Draft of the Guidance for Cyber Resilience of Ships and Systems

(Development Review : For external opinion inquiry)

2024. 2.

Machinery Rule Development Team

2024

Guidance for Cyber Resilience of Ships and Systems

KR

2024

Guidance for Cyber Resilience of Ships and Systems

KR

APPLICATION OF "GUIDANCE FOR CYBER RESILIENCE OF SHIPS AND SYSTEMS"

1. Unless expressly specified otherwise, the requirements in the Guidance apply to ships and systems for which contracts for construction are signed on or after 1 July 2024.

CONTENTS

CHAPTER 1   General

Section 1   General

101. Aim and purpose

1. The aim of this Guidance is to provide a minimum set of requirements for Cyber Resilience of ships, with the purpose of providing technical means to stakeholders which would lead to cyber resilient ships.

2. This Guidance targets the ship as a collective entity for Cyber Resilience and is intended as a base for the complementary application of other industry standards addressing Cyber Resilience of on-board systems, equipment and components.

3. Minimum requirements for Cyber Resilience of on-board systems and equipment are given in **Ch 3**.

102. Application

1. The requirements of this Guidance shall apply to the ships intended to be registered and maintained under this Society in accordance with **Pt 1** of Rules of the Classification of Steel Ships(hereafter referred to as the Class Rules).

2. The minimum requirements for Cyber Resilience in **Ch 2** of this Guidance shall apply to ships requiring the Classification Survey during Construction.

3. The minimum requirements for Cyber Resilience in **Ch 3** of this Guidance shall apply to on-board systems and equipment in the ship subject to **Ch 2**.

4. The additional requirements in **Ch 4** of this Guidance shall apply to the cyber security management system of ships upon the request of the shipowner.

5. The relevant requirements in **Pt 6, Ch 2 of the Class Rules** in addition to the requirements in this Guidance shall be satisfied.

6. The cyber incidents considered in this Guidance are events resulting from any offensive manoeuvre that targets the operational technology (OT) systems onboard ships as defined in **Sec 2**.

7. Items not specified in this Guidance shall satisfy the relevant requirements in the Class Rules.

103. Scope of applicability

1. Vessels in scope
 (1) Passenger ships (including passenger high-speed craft) engaged in international voyages
 (2) Cargo ships of 500 GT and upwards engaged in international voyages
 (3) High speed craft of 500 GT and upwards engaged in international voyages
 (4) Mobile offshore drilling units of 500 GT and upwards
 (5) Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc)
 (Note) This Guidance may be used as non-mandatory guidance to the following.
   1) Ships of war, troopships and naval vessel
   2) Cargo ships less than 500 GT
   3) Vessels not propelled by mechanical means
   4) Wooden ships of primitive build
   5) Passenger yachts (passengers not more than 12)
   6) Pleasure yachts not engaged in trade

7) Fishing vessels

8) Site specific offshore installations (i.e. FPSOs, FSUs, etc.)

2. Systems in scope

(1) Operational Technology (OT) systems onboard ships, i.e. those computer based systems (hereafter referred to as CBS) using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

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

(A) Propulsion

(B) Steering

(C) Anchoring and mooring

(D) Electrical power generation and distribution

(E) Fire detection and extinguishing systems

(F) Bilge and ballast systems, loading computer

(G) Watertight integrity and flooding detection

(H) Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)

(I) Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)

(2) Navigation and communication system

(A) Navigational systems required by statutory regulations

(B) Internal and external communication systems required by the Class Rules and statutory regulations

(3) Any Internet Protocol (IP)-based communication interface from CBSs in scope of this UR to other systems.

(Note) Examples of such systems are, but not limited to, the following:

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)

3. Exclusion of a system from the application

A CBS may be excluded from the application scope of this Guidance on condition that a risk assessment is performed for the CBS in accordance with **Sec 3** and it verified by this Society that it is found to meet the acceptance criteria of **304**.

104. Class notations

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

1. **Cyber Resilience**: ships having Cyber Resilience throughout the ships' lifecycle in accordance with the relevant requirements in **Ch 2**.

2. **Cyber Resilience(Managed)**: Ships implementing cyber security management system based on cyber risk management process in accordance with the additional requirements in **Ch 4** in addition to the requirements in **Ch 2**.

105. System Category

System categories are defined in **Pt 6, Ch 2, Sec 4** of the Class Rules on the basis of the

consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.

106. Equivalence

For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in **Ch 3, Sec 4** may be accepted by this Society, on the condition that requirements in UR **Ch 2** are complied with.

107. Reference

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

1. **IACS UR E22 Rev.3**: Computer-based systems

2. **IACS UR E26 Rev.1**: Cyber resilience of ships

3. **IACS UR E27 Rev.1**: Cyber resilience of on-board systems and equipment

4. **IACS Rec.166**: Cyber resilience

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

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

Section 2 Definitions and abbreviation

201. Definitions

1. **Annual survey**: See **Pt 1, Ch 2, Sec 2** of the Class Rules

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

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

4. **Availability**: property of ensuring timely and reliable access to and use of control system information and functionality

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

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

7. **Conduit**: Logical grouping of communication channels, connecting two or more zones, that share common security requirements

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

9. **Confidentiality**: Property of preserving authorized restrictions on information access and disclosure.

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

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

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

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

14. **Essential services**: Services for propulsion and steering, and safety of the ship. Essential services comprise "Primary Essential Services" and "Secondary Essential Services": Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering; Secondary Essential Services are those services which need not necessarily be in

continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

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

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

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

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

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

20. **Integrity**: Property of protecting the accuracy and completeness of assets.

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

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

23. **Network segment**: In the context of this Guidance, a network segment is an OSI layer-2 Ethernet segment (a broadcast domain).
(Note) TCP/IP: Network address plan is prefixed by their IP addresses and the network mask. Communication between network segments is only possible by the use of routing service at network layer (OSI Layer 3).

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

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

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

27. **OT system**: Computer based systems, which provide control, alarm, monitoring, safety or internal communication functions.

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

29. **Physical network segment**: The same as "Network segment", but where physical components are not shared by other network segments.

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

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

32. **Security zone**: A collection of CBSs in the scope of applicability of this Guidance 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.

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

34. **Special survey:** See **Pt 1, Ch 2, Sec 4** of the Class Rules.

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

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

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

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

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

202. Abbreviation

1. **AS:** Annual Survey

2. **ACL:** Access Control List

3. **CBS:** Computer Based System

4. **COTS:** Commercial-Off-The-Shelf

5. **DoS:** Denial of Service

6. **HMI:** Human-Machine Interface

7. **IDS:** Intrusion Detection System

8. **IPS:** Intrusion Prevention System

9. **IT:** Information Technology

10. **MoC:** Management of Change

11. **OT:** Operational Technology

12. **TCP/IP:** Transmission Control Protocol/Internet Protocol

13. **SDLC:** Secure Development Life-Cycle

14. **SS:** Special Survey

Section 3 Risk assessment for exclusion of CBS from the application of requirements

301. Requirement

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

302. Rationale

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

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

303. Requirement details

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

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

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

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

5. Emerging risks related to the specific configuration of the CBS under examination shall be also identified. In the risk assessment, the following elements shall be considered:
   (1) Asset vulnerabilities;
   (2) Threats, both internal and external;
   (3) Potential impacts of cyber incidents affecting the asset on human safety, safety of the vessel and/or threat to the environment;
   (4) Possible effects related to integration of systems, or interfaces among systems, including systems not onboard (e.g. if remote access to onboard systems is provided).

304. Acceptance criteria

1. Exclusion of a CBS falling under the scope of applicability of this Guidance from the application of relevant requirements can be accepted by this Society only if assurance is given that the operation

of the CBS has no impact on the safety of operations regarding cyber risk.

2. The said exclusion may be accepted for a CBS which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by this Society. This Society may also require submittal of additional documents to consider the said exclusion.

3. The following criteria shall be met to exclude a system from the scope of applicability of this Guidance.
    (1) The CBS shall be isolated. (i.e, have no IP-network connections to other systems or networks)
    (2) The CBS shall have no accessible physical interface ports. Unused interfaces shall be logically disabled. It shall not be possible to connect unauthorised devices to the CBS.
    (3) The CBS must be located in areas to which physical access is controlled.
    (4) The CBS shall not be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Guidance. (see **103**)

4. The following additional criteria should be considered for the evaluation of risk level acceptability:
    (1) The CBS should not serve ship functions of category III.
    (2) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the CBS have been duly considered in the risk assessment.
    (3) The attack surface for the CBS is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points.

CHAPTER 2   Cyber Resilience of Ships

Section 1   General

101. Introduction

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

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

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

4. It is considered that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

102. Application

1. The requirements of this Chapter apply to ships in the application scope according to **Ch 1, 103. 1** during the ship's entire life cycle.

2. On-board systems and equipment in the application scope of this Chapter shall meet the minimum requirements of **Ch 3** in addition to this Chapter.

3. Unless expressly specified otherwise, CBS and network referred to in this Chapter mean the CBS and network in the application scope of the Guidance according to **Ch 1, 103. 2**.

Section 2 Classification Survey

201. General

The classification survey shall be carried out by this Society by assessment of documentation and survey in the relevant phases as specified in this Section.

