.1.3)	Required security capabilities (refer to 3.3.1)	Approval[1]
	Additional security capabilities, if applicable (refer to 3.3.2)	
Test procedures for security capabilities (refer to 3.2.1.4)	Required security capabilities (refer to 3.3.1)	Approval[1]
	Additional security capabilities, if applicable (refer to 3.3.2)	
Security configuration guidelines (refer to 3.2.1.5)	Network and security configuration settings (refer to item 29, Table 3.3.1)	For information[1]
Secure development lifecycle (refer to 3.2.1.6)	SDLC requirements (refer to 3.4)	Approval[1]
Plans for maintenance and verification (refer to 3.2.1.7)	Security functionality verification (refer to item 19, Table 3.3.1)	For information[1]
Information supporting Incident Response Plan and Recovery Plan (refer to 3.2.1.8)	Auditable events (refer to item 13, Table 3.3.1)	For information[1]
	Deterministic output (refer to item 20, Table 3.3.1)	For information[1]
	System backup (refer to item 26, Table 3.3.1)	For information[1]
	System recovery and reconstitution (refer to item 27, Table 3.3.1)	For information[1]
Management of change plan (refer to 3.2.1.9)	Management of change process (refer to 7.9.7, Part XV "Automation")	For information[1]
Test reports (refer to 3.2.1.10)	Configuration of security capabilities and hardening (refer to 3.2.1.5 and 3.4.7)	For information[2]

[1] Required for CBS without the Type Approval Certificate confirming compliance of security capabilities with the requirements of Section 3.

[2] Required for CBS with the Type Approval Certificate confirming compliance of security capabilities with the requirements of Section 3.

Russian Maritime Register of Shipping

Rules for the Classification and Construction of Sea-Going Ships
Part XXI
Cyber Resilience

FAI "Russian Maritime Register of Shipping"
7, Litera A, Millionnaya Ulitsa,
St. Petersburg, 191181
Russian Federation
www.rs-class.org/en/