1. Documentation to be submitted

(1) Documentation to be submitted by suppliers to this Society is specified in **Ch 3**. The approved versions of this documentation shall also be provided by the suppliers to the systems integrator as specified in **Ch 3, 202. 3**. (see **Table 3.2.1**)

(2) Documents to be provided by the systems integrator are listed in **202. 1** and **202. 2**. (see **Table 2.2.1**)

(3) Documents to be provided by the shipowner are listed in **203. 1** (see **Table 2.2.1**)

2. Provision documentation to a shipowner

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

(1) Documentation of the CBSs provided by the suppliers (see **Ch 3 202**)

(2) Documentation produced by the systems integrator (see **202. 1**, **202. 2** and **Table 2.2.1**)

Table 2.2.1 Summary of actions and documents

Document	Ref.	Systems integrator			Shipowner			
		Design	Cons.	Onboard Test	Oper.	1st AS	AS	SS
Approved supplier documentation	Ch 3, 201		M	M	M			
Zones and conduit diagram	202.1 (1)	A	M	M	M			
Cyber security design description	202.1 (1)	A	M	M	M			
Vessel asset inventory	202.1 (1)	A	M	M	M			
Risk assessment for the exclusion of CBS[1]	202.1 (1)	A	M	M	M			
Description of compensating countermeasures[1]	202.1 (1)	A	M	M	M			
Ship Cyber Resilience test procedure	202.2 (2)		A	S	M			S
Ship cyber security and resilience program	203.2 (1)							
– Management of change (MoC)	401.1 (5)							
– Management of software updates	401.1 (5)							
– Management of firewalls	402.1 (5)							
– Management of malware protection	402.3 (5)							
– Management of access control	402.4 (5)							
– Management of confidential information	402.4 (5)				M	A & S	S	
– Management of remote access	402.6 (5)							
– Management of mobile and portable devices	402.7 (5)							
– Detection of security anomalies	403.1 (5)							
– Verification of security functions	403.2 (5)							
– Incident response plans	404.1 (5)							
– Recovery plans	405.1 (5)							

1. [1] If applicable
2. A (Approval): The stakeholder shall submit the document to this Society for verification and approval of compliance with requirements in this Chapter.
3. M (Maintain): The stakeholder shall keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records shall be submitted to

the Class society as per **Pt 6, Ch 2, Sec 4** of the Class Rules.
4. S (Survey): The stakeholder shall demonstrate compliance to the this Society in accordance with the approved document.

3. **Kinds of surveys**

Kinds of surveys for the Cyber Resilience of ships are as follows:

(1) Classification Survey during Construction (hereafter referred to as "Classification Survey")

Classification Survey is carried out when there is the application for Classification Survey under construction, and includes document approval and on-board test during the following phases:

(A) Design phase

(B) Construction phase

(C) On-board test phase

(2) Survey for maintaining Classification (hereafter referred to as "Classification Maintenance Survey")

Classification Maintenance Survey shall be carried out to maintain classification after delivery of a ship, and includes the following surveys:

(A) Annual Surveys

(a) 1st Annual Survey

1st annual survey shall be carried out at intervals specified in **Pt 1, Ch 2, Sec 2**.

(b) Subsequent Surveys

Subsequent Surveys shall be carried from at 2nd Annual Survey to at 4th Annual Survey at intervals specified in **Pt 1, Ch 2, Sec 2**.

(B) Special Surveys

Special Surveys shall be carried out at intervals specified in **Pt 1, Ch 2, Sec 4**.

(C) Occasional Surveys

Occasional Surveys shall be carried out at intervals specified in **Pt 1, Ch 2, Sec 10**.

202. **Classification Survey**

1. **During Design and Construction phase**

(1) Approval Documents and data

(A) Zone and conduit diagram

The content of this document is specified in **402. 1** (4) (A).

(B) Cyber security design description (CSDD)

The content of this document is specified in subsections "Design phase" for each requirement in **Sec 4**.

(C) Vessel asset inventory

The content of this document is specified in **401. 1**.

(D) Risk assessment for the exclusion of CBSs

The content of this document is specified in **Ch 1, Sec 3**.

(E) Description of compensating countermeasures

If any CBS has been approved with compensating countermeasures in lieu of a requirement in **Ch 3**, this document shall specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also **Ch 3, 301. 3** requiring that the supplier describes such compensating countermeasures in the system documentation.

(2) The supplier shall demonstrate compliance to this Society by following the certification process specified in **Ch 3, Sec 2**.

(3) The systems integrator shall demonstrate compliance by submitting documents in the above (1) to this Society for assessment.

(4) During the design and construction phases, modifications to the design shall be carried out in accordance with the management of change (MoC) requirements in **Pt 6, Ch 2, Sec 4** of the Class Rules.

2. On-board Test

(1) Before final on-board testing of the ship, the systems integrator shall:
   (A) Submit updated design documentation to this Society (as-built versions of the documents in **202.1 (1)**)
   (B) Submit ship cyber resilience test procedure to this Society describing how to demonstrate compliance with this Chapter by testing and/or analytic evaluation.
   (C) Carry out testing, witnessed by this Society, in accordance with the approved ship cyber resilience test procedure.

(2) Ship cyber resilience test procedure
   (A) The content of this document is specified for the On-board test phase in each subsection "Classification Survey" in **Sec 4**.
   (B) On-board test of CBSs
      (a) For each CBS, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS. (see **Ch 3**)
      (b) Testing of such security functions may be omitted if specified in the respective subsection "on-board test phase", on the condition that these security functions have been successfully tested during the certification of the CBS as per **Ch 3**.
      (c) Nevertheless, all tests shall be included in the ship cyber resilience test procedure and the decision to omit tests will be taken by this Society.
      (d) Tests may generally not be omitted if findings/comments are carried over from the certification process to the on-board test phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the CBS after the certification process.
   (C) The ship cyber resilience test procedure shall also specify how to test any compensating countermeasures described in **202. 1 (1) (E)**.
   (D) The Ship cyber resilience test procedure shall include means to update status and record findings during the testing, and specify the following information:
      (a) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
      (b) Test equipment
      (c) Initial condition(s)
      (d) Test methodology, detailed test steps
      (e) Expected results and acceptance criteria
   (E) Before submitting the Ship cyber resilience test procedure to this Society, the systems integrator shall verify that the information is updated and placed under change management;
      (a) It is aligned with the latest configurations of CBSs and networks connecting such systems together onboard the ship and to other CBSs not onboard (e.g., ashore).
      (b) The tests documented are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of CBSs and networks onboard.
   (F) The systems integrator shall document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Ship cyber resilience test

procedure.

(G) The testing shall be carried out on board in accordance with the approved Ship cyber resilience test procedure after other commissioning activities for the CBSs are completed.

(H) This Society may request the execution of additional tests if deemed necessary.

203. Classification Maintenance Survey

1. General

(1) After the ship has been delivered to the shipowner, the shipowner shall manage technical and organisational security countermeasures by establishing and implementing processes as specified in this Chapter.

(2) Modifications to the CBS shall be carried out in accordance with the management of change (MoC) requirements in **Pt 6, Ch 2, Sec 4** of the Class Rules. This includes keeping documentation of the CBSs up to date.

(3) The shipowner, with the support of suppliers, shall keep the Ship cyber resilience test procedure up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore). The shipowner shall update the Ship cyber resilience test procedure considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment.

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

(5) The shipowner, with the support of supplier, shall keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of CBSs onboard the ship and the networks connecting such systems.

(6) The shipowner shall retain onboard a copy of results of execution of tests and an updated Ship cyber resilience test procedure and make them available to this Society.

2. Annual survey

(1) First Annual Survey

(A) In due time(6 months in advance of the initial annual survey as possible) before the first Annual Survey of the ship, the shipowner shall submit to this Society a Ship cyber security and resilience program documenting management of cyber security and cyber resilience of the CBSs.

(B) The Ship cyber security and resilience program shall include policies, procedures, plans and/or other information documenting the processes/activities specified in subsections "Classification Maintenance Survey" in **Sec 4**.

(C) After this Society has approved the Ship cyber security and resilience program, the shipowner shall in the first annual survey demonstrate compliance by presenting records or other documented evidence of implementation of the processes described in the approved Ship cyber security and resilience program.

(D) When the vessel management company is changed, additional approval of the Ship cyber security and resilience program may be requested by this Society if deemed necessary.

(2) Subsequent Annual Surveys

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

3. Special survey

Upon renewal of the ship's classification certificate, the shipowner shall carry out testing witnessed by this Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards shall be demonstrated at Special survey whereas other need only be carried out upon request by this Society based on modifications to the CBSs as specified in subsections "Classification Maintenance Survey" in **Sec 4**.

Section 3 Goals and organization of requirements

301. Primary goal

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

2. Safe and secure shipping can be achieved through effective cyber risk management system. To support safe and secure shipping resilient to cyber risk, the following sub-goals for the management of cyber risk are defined in the five functional elements listed in **302**.

302. Sub-goals per functional element

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

Table 2.3.1 Sub-goals per functional element

No.	Functional element	Goal	Content
1	Identify	The requirements for the 'Identify' functional element are aimed at identifying: 1) The CBSs onboard, their interdependencies and the relevant information flows; 2) The key resources involved in their management, operation and governance, their roles and responsibilities.	Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.
2	Protect	The requirements for the Protect functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential incident.	Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.
3	Detect	The requirements for the Detect functional element are aimed at the development and implementation of appropriate means supporting the ability to reveal and recognize anomalous activity on CBSs and networks onboard and identify cyber incidents.	Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.
4	Respond	The requirements for the Respond functional element are aimed at the development and implementation of appropriate means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of CBSs and networks onboard.	Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.
5	Recover	The requirements for the Recover functional element are aimed at the development and implementation of appropriate means supporting the ability to restore CBSs and networks onboard affected by cyber incidents.	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.

303. Organization of requirements

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

2. For each requirement, a rationale is given.

3. A summary of actions to be carried out and documentation to be made available is also given in **Table 2.2.1** for each phase of the ship's life and relevant stakeholders participating to such phase.

4. **Sec 4** contains the requirements to be satisfied in order to achieve the primary goal defined in **301**, organized according to the five functional elements identified in **302**.

304. Stakeholders

1. The requirements shall be fulfilled by the stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified (see also **Ch 1, Sec 2** for definitions):
   (1) Shipowner/Company
   (2) Systems integrator
   (3) Supplier
   (4) This Classification Society

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

Section 4 Requirements for Cyber Resilience of ships

401. Identify

1. Vessel asset inventory

(1) Requirement

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

(2) Requirement details

(A) The vessel asset inventory shall include at least the CBSs indicated in **Ch 1, 103. 2**, if present onboard.

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

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

(D) Hardware

For all hardware devices, the vessel asset inventory shall include at least the information in **Ch 3, 301. 1**. In addition, the vessel asset inventory may specify system category and security zone associated with the CBS.

(E) Software

(a) For all software(e.g., application program, operating system, firmware), the vessel asset inventory shall include at least the information in **Ch 3, 301. 1**.

(b) The software of the CBSs shall be maintained and updated in accordance with the shipowner's process for management of software maintenance and update policy in the Ship cyber security and resilience program, see **203**.

(3) Rationale

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

(4) Classification Survey

(A) Design phase

(a) The systems integrator shall submit vessel asset inventory to this Society. (refer to **202. 1** (1))

(b) The vessel asset inventory shall incorporate the asset inventories of all individual CBSs. Any equipment delivered by the systems integrator shall also be included in the vessel asset inventory.

(B) Construction phase

The systems integrator shall keep the vessel asset inventory updated.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure(refer to **202. 2** (2) and demonstrate to this Society that:

Vessel asset inventory is updated and completed at delivery

CBSs are correctly represented by the vessel asset inventory

Software of the CBSs has been kept updated, e.g. by vulnerability scanning or by

checking the software versions of CBSs while switched on.

(5) Classification Maintenance Survey

    (A) General

        (a) For general requirements to surveys in the operation phase, see **203**.

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

          Management of change (**203. 1**)

          Hardware and software modifications (**401.1 (2)**)

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

          Vulnerabilities and cyber risks (**401. 1 (2)** and **401. 1 (3)**)

          Security patching (**402. 6 (2) (E)**)

    (B) First annual survey

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

        (a) The approved management of change process has been adhered to.

        (b) Known vulnerabilities and functional dependencies have been considered for the software in the CBSs.

        (c) The Vessel asset inventory has been kept updated.

    (C) Subsequent annual surveys

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

    (D) Special Survey

    The shipowner shall demonstrate to this Society the activities in **401. 1 (4) (C)** as per the Ship cyber resilience test procedure.

402. Protect

1. Security Zones and Network Segmentation

(1) Requirement

    (A) All CBSs shall be grouped into security zones with well-defined security policies and security capabilities.

    (B) Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.)

    (C) Only explicitly allowed traffic shall traverse a security zone boundary.

(2) Requirement details

    (A) A security zone may contain multiple CBSs and networks, all of which shall comply with applicable security requirements given in this Chapter and **Ch 3**.

    (B) The network(s) of a security zone shall be logically or physically segmented from other zones or networks. See also **402. 6 (2)**.

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

    (D) Navigational and communication systems shall not be in the same security zone as machinery or cargo systems. If navigation and/or radio-communication systems are approved in accordance with other equivalent standard(s) (see **Ch 3, 102. 2**), these systems should be in a dedicated security zone.

(E) Wireless devices shall be in dedicated security zones. See also **402. 5**.

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

(G) It shall be possible to isolate a security zone without affecting the primary functionality of the CBSs in the zone, see also **404. 3**.

(3) Rationale

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

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

(4) Classification Survey

(A) Design phase

(a) The systems integrator shall submit Zones and conduit diagram and the Cyber security design description, see **202. 1** (1).

(b) The Zones and conduit diagram shall illustrate the CBSs, how they are grouped into security zones, and include the following information:

Clear indication of the security zones

Simplified illustration of each CBS, and indication of the security zone in which the 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 (**Ch 3, 301. 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).

(c) The systems integrator shall include the following information in the Cyber security design description:

A short description of the CBSs allocated to the security zone. It shall be possible to identify each CBS in the Zones and conduit diagram.

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

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

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

(B) Construction phase

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

(C) On-board test phase

The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate to this Society that:

(a) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.

(b) Security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.

(5) Classification Maintenance Survey

(A) General

(a) For general requirements to surveys in the operation phase, see **203**.

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

Principle of Least Functionality (**402. 2 (1)**)

Explicitly allowed traffic (**402. 1 (1)**)

Protection against denial of service (DoS) events (**402. 2 (1)**)

Inspection of security audit records (**403. 1 (2)**)

(B) First annual survey

The shipowner shall demonstrate to this Society that the Zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.

(C) Subsequent annual surveys

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

(D) Special survey

The shipowner shall demonstrate to this Society the activities in **402. 1** (4) (C) as per the Ship cyber resilience test procedure.

2. Network protection safeguards

(1) Requirement

(A) Security zones shall be protected by firewalls or equivalent means as specified in **402. 1**.

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

(C) The CBSs 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) Requirement details

(A) The design of network shall include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic.

(B) Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format.

(3) Rationale

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

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

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

(4) Classification Survey

(A) Design phase: No requirements.

(B) Construction phase: No requirements.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate the following to this Society:

(i) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.

(ii) 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)

(iii) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the CBSs have been removed or prohibited in accordance with hardening guidelines provided by the suppliers, see **Ch 3, 203. 5** (7) and **Ch 3, 502. 7**.

(b) The tests in the above (ii) and (iii) may be omitted if performed during the certification of CBSs as per **202. 2** (2)

(5) Classification Maintenance Survey

For general requirements to surveys in the operation phase, see section 203.

(A) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **402. 2** (4) (C) as per the Ship cyber resilience test procedure.

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

(1) Requirement

CBSs shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.

(2) Requirement details

(A) Malware protection shall be implemented on CBSs. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software shall be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for system Cat.II and Cat.III CBSs performing real-time tasks).

(B) On CBSs where anti-virus and anti-malware software cannot be installed, malware protection shall be implemented in the form of operational procedures, physical

safeguards, or according to manufacturer's recommendations.
(3) 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.

Anti-virus, anti-malware, anti-spam 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 CBSs are electronic mail, electronic mail attachments, websites, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops.

(4) Classification Survey
  (A) Design phase
    The systems integrator shall include the following information in the Cyber security design description:
    (a) For each CBS, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.
    (b) For CBSs with anti-malware software, information about how to keep the software updated.
    (c) Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system.
  (B) Construction phase
    The systems integrator shall ensure that malware protection is kept updated during the construction phase.
  (C) On-board test phase
    (a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate the following to this Society:
      Approved anti-malware software or other compensating countermeasures is effective (test e.g., with a trustworthy anti-malware test file).
    (b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2)

(5) Classification Maintenance Survey
  (A) General
    (a) For general requirements to surveys in the operation phase, see **203**.
    (b) The shipowner shall in the Ship cyber security and resilience program describe the management of malware protection, addressing at least the following requirements in this Chapter:
      Maintenance/update (**402. 3** (2))
      Operational procedures, physical safeguards (402.3 (2))
      Use of mobile, portable, removable media (**402. 4** (2) (D) and **402. 7** (2))
      Access control (**402. 4**)
  (B) First annual survey
    The shipowner shall present to this Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    (a) Any anti-malware software has been maintained and updated.
    (b) Procedures for use of portable, mobile or removable devices have been followed.
    (c) Policies and procedures for access control have been followed.

(d) Physical safeguards are maintained.
(C) Subsequent annual surveys
The shipowner shall upon request by this Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
(D) Special survey
The shipowner shall demonstrate to this Society the activities in section 402.3.(4).(C) as per the Ship cyber resilience test procedure.

4. Access control
(1) Requirement
  (A) CBSs and networks shall provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.
  (B) 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) Requirement details
  Access to CBSs and networks in the scope of applicability of this Chapter 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.
  (A) Physical access control
    CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.
  (B) Physical access control for visitors
    Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.
  (C) Physical access control of network access points
    (a) Access points to onboard networks connecting Cat.II and/or Cat.III CBSs shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance.
    (b) Independent computers isolated from all on-board networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, shall be used in case of occasional connection requested by a visitor (e.g. for printing documents).
  (D) Removable media controls
    A policy for the use of removable media devices shall be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. See also **402. 7**.
  (E) Management of credentials
    (a) CBSs and relevant information shall be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel shall be left active only for a limited period according to the role and responsibility of the account holder and shall be removed when no longer needed.

(Note) CBSs shall identify and authenticate human users as per item no.1 in **Table 3.4.1** of **Ch 3**. In other words, it is not necessary to "uniquely" identify and authenticate all human users.

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

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

(F) Least privilege principle

(a) Any human user allowed to access CBS and networks in the scope of applicability of this Chapter shall have only the bare minimum privileges necessary to perform its function.

(b) 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.

(3) Rationale

Attackers may attempt to access the ship's systems and data from either onboard the ship, within the company, or remotely through connectivity with the internet. Physical and logical access controls to cyber assets, networks etc. should then be implemented to ensure safety of the ship and its cargo.

Physical threats and relevant countermeasures are also considered in the ISPS Code. Similarly, the ISM Code contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of ISPS and ISM Codes may imply inclusion in the Ship Security Plan (SSP) and Safety Management System (SMS) of instructions and procedures for access control to safety critical assets.

(4) Classification Survey

(A) Design phase

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

(a) Location and physical access controls for the CBSs. Devices providing Human Machine Interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices shall be specified.

(B) Construction phase

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

(C) On-board test phase

The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate the following to this Society:

(a) Components of the CBSs are located in areas or enclosures where physical access can be controlled to authorized personnel.

(b) User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of CBSs as per **202. 2** (2)

(5) Classification Maintenance Survey
   (A) General
      (a) For general requirements to surveys in the operation phase, see **203**.
      (b) The shipowner shall in the Ship cyber security and resilience program describe the management of logical and physical access, addressing at least the following requirements in this Chapter:
         Physical access control (**402. 4** (2) (A))
         Physical access control for visitors (**402. 4** (2) (B))
         Physical access control of network access points (**402. 4** (2) (C))
         Management of credentials (**402. 4** (2) (E))
         Least privilege policy (**402. 4** (2) (F))
      (c) The shipowner shall in the Ship cyber security and resilience program describe the management of confidential information, addressing at least the following requirements in this Chapter:
         Confidential information (**401. 1** (2))
         Information allowed to authorized personnel (**402. 4** (2))
         Information transmitted on the wireless network (**402. 5** (2))
   (B) First annual survey
      The shipowner shall present to this Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
      (a) Personnel are authorized to access the CBSs in accordance with their responsibilities.
      (b) Only authorised devices are connected to the CBSs.
      (c) Visitors are given access to the CBSs according to relevant policies and procedures.
      (d) Physical access controls are maintained and applied.
      (e) Credentials, keys, secrets, certificates, relevant CBS documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures.
   (C) Subsequent annual surveys
      The shipowner shall upon request by this Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

5. Wireless communication
   (1) Requirement
   Wireless communication networks in the scope of this Chapter shall be designed, implemented and maintained to ensure that:
   (A) Cyber incidents will not propagate to other control systems
   (B) Only authorised human users will gain access to the wireless network
   (C) Only authorised processes and devices will be allowed to communicate on the wireless network
   (D) Information in transit on the wireless network cannot be manipulated or disclosed
   (2) Requirement details
   (A) Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices shall be applied to ensure integrity and confidentiality of the information transmitted on the wireless network.
   (B) Devices on the wireless network shall only communicate on the wireless network (i.e. they shall not be "dual-homed")
   (C) Wireless networks shall be designed as separate segments in accordance with **402. 1** and protected as per **402. 2**.
   (D) Wireless access points and other devices in the network shall be installed and configured

such that access to the network can be controlled.

(E) The network device or system utilizing wireless communication shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication.

(3) Rationale

(A) Wireless networks give rise to additional or different cybersecurity risks than wired networks. This is mainly due to less physical protection of the devices and the use of the radio frequency communication.

(B) Inadequate physical access control may lead to unauthorised personnel gaining access to the physical devices, which in turn could lead to circumventing logical access restrictions or deployment of rogue devices on the network.

(C) Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn could cater for attacks such as Piggybacking or Evil twin attacks (see https://us-cert.cisa.gov/ncas/tips/ST05-003).

(4) Classification Survey

(A) Design phase

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

(a) Description of wireless networks in the scope of applicability of this Chapter and how these are implemented as separate security zones. The description shall include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules)

(B) Construction phase

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

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate the following to this Society:

Only authorised 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 analyser tool).

(b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2)

(5) Classification Maintenance Survey

(A) For general requirements to surveys in the operation phase, see section 203.

(B) Special survey

Subject to modifications of the wireless networks, the shipowner shall demonstrate to this Society the activities in **402. 5** (4) (C) as per the Ship cyber resilience test procedure.

6. Remote access control and communication with untrusted networks

(1) Requirement

CBSs shall be protected against unauthorized access and other cyber threats from untrusted networks.

(2) Requirement details

(A) User's manual shall be delivered for control of remote access to onboard IT and OT systems. Clear guidelines shall identify roles and permissions with functions.

(B) For CBSs in the scope of applicability of this Chapter, no IP address shall be exposed to untrusted networks.

(C) Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at

network or transport layer. Confidentiality shall be ensured for information that is subject to read authorization.

(D) Design

CBSs in the scope of applicability of this Chapter shall:

(a) 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.

(b) 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.

(c) provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident.

(E) Additional requirements for remote maintenance

When remote access is used for maintenance, the following requirements shall be complied with in addition to those in **402. 6** (2) (D):

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

(b) 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.

(c) Suppliers shall provide plans for- and make security updates available to the shipowner, see **Ch 3, 502. 2** and **Ch 3, 502. 3** and **Ch 3, 502. 4**.

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

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

(f) After a configurable number of failed remote access attempts, the next attempt shall be blocked for a predetermined length of time.

(g) 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.

(3) Rationale

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

(4) Classification Survey

(A) Design phase

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

(a) Identification of each CBS in the scope of applicability of this Chapter that can be

remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.

(b) For each CBS, a description of compliance with requirements in 402. 6. (2), as applicable.

(B) Construction phase

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

(C) On-board test phase

The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate the following to this Society:

(a) Communication with untrusted networks is secured in accordance with **Ch 3, 402**. and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).

(b) Remote access requires multifactor authentication of the remote user.

(c) A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.

(d) Remote connections must be explicitly accepted by responsible personnel on board.

(e) Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.

(f) Remote sessions are logged (see **Ch 3, 401**. item no.13).

(g) Instructions or procedures are provided by the respective product suppliers (see **Ch 3, 301. 3**).

(5) Classification Maintenance Survey

(A) General

(a) For general requirements to surveys in the operation phase, see section 203.

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

User's manual (**402. 6** (2))

Roles and permissions (**402. 6** (2))

Patches and updates (**402. 6** (2) (E))

Confirmation prior to undertaking remote software update (**402. 6** (2) (E))

Interrupt, abort, roll back (**402. 6** (2) (E))

(B) First annual survey

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

(a) Remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals.

(b) Installation of security patches and other software updates have been carried out in accordance with Management of change procedures and in cooperation with the supplier.

(C) Subsequent Annual survey

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

(D) Special survey

The shipowner shall demonstrate to this Society the activities in **402. 6** (4) (C) as per the Ship cyber resilience test procedure.

7. Use of Mobile and Portable Devices

(1) Requirement

The use of mobile and portable devices in CBSs shall be limited to only necessary activities and be controlled in accordance with **Ch 3, 401**. item no.10. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked.

(2) Requirement details

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

(3) Rationale

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

(4) Classification Survey

(A) Design phase

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

(a) Any CBSs in the scope of applicability that do not meet the requirements in **Ch 3, 401**. item no.10, i.e., that shall have protection of interface ports by physical means such as port blockers.

(B) Construction phase

The systems integrator shall ensure that use of physical interface ports in the CBSs is controlled in accordance with **Ch 3, 401**. item no.10, and that any use of such devices follows procedures to prevent malware from being introduced in the CBS.

(C) On-board test phase

The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate to this Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures shall be demonstrated as relevant:

(a) Use of mobile and portable devices is restricted to authorised users.

(b) Interface ports can only be used by specific device types.

(c) Files cannot be transferred to the system from such devices.

(d) Files on such devices will not be automatically executed (by disabling autorun)

(e) Network access is limited to specific MAC or IP addresses.

(f) Unused interface ports are disabled.

(g) Unused interface ports are physically blocked.

(5) Classification Maintenance Survey

(A) General

(a) For general requirements to surveys in the operation phase, see **203**.

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

Policy and procedures (**402. 4** (2) (D))

Physical block of interface ports (**402. 7** (1))

Use by authorized personnel (**402. 7** (2))

Connect only authorized devices (**402. 7** (2))

Consider risk of introducing malware (**402. 7** (2))

(B) First annual survey

The shipowner shall present to this Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
(a) The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures.
(b) Only authorised devices are connected to the CBSs.
(c) Means to restrict use of physical interface ports are implemented as per approved design documentation.
(C) Subsequent annual surveys
The shipowner shall upon request by this Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
(D) Special survey
The shipowner shall demonstrate to this Society the activities in **402. 7** (4) (C) as per the Ship cyber resilience test procedure.

403. Detect

1. Network operation monitoring
(1) Requirement
Networks in scope of this Chapter shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.
(2) Requirement details
(A) Measures to monitor networks in the scope of applicability of this Chapter shall have the following capabilities:
(a) Monitoring and protection against excessive traffic
(b) Monitoring of network connections
(c) Monitoring and recording of device management activities
(d) Protection against connection of unauthorized devices
(e) Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See **Pt 6, Ch 2, 407.** of the Class Rules.
(B) Intrusion detection systems (IDS) may be implemented, subject to the following:
(a) The IDS shall be qualified by the supplier of the respective CBS
(b) The IDS shall be passive and not activate protection functions that may affect the performance of the CBS
(c) Relevant personnel should be trained and qualified for using the IDS
(3) Rationale
Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction could result in incidents where the vessel is ill-prepared for the threat. To enable an early response to attacks targeting these types of unknown vulnerabilities, technology capable of detecting unusual events is required. A monitoring system that can detect anomalies in networks and that can use post-incident analysis provides the ability to appropriately respond and further recover from a cyber event.
(4) Classification Survey
(A) Design phase: no requirements.
(B) Construction phase: no requirements.
(C) On-board test phase
(a) The systems integrator shall specify in the Ship cyber resilience test procedure and demonstrate to this Society the network monitoring and protection mechanisms in the CBSs.
Test that disconnected network connections will 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 **404. 4** (2).

Demonstrate that the CBS will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also **402. 2** (2) (C))

Demonstrate generation of audit records (logging of security-related events)

If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the CBSs.

(b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(c) Any Intrusion detection systems in the CBSs in scope of applicability to be implemented shall be subject to verification by this Society. Relevant documentation shall be submitted for approval, and survey/tests shall be carried out on board.

(5) Classification Maintenance Survey

(A) General

(a) For general requirements to surveys in the operation phase, see section 203.

(b) The shipowner shall in the Ship cyber security and resilience program describe the management activities to detect anomalies in the CBSs and networks, addressing at least the following requirements in this Chapter:

Reveal and recognize anomalous activity (**403**)

Inspection of security audit records (**403. 1** (2))

Instructions or procedures to detect incidents (**404. 1** (1))

(c) The above activities may be addressed together with incident response in **404. 1**.

(B) First annual survey

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

(a) The CBSs are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the CBSs.

(C) Subsequent annual surveys

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

(D) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **403. 1** (4) (C) as per the Ship cyber resilience test procedure.

2. Verification and diagnostic functions of CBS and networks

(1) Requirement

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

(2) Requirement details

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

(3) Rationale

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

Wireshark, nmap, etc.). It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the CBS.

(4) Classification Survey

 (A) Design phase: no requirements.

 (B) Construction phase: no requirements.

 (C) On-board test phase

  (a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2) and demonstrate to this Society the effectiveness of the procedures for verification of security functions provided by the suppliers.

  (b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

 (A) General

  (a) For general requirements to surveys in the operation phase, see **203**.

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

   Test and maintenance periods (**403. 2** (2))

   Periodic maintenance (**203. 3**)

 (B) First annual survey

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

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

 (C) Subsequent annual surveys

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

404. Respond

1. Incident response plan

(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 CBSs.

(2) Requirement details

 (A) The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the Incident Response Plan to be placed onboard at the first annual Survey. The Incident Response Plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

 (B) The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.

 (C) The incident response plan shall, as a minimum, include the following information:

  (a) Breakpoints for the isolation of compromised systems;

  (b) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events;

  (c) A description of expected major consequences related to cyber incidents;

(d) Response options, prioritizing those which do not rely on either shut down or transfer to independent or loc1al control, if any.

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

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

(3) Rationale

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

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

(4) Classification Survey

(A) Design phase

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

(a) References to information provided by the suppliers (see **Ch 3, 301. 8**) that may be applied by the shipowner to establish plans for incident response.

(B) Construction phase: no requirements.

(C) On-board test phase: no requirements.

(5) Classification Maintenance Survey

(A) General

(a) For general requirements to surveys in the operation phase, see **203**.

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

Description of who, when and how to respond to cyber incidents in accordance with requirements of **404. 1**.

Procedures or instructions for local/manual control in accordance with requirements in **404. 2**.

Procedures or instructions for isolation of security zones in accordance with requirements in **404. 3**.

Description of expected behaviour of the CBSs in the event of cyber incidents in accordance with requirements in **404. 4**.

(B) First annual survey

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

(a) The incident response plans are available for the responsible personnel onboard.

(b) Procedures or instructions for local/manual controls are available for responsible personnel onboard.

(c) Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.

(d) Any cyber incidents have been responded to in accordance with the incident response plans.

(C) Subsequent annual surveys

The shipowner shall upon request by this Society demonstrate implementation of the Ship

cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

2. Local, independent and/or manual operation

(1) Requirement

Any CBS needed for local backup control as required by **Pt 6, Ch, 2, 201. 4** of the Class Rules shall be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation.

(2) Requirement details

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

(B) If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in **402. 1** and **402. 2** shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone. Notwithstanding the above, special considerations can be given to CBSs with different concepts on case by case basis.

(C) The CBS for local control and monitoring shall otherwise comply with requirements in this Chapter.

(3) Rationale

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

(4) Classification Survey

(A) Design phase

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

(a) Description of how the local controls specified in **Pt 6, Ch, 2, 201. 4** of the Class Rules are protected from cyber incidents in any connected remote or automatic control systems.

(B) Construction phase

No requirements.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2)) and demonstrate to this Society that the required local controls in the scope of applicability of this Chapter needed for safety of the ship can be operated independently of any remote or automatic control systems.

(b) The tests shall be carried out by disconnecting all networks from the local control system to other systems/devices.

(c) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

For general requirements to surveys in the operation phase, see **203**.

(A) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **404. 2** (4) (C) as per the Ship cyber resilience test procedure.

3. Network isolation

(1) Requirement

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

(2) Requirement details

(A) 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.

(B) There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner.

(C) Individual system's data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.

(3) Rationale

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

(4) Classification Survey

(A) Design phase

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

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

(B) Construction phase: no requirements.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2)) and demonstrate to this Society by disconnecting all networks traversing security zone boundaries, that the CBSs in the security zone will maintain adequate operational functionality without network communication with other security zones or networks.

(b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

For general requirements to surveys in the operation phase, see 203.

(A) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **404. 3** (4) (C) as per the Ship cyber resilience test procedure.

4. Fallback to a minimal risk condition

(1) Requirement

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

(2) Requirement details

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

(a) bringing the system to a complete stop or other safe state;

(b) disengaging the system;

(c) transferring control to another system or human operator;

(d) other compensating actions.

(B) Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition.

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

(3) Rationale

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

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

(4) Classification Survey

(A) Design phase

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

(a) Specification of safe state for the control functions in the CBSs.

(B) Construction phase: no requirements.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2)) and demonstrate to this Society that CBSs in the scope of applicability of this Chapter respond to cyber incidents in a safe manner (as per **404. 4** (4) (A)), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means.

(b) The tests shall at least include denial of service (DoS) attacks and may be done together with related test in **403. 1** (4) (C).

(c) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

For general requirements to surveys in the operation phase, see **203**.

(A) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **404. 4** (4) (C) as per the Ship cyber resilience test procedure.

405. Recover

1. Recovery plan

(1) Requirement

A recovery plan shall be made by the shipowner to support restoring CBSs 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) Requirement details

(A) The various stakeholders involved in the design and construction phases of the ship shall provide information to the shipowner for the preparation of the recovery plan to be placed on-board at the first annual Survey. The recovery plan shall be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

(B) Recovery plans shall be easily understandable by the crew and external personnel and include essential instructions and procedures to ensure the recovery of a failed system

and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board shall be available.

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

(a) System recovery: methods and procedures to recover communication capabilities shall be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.

(b) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation shall be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

(D) Once the recovery objectives are defined, a list of potential cyber incidents shall be created, and the recovery procedure developed and described. Recovery plans shall include, or refer to the following information;

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

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

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

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

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

(f) Current configuration information for all components.

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

(F) Recovery plans in hard copy onboard and ashore shall be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

(3) Rationale

Incident response procedures are an essential part of system recovery. Responsible personnel should consider carefully and be aware of the implications of recovery actions (such as wiping of drives) and execute them carefully. It should be noted, however, that some recovery actions may result in the destruction of evidence that could provide valuable information on the causes of an incident.

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

(4) Classification Survey

(A) Design phase

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

(a) references to information provided by the suppliers (see **Ch 3, 301. 8**) that may be applied by the shipowner to establish plans to recover from cyber incidents.

(B) Construction phase: no requirements.

(C) On-board test phase

(a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2 (2)**) and demonstrate to this Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in **405. 2** and **405. 3**.

(b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

(A) General

    (a) For general requirements to surveys in the operation phase, see **203**.

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

    Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in **405. 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 the CBSs in accordance with requirements in **405. 2**.

    Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in **405. 2** and **405. 3**.

(B) First annual survey

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

    (a) Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.

    (b) Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.

    (c) Backup of the CBSs have been taken in accordance with the policies and procedures.

    (d) Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel on-board.

(C) Subsequent annual surveys

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

2. Backup and restore capability

(1) Requirement

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

(2) Requirement details

(A) Restore capability

    (a) CBSs shall have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident.

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

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

(B) Backup

    (a) CBSs and networks shall provide backup for data. The use of offline backups shall also be considered to improve tolerance against ransomware and worms affecting online backup appliances.

    (b) Backup plans shall be developed, including scope, mode and frequency, storage medium and retention period.

(3) Rationale

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

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

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

(C) Setting up a backup schedule;

(D) Monitoring the backup and recovery environment;

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

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

(4) Classification Survey

  (A) Design phase: no requirements.

  (B) Construction phase: no requirements.

  (C) On-board test phase

    (a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2)) and demonstrate to this Society the procedures and instructions for backup and restore provided by the suppliers for CBSs in the scope of applicability of this Chapter.

    (b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).

(5) Classification Maintenance Survey

For general requirements to surveys in the operation phase, see 203.

  (A) Special survey

Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **405. 2** (4) (C) as per the Ship cyber resilience test procedure.

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

(1) Requirement

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

  (B) Suitable documentation on how to execute the above-mentioned operations shall be available to on-board personnel.

(2) Requirement details

  (A) CBS and networks shall be capable of:

    (a) controlled shutdown allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe, consistent and known state.

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

    (c) rolling back to a previous configuration and/or state, to restore system integrity and consistency.

    (d) restarting and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source. Restart time shall be compatible with the system's intended service and shall not bring other connected systems, or the integrated system it is part of, to an inconsistent or unsafe state.

  (B) Documentation shall be available to onboard personnel on how to execute the above-mentioned operations in case of a system affected by a cyber incident.

(3) Rationale

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

While in the case of some cyber incidents hard shutdowns may be considered as a safety precaution, controlled shutdown is preferable in case of integrated systems to keep them in a consistent and known state with predictable behaviour. When standard shutdown procedures

are not done, data or program and operating system files corruption may occur. In case of OT systems, the result of corruption can be instability, incorrect functioning or failure to provide the intended service.

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

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

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

(4) Classification Survey
  (A) Design phase
      The systems integrator shall include the following information in the Cyber security design description:
      (a) references to product manuals or procedures describing how to safely shut down, reset, restore and restart the CBSs.
  (B) Construction phase: No requirements.
  (C) On-board test phase
      (a) The systems integrator shall submit Ship cyber resilience test procedure (refer to **202. 2** (2)) and demonstrate to this Society that manuals or procedures are established for shutdown, reset and restore of the CBSs. These manuals/procedures shall be provided to the shipowner.
      (b) The above tests may be omitted if performed during the certification of CBSs as per **202. 2** (2).
(5) Classification Maintenance Survey
    For general requirements to surveys in the operation phase, see 203.
  (A) Special survey
      Subject to modifications of the CBSs, the shipowner shall demonstrate to this Society the activities in **405. 3** (4) (C) as per the Ship cyber resilience test procedure. ↵

CHAPTER 3   Cyber Resilience of Systems and Equipment

Section 1   General

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

102. Application
1. The requirements in this Chapter apply to the computer-based system(CBS) in the application scope of this Guidance as specified in **Ch 1, 103. 2**.
2. For navigation and radio communication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in **Sec 4** may accepted by the Society, on the condition that relevant requirements in **Ch 2** are complied with.
3. **Sec 4** specifies the required security capabilities for CBSs.
4. The requirements in **Sec 4** are based on the selected requirements in IEC 62443-3-3. Reference can be made to the standards referenced to determine the full content, rationale and relevant guidance for each requirement.

103. Limitations
1. This Chapter does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:
   (1) **Ch 3, Sec 23** of **Guidance for Approval of Manufacturing Process and Type Approval, etc.** for environmental performance for the system hardware
   (2) **Pt 6, Ch 2, Sec 4** of the Rules for safety of equipment for the functionality of the software

104. Security Philosophy
1. Systems and Equipment
   (1) A System can consist of group of hardware and software enabling safe, secure and reliable operation of a process. Typical example could be Engine control system, DP system, etc.
   (2) Equipment may be one of the following.
      (A) Network devices (i.e. routers, managed switches)
      (B) Security devices (i.e. firewall, Intrusion Detection System)
      (C) Computers (i.e. workstation, servers)
      (D) Automation devices (i.e. Programmable Logic Controllers)
      (E) Virtual machine cloud-hosted
2. Cyber Resilience

The Cyber Resilience requirements in **Sec 4** will be applicable for all systems in the scope of **Ch 1, 103** as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

3. Essential Systems Availability

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

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

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

4. Compensating Countermeasures

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

(2) Compensating countermeasure(s) shall meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each requirement and the related items in the standards, and follow the principles specified in **301. 3**.

Section 2 Survey of Systems and Equipment

201. General

1. Determination on the application of CBS
Suppliers shall in cooperation with the System integrator determine if this Chapter is mandatory for the CBS. (see **Fig 3.2.1**)
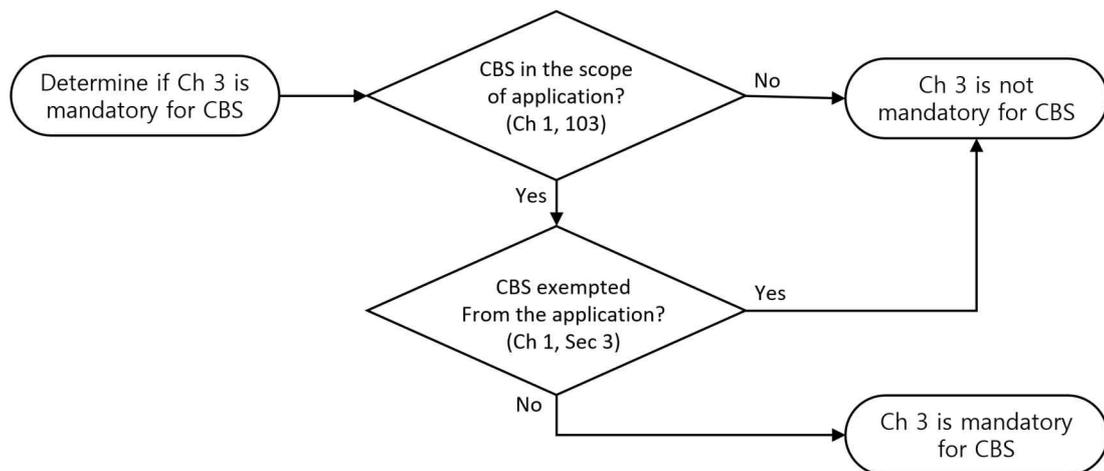
Fig 3.2.1 Determination on the application of CBS

2. Type Approval(TA) for Cyber Resilience
(1) The CBSs in the application scope of this Guidance shall be basically type-approved by this Society for Cyber Resilience according to the relevant requirements in this Chapter.
(2) The procedure and relevant matters related to the Type Approval for Cyber Resilience shall follow **the Guidance for Approval of Manufacturing Process and Type Approval, etc**.

3. Plan approval and inspection procedure for the ship-specific CBS
(1) The survey requirements for the ship-specific CBSs shall satisfy with **Pt 6, Ch 2, Sec 4 of the Class Rules** in addition to the requirement in this Chapter.
(2) In general, the plan approval and inspection for the ship-specific CBSs shall follow the procedure as indicated in **Fig 3.2.2**.
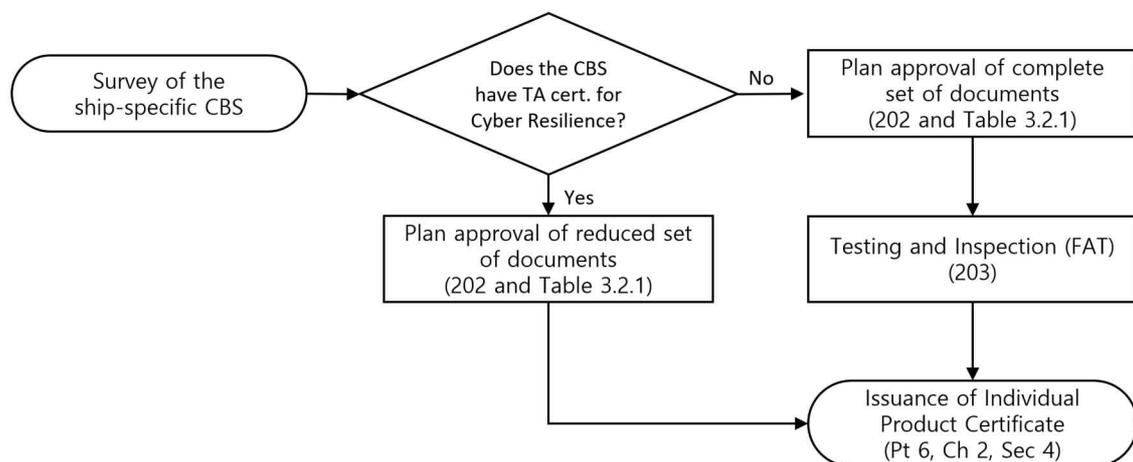
Fig 3.2.2 Plan approval and inspection procedure for ship-specific CBS

(3) Unless the CBS has the type approval certificate for Cyber Resilience, the CBS shall be tested and inspected including the plan approval of the completed set of documents as specified in **Table 3.2.1**. (see also **Fig 3.2.2**)

(4) Where IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in Sec 4 are applied for navigation and radio communication systems in accordance with **102. 2**, it shall be satisfactory to the following:

(A) The plan approval and inspection procedure shall demonstrated as indicated in **Fig 3.2.2**.

(B) Where considered necessary by the Society, additional plan approvals and inspections may be required to demonstrate correspondingly applied to the requirements in **Ch 2**.

(5) Where the CBSs, which do not require testing and inspection by Pt 6, Ch 2 of the Class Rules, have the Type Approval certificate for Cyber Resilience, testing and inspection along with the issuance of an individual product certificate according to 203 are not required for such CBSs.

202. Plan approval

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

2. If the CBS holds a valid Type approval certificate covering the requirements of this UR, subject to approval by the Society, the supplier may submit a reduced set of vessel-specific documents to the Society. (see **Table 3.2.1**)

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

Table 3.2.1 Document list for submission

No.	Document	Requirements	TA	Drawing approval	
				with TA	without TA
1	CBS asset inventory	To be incorporated in Vessel asset inventory (**Ch 2, 401. 1**)	Approve	Approve	Approve
2	Topology diagrams	Enabling System integrator to design security zones and conduits (**Ch 2, 402. 1**)	Approve	Approve	Approve
3	Description of security capabilities	Required security capabilities (**Ch 3, 401.**)	Approve		Approve
		Additional security capabilities, if applicable (**Ch 3, 402.**)			
4	Test procedure for security capabilities	Required security capabilities (**Ch 3, 401.**)	Approve		Approve
		Additional security capabilities, if applicable (**Ch 3, 402.**)			
5	Security configuration guidelines	Network and security configuration settings (**Ch 3, 401.** item no.29)	Info		Info
6	Secure development lifecycle	SDLC requirements (**Ch 3, Sec 5**)	Approve		Approve

7	Plans for maintenance and verification	Security functionality verification (Pt 6, Ch 2 Sec 4 of the Rules)	Info		Info
8	Information supporting incident response and recovery plans	Auditable events (Ch 3, 401. item no.13)	Info		Info
		Deterministic output (Ch 3, 401. item no.20)	Info		Info
		System backup (Ch 3, 401. item no.26)	Info		Info
		System recovery and reconstitution (Ch 3, 401. item no.27)	Info		Info
9	Management of change plan	Management of change process (Pt 6, Ch 2 Sec 4 of the Class Rules)	Info		Info
10	Test reports	Configuration of security capabilities and hardening (Ch 3, 301. 5, 501. 7)	Info	Info	Info

203. Testing and inspection

1. General

(1) Testing and inspection is a vessel-specific verification activity required for CBSs that do not hold a valid Type Approval certificate covering the requirements of this Chapter.

(2) The objective of testing and inspection is to demonstrate by testing and/or analytic evaluation that the CBS complies with relevant requirements in this Chapter. The testing and inspection shall be carried out at the supplier's premises or at other test site having the adequate apparatus for testing and inspection.

(3) After completed testing and inspection, this Society will issue an Individual product certificate and the supplier shall provide the certificate to the system integrator upon delivery of the CBS.

(4) Testing and inspection comply with the requirements specified in **203. 2** to **203. 5**.

2. General survey items

(1) The supplier shall demonstrate that design, construction, and internal testing has been completed.

(2) It shall also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This shall be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (**301. 1**) and the topology diagrams (**301. 2**).

3. Test of security capabilities

(1) The supplier shall test the required security capabilities on the system to be delivered. The tests shall be carried out in accordance with the approved test procedure in **301. 4** and be witnessed/accepted by our Surveyor.

(2) The tests shall provide the Society's surveyor with reasonable assurance that all requirements are met. This implies that testing of identical components is normally not required.

4. Correct configuration of security capabilities

(1) The supplier shall test/demonstrate for the class surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in **301. 5**. This demonstration may be carried out in conjunction with testing of the security capabilities.

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

5. Secure development lifecycle

The supplier shall, in accordance with documentation in **301. 6**, demonstrate compliance with requirements for secure development lifecycle in **Sec 5**.

(1) Controls for private keys (IEC 62443-4-1/SM-8)

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

    (B) 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.

    (C) 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.

(2) Security update documentation (IEC 62443-4-1/SUM-2)

    The supplier shall present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users shall include the items listed in **502. 2**.

(3) Dependent component security update documentation (IEC 62443-4-1/SUM-3)

    The supplier shall present management system documentation, as required by **502. 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.

(4) Security update delivery (IEC 62443-4-1/SUM-4)

    The supplier shall present management system documentation, 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.

(5) Product defence in depth (IEC 62443-4-1/SG-1)

    (A) The supplier shall present management system documentation, as required by **502. 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 the CBS during installation, maintenance and operation.

    (B) Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

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

    The supplier shall present management system documentation, 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.

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

    (A) The supplier shall present management system documentation, as required by **502. 7**, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.

    (B) The guidelines shall specify how to reduce vulnerabilities in the system by removal/prohibiting/disabling of unnecessary software, accounts, services, etc.

<div align="center">

Section 3 Approval documents and data

</div>

301. Approval documents and data of CBS

The following documents shall be submitted to the society for review and approval in accordance with the requirements in this Chapter. (see also **Sec 2**)

1. **CBS asset inventory**

    The CBS asset inventory shall include the information below.

    (1) List of hardware components (e.g., host devices, embedded devices, network devices)

        (A) Name

        (B) Brand/manufacturer

        (C) Model/type

        (D) Short description of functionality/purpose

        (E) Physical interfaces (e.g., network, serial)

        (F) Name/type of system software (e.g., operating system, firmware)

        (G) Version and patch level of system software

        (H) Supported communication protocols

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

        (A) The hardware component where it is installed

        (B) Brand/manufacturer

        (C) Model/type

        (D) Short description of functionality/purpose

        (E) Version of software

2. **Topology diagram**

    (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 the following:

        (A) All endpoints and network devices, including identification of redundant units

        (B) Communication cables (networks, serial links), including communication with I/O units

        (C) 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:

        (A) Communication endpoints (e.g. workstations, controllers, servers)

        (B) Network devices (switches, routers, firewalls)

        (C) Physical and virtual computers

        (D) Physical and virtual communication paths

        (E) Communication protocols

    (3) One combined topology diagram may be acceptable if all requested information can be clearly illustrated.

3. **Description of security capabilities**

    (1) This document shall describe how the CBS with its hardware and software components meets the required security capabilities in **401**.

    (2) Any network interfaces to other CBSs in the scope of applicability of **Ch 2** shall be described. The description shall include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (see **Ch 2, 402. 2** (1)) shall be described in detail if delivered as part of the CBS.

    (3) Any network interfaces to other systems or networks outside the scope of applicability of

untrusted networks(see **Ch 2**) shall be described. The description shall specify compliance with the additional security capabilities in **402**, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see **Ch 2, 402. 2** (1)) shall be described in detail if delivered as part of the 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 should:

  (A) Protect against the same threats as the original requirement

  (B) Provide an equal level of protection as the original requirement

  (C) Not be a security control that is required by other requirements in this Chapter.

  (D) Not introduce higher security risk

(6) Any supporting documents (e.g. OEM information) necessary to verify compliance with the requirements shall be referenced in the description and submitted.

4. Test procedure of security capabilities

(1) This document shall describe how to demonstrate by testing that the system complies with the requirements in **401 and 402**, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered.

(2) The procedure shall include a separate chapter for each applicable requirement and describe:

  (A) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)

  (B) Test equipment

  (C) Initial condition(s)

  (D) Test methodology, detailed test steps

  (E) Expected results and acceptance criteria

(3) The procedure shall also include means to update test results and record findings during the testing.

5. Security configuration guidelines

(1) 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 **Ch 2** and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)

(2) The document shall serve as basis for verification of **401** item no.29.

6. Secure development lifecycle documents

(1) This documentation shall be submitted to the Society upon request and shall describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in **Sec 5**.

(2) Software updates and patching shall be described.

(3) The document shall prepare the Society for survey as per **203. 5**.

7. Plans for maintenance and verification of the CBS

This document shall be submitted to the Society upon request and shall include procedures for security-related maintenance and testing of the system. The document shall include instructions for how the user can verify correct operation of the system's security functions as required by **401**, item no.19.

8. Information supporting the owner's incident response and recovery plan

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

(1) Local independent control (see **Ch 2, 404. 2**)

(2) Network isolation (see **Ch 2, 404. 3**)

(3) Forensics by use of audit records (see **401.** item no.13)

(4) Deterministic output (see **401.** item no.20)

(5) Backup (see **401.** item no.26)

(6) Restore (see **401.** item no.27)

(7) Controlled shutdown, reset, roll-back and restart (see **Ch 2, 405. 3**)

9. Management of change plan

This document shall be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by **Pt 6, Ch 2 Sec 4 of the Class Rule**.

10. Test reports

CBSs with Type approval certificate covering the security capabilities of this UR may be exempted from survey by the Society. However, test reports signed by the supplier shall be submitted to the Society, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the Society in survey. (see **203**)

Section 4 System Requirements

401. Required security capabilities

1. The following security capabilities are required for all CBSs in the scope specified in **Sec 1**.

Table 3.4.1 Required security capabilities

Item no.	Objective	Requirements	Reference
○ Protect against casual or coincidental access by unauthenticated entities			
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces	IEC62443-3-3/ SR1.1
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account	IEC62443-3-3/ SR1.3
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role.	IEC62443-3-3/ SR1.4
4	Authenticator management	The CBS shall provide the capability to: - Initialize authenticator content - Change all default authenticators upon control system installation - Change/refresh all authenticators - Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	IEC62443-3-3/ SR1.5
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	IEC62443-3-3/ SR1.6
6	Strength of password-based authentication	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	IEC62443-3-3/ SR1.7
7	Authenticator feedback	The CBS shall obscure feedback during the authentication process.	IEC62443-3-3/ SR1.10
○ Protect against casual or coincidental misuse			
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.	IEC62443-3-3/ SR2.1
9	Wireless use control	The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices.	IEC62443-3-3/ SR2.2

10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system shall include the capability to Limit the use of portable and mobile devices only to those permitted by design Restrict code and data transfer to/from portable and mobile devices (Note) Port limits / blockers (and silicone) could be accepted for a specific system	IEC62443-3-3/ SR2.3
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, Active X and PDF.	IEC62443-3-3/ SR2.4
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock.	IEC62443-3-3/ SR2.5
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication.	IEC62443-3-3/ SR2.8
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded.	IEC62443-3-3/ SR2.9
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure.	IEC62443-3-3/ SR2.10
16	Timestamps	The CBS shall timestamp audit records.	IEC62443-3-3/ SR2.11
○ Protect the integrity of the CBS against casual or coincidental manipulation			
17	Communication integrity	The CBS shall protect the integrity of transmitted information. (Note) Cryptographic mechanisms shall be employed for wireless networks.	IEC62443-3-3/ SR3.1
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It hall have the feature for updating the protection mechanisms.	IEC62443-3-3/ SR3.2
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report\when anomalies occur during maintenance.	IEC62443-3-3/ SR3.3
20	Deterministic output	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be	IEC62443-3-3/ SR3.6

		maintained as a result of an attack. The predetermined state could be: - Unpowered state, - Last-known value, or - Fixed value	
○ Prevent the unauthorized disclosure of information via eavesdropping or casual exposure			
21	Information confidentiality	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit.	IEC62443-3-3/ SR4.1
22	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations.	IEC62443-3-3/ SR4.3
○ Monitor the operation of the CBS and respond to incidents			
23	Audit log accessibility	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools.	IEC62443-3-3/ SR6.1
○ Ensure that the control system operates reliably under normal production conditions			
24	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload- based DoS events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed.	IEC62443-3-3/ SR7.1
25	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	IEC62443-3-3/ SR7.2
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations	IEC62443-3-3/ SR7.3
27	System recovery and reconstitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.	IEC62443-3-3/ SR7.4
28	Alternative power source	The CBS shall provide the capability to switch to and from an alternative power source without affecting the	IEC62443-3-3/ SR7.5

		existing security state or a documented degraded mode.	
29	Network and security configuration settings	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings.	IEC62443-3-3/ SR7.6
30	Least Functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the CBS: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software	IEC62443-3-3/ SR7.7

402. Additional security capabilities

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

2. CBSs with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection in **Ch 2, 402. 1, 402. 2**

Table 3.4.2 Additional security capabilities

Item no.	Objective	Requirements	Reference
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network.	IEC62443-3-3/ SR1.1, RE2
32	Software process and device identification and authentication	The CBS shall identify and authenticate software processes and devices.	IEC62443-3-3/ SR1.2
33	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period.	IEC62443-3-3/ SR1.11
34	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	IEC62443-3-3/ SR1.12
35	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled.	IEC62443-3-3/ SR1.13
36	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board.	IEC62443-3-3/ SR1.13, RE1
37	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable	IEC62443-3-3/ SR2.6

		time period of inactivity or manually by the user who initiated the session.	
38	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks.	IEC62443-3-3/ SR3.1, RE1
39	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS.	IEC62443-3-3/ SR3.5
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected.	IEC62443-3-3/ SR3.8
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions).	IEC62443-3-3/ SR3.8, RE1

<p style="text-align: center;">

Section 5 Secure Development Lifecycle Requirements

501. General

1. A Secure Development Lifecycle (SDLC) broadly addressing security aspects in following stages shall be followed for the development of systems or equipment.
    (1) Requirement analysis phase
    (2) Design phase
    (3) Implementation phase
    (4) Verification phase
    (5) Release phase
    (6) Maintenance Phase
    (7) End of life phase

2. A document, shall be produced that records how the security aspects have been addressed in above phases and shall at minimum integrate controlled processes as set out in below **502. 1** to **7**.

3. The said document is required to be submitted to this Society for review and approval.

502. Requirements

1. Controls for private keys (IEC 62443-4-1/SM-8)
    The manufacturer shall have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.

2. Security update documentation (IEC 62443-4-1/SUM-2)
    A process shall be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to:
    (1) The product version number(s) to which the security patch applies;
    (2) Instructions on how to apply approved patches manually and via an automated process;
    (3) Description of any impacts that applying the patch to the product can have, including reboot;
    (4) Instructions on how to verify that an approved patch has been applied; and
    (5) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.

3. Dependent component security update documentation (IEC 62443-4-1/SUM-3)
    A process shall be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to:
    (1) Stating whether the product is compatible with the dependent component or operating system security update;

4. Security update delivery (IEC 62443-4-1/SUM-4)
    A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.
    (Note) The manufacturer shall have QA process to test the updates before releasing.

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

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

A process shall be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used.

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

A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines shall include, but are not limited to, instructions, rationale and recommendations for the following:

(1) Integration of the product, including third-party components, with its product security context
(2) Integration of the product's application programming interfaces/protocols with user applications;
(3) Applying and maintaining the product's defence in depth strategy
(4) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
 (A) its contribution to the product's defence in depth strategy
 (B) descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
 (C) setting/changing/deleting its value;
(5) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product;
(6) Instructions and recommendations for periodic security maintenance activities;
(7) Instructions for reporting security incidents for the product to the supplier;
(8) Description of the security best practices for maintenance and administration of the product.

CHAPTER 4 Additional Requirements for Cyber Security Management System of ships

Section 1 General

101. Goals

1. The additional requirements in this chapter aim to support the implementation of comprehensive cyber security management based on cyber risk management processes during the operational phase of the Cyber Resilience Ship constructed as per the requirements of **Ch 2**.

2. When the Cyber Resilience Ships constructed as per the requirements of **Ch 2** further meet the requirements in this Chapter, such ships will fulfill the cyber risk management requirements according to IMO Resolution MSC.428 (98), and it will also meet the minimum inspection requirements for ship cyber security by the shippers such as OCIMF and RightShip.

102. Application

1. The requirements in this Chapter shall be additionally applied upon the request of the shipowner for the ships constructed as per the requirements of **Ch 2**.

2. The ship that additionally meets the requirements in this Chapter is assigned with the Class notation "**Cyber Resilience(Managed)**".

3. Except expressly specified otherwise, the requirements of this Chapter shall apply to CBSs and networks in the application scope according to **Ch 1, 103**.

103. Limitation

1. Where any cyber security-related regulation required by International Conventions, laws of flag states, and domestic laws of ports of call, are not specified within this Guidance, it is not included in the Classification Survey by this Society and the responsibility for the compliance of such regulations lies with the shipowner.

104. Approval documents and data

1. Ship cyber security and resilience program
   The Ship cyber security and resilience program shall conform to the requirements in **201. 1**.

2. Documents or data for reference
   Shipowner shall submit the following documents or data for reference.
   (1) Ship cyber risk assessment report and risk management plan
   (2) Cyber security organization chart and job description of security personnel

105. Classification Survey of ship

1. General
   (1) Kinds and intervals of classification survey according to this Chapter shall follow Ch 2, 201. 4.
   (2) Survey requirements of a ship shall comply with Ch 2, 203 in addition to this Chapter.

2. Annual Survey
   (1) Shipowner shall submit the documents and data to this Society and be approved in due time prior to the initial Annual Survey carried out according to this Chapter.
   (2) The shipowner shall present to this Society at least the following records or evidence

demonstrating implementation of requirements in Sec 2, but, it is not limited to this:

(A) Ship cyber risk assessment report and risk management result.

(B) training plan and report related to cyber security

(C) Cyber security incident report (if any)

(D) Internal audit plan and report related to cyber security

Section 2   Additional Requirements

201. Security policy

1. The Ship cyber security and resilience program specified in **Ch 2, 203. 1** (2) shall additionally address the following policies:
(1) Policy for cyber risk management
(2) Roles and responsibilities for cyber security management
(3) Policy for Crew Awareness and Training
(4) Policy for internal audit regarding cyber security

2. The shipowner shall place, review and manage the Ship cyber security and resilience program onboard.

3. The shipowner shall designate and assign responsibility and authority to the personnel who have the competencies to operate and manage the program.

202. Cyber risk management process

1. The shipowner shall establish a cyber risk management process, including identification, analysis, evaluation, and processing of cyber risks to CBS and networks in a ship.

2. Internal and external cyber threats that may adversely affect the operation of CBSs and networks on board ship shall be identified and listed.

3. The Cyber risk assessment for CBSs and networks on board ship shall be conducted periodically taking into account cyber threats and vulnerabilities.

4. Priorities for risk level shall be determined based on the results of the Cyber risk assessment, and improvement actions shall be taken if deemed necessary.

203. Awareness and training

1. A cyber security training plan shall be established for on-board personnel involved in security activities, and security training should be conducted periodically in an appropriate manner.

2. Awareness-raising activities for cyber security in a ship shall be properly implemented.
(Note) Examples of such awareness-raising activities may include:
1) Sharing of information related to cyber security issues such as external cyber security threats, cyber incident cases, etc., to crews.
2) Posting promotion materials to raise cybersecurity awareness (e.g, Instruction on safe usage of mobile devices, Instruction on safeguarding passwords, Instruction for malware prevention, etc.)

204. Incident Response and Recovery

1. The shipowner shall define the roles and responsibilities of the organization or crews responsible for immediate response and recovery activities to system operation and security issues in a ship.

2. An emergency contact network shall be established and kept it up to date to enable prompt communication with internal and external personnel.

3. In the event of a cyber incident onboard ship, procedures shall be established and implemented to notify the appropriate competent authorities and report to the relevant person in charge.

205. Cyber security internal audit

1. Cyber security internal audit procedure shall be established and conducted periodically. ⇩

Appendix I – Summary of requirements and documents for ships

Vessel asset inventory (Ch 2, 401. 1)			
CBS security capabilities	Provide documentation of product security updates	Ch 3, 502. 2	
	Provide documentation of dependent component security updates	Ch 3, 502. 3	
	Provide security updates	Ch 3, 502. 4	
CBS documentation	CBS asset inventory	Ch 3, 301. 1	
	Management of change plan	Ch 3, 301. 9	
Vessel design documentation	Vessel asset inventory	Ch 2, 401. 1 (4) (A)	
Ship cyber security and resilience program	Management of change	Ch 2, 401. 1 (5)	
	Management of software updates	Ch 2, 401. 1 (5)	
Security zones and network segmentation (Ch 2, 402. 1)			
CBS security capabilities			
CBS documentation	Topology diagrams	Ch 3, 301. 2	
Vessel design documentation	Zones and conduit diagram	Ch 2, 402. 1 (4) (A)	
	Design description	Ch 2, 402. 1 (4) (A)	
	Ship cyber resilience test procedure	Ch 2, 402. 1 (4) (C)	
Ship cyber security and resilience program	Management of security zone boundary devices (e.g., firewalls)	Ch 2, 402. 1. (5)	
Network protection safeguards (Ch 2, 402. 2)			
CBS security capabilities	Denial of service (DoS) protection (item 24)	Ch 3, 401.	
	Deterministic output (item 20)		
CBS documentation	Description of security capabilities	Ch 3, 301. 3	
	Test procedure for security capabilities	Ch 3, 301. 4	
Vessel design documentation	Ship cyber resilience test procedure	Ch 2, 402. 2 (4) (C)	
Ship cyber security and resilience program			
Antivirus, antimalware, antispam and other protections from malicious code (Ch 2, 402. 3)			
CBS security capabilities	Malicious code protection (#18)	Ch 3, 401	
CBS documentation	Description of security capabilities	Ch 3, 301. 3	
	Test procedure for security capabilities	Ch 3, 301. 4	
Vessel design documentation	Design description	Ch 2, 402. 3 (4) (A)	
	Ship cyber resilience test procedure	Ch 2, 402. 3 (4) (C)	
Ship cyber security and resilience program	Management of malware protection	Ch 2, 402. 3 (5)	
Access control (Ch 2, 402. 4)			
CBS security capabilities	Human user id. and auth. (#1) Account management (#2) Identifier management (#3) Authenticator management (#4) Authorization enforcement (#8)	Ch 3, 401.	
CBS documentation	Description of security capabilities	Ch 3, 301. 3	
	Test procedure for security capabilities	Ch 3, 301. 4	
Vessel design documentation	Design description	Ch 2, 402. 4 (4) (A)	

	Ship cyber resilience test procedure	Ch 2, 402. 4 (4) (C)
Ship cyber security and resilience program	Management of confidential information	Ch 2, 402. 4 (5)
	Management of logical and physical access	

Wireless communication (Ch 2, 402. 5)		
CBS security capabilities	Wireless access management (#5)	Ch 3, 401.
	Wireless use control (#9)	
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
Vessel design documentation	Design description	Ch 2, 402. 5 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 402. 5 (4) (C)
Ship cyber security and resilience program		

Remote access control and communication with untrusted networks (Ch 2, 402. 6)		
CBS security capabilities	Multifactor authentication (#31)	Ch 3, 402.
	Process / device id. and auth. (#32)	
	Unsuccessful login attempts (#33)	
	System use notification (#34)	
	Access via untrusted networks (#35)	
	Explicit access request approval (#36)	
	Remote session termination (#37)	
	Cryptographic integrity protection (#38)	
	Input validation (#39)	
	Session integrity (#40)	
	Invalidation of session ID (#41)	
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
Vessel design documentation	Design description	Ch 2, 402. 6 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 402. 6 (4) (C)
Ship cyber security and resilience program	Management of remote access and communication with/via untrusted networks	Ch 2, 402. 6 (5)

Use of mobile and portable devices (Ch 2, 402. 7)		
CBS security capabilities	Use control for portable devices (#10)	Ch 3, 401
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
Vessel design documentation	Design description	Ch 2, 402. 7 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 402. 7 (4) (C)
Ship cyber security and resilience program	Management of mobile and portable devices	Ch 2, 402. 7 (5)

Network operation monitoring (Ch 2, 403. 1)		
CBS security capabilities	Use control for portable devices (#10)	Ch 3, 401
	Auditable events (#13)	
	Denial of service (DoS) protection (#24)	
	Alarm excessive bandwidth use	Pt 6, Ch 2, Sec 4 of the Class Rules
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
Vessel design documentation	Ship cyber resilience test procedure	Ch 2, 403. 1 (4) (C)
Ship cyber security and	Incident response plans	Ch 2, 403. 1 (5)

resilience program		
Verification and diagnostic functions of CBS and networks (Ch 2, 403. 2)		
CBS security capabilities	Security function verification (#19)	Ch 3, 401.
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
	Plans for maintenance and verification	Ch 3, 301. 7
Vessel design documentation	Ship cyber resilience test procedure	Ch 2, 403. 2 (4) (C)
Ship cyber security and resilience program	Verification of security functions	Ch 2, 403. 2 (5)
Incident response plan (Ch 2, 404. 1)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
	Information supporting incident response and recovery plans	Ch 3, 301. 8
Vessel design documentation	Design description	Ch 2, 404. 1 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 404. 1 (4) (C)
Ship cyber security and resilience program	Incident response plans	Ch 2, 404. 1 (5)
Local, independent and/or manual operation (Ch 2, 404. 2)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
	Information supporting incident response and recovery plans	Ch 3, 301. 8
Vessel design documentation	Design description	Ch 2, 404. 2 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 404. 2 (4) (C)
Ship cyber security and resilience program	Incident response plans	Ch 2, 404. 2 (5)
Network isolation (Ch 2, 404. 3)		
CBS security capabilities		
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
	Information supporting incident response and recovery plans	Ch 3, 301. 8
Vessel design documentation	Design description	Ch 2, 404. 3 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 404. 3 (4) (C)
Ship cyber security and resilience program	Incident response plans	Ch 2, 404. 3 (5)
Fallback to a minimal risk condition (Ch 2, 404. 4)		
CBS security capabilities	Deterministic output (#20)	Ch 3, 4.1)
CBS documentation	Description of security capabilities	Ch 3, 301. 3
	Test procedure for security capabilities	Ch 3, 301. 4
	Information supporting incident response and recovery plans	Ch 3, 301. 8
Vessel design documentation	Design description	Ch 2, 404. 4 (4) (A)
	Ship cyber resilience test procedure	Ch 2, 404. 4 (4) (C)

Ship cyber security and resilience program	Incident response plans	Ch 2, 404. 4 (5)
Recovery plan (Ch 2, 405. 1)		
CBS security capabilities		
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	Ch 3, 301. 3 Ch 3, 301. 4 Ch 3, 301. 8
Vessel design documentation	Design description Ship cyber resilience test procedure	Ch 2, 405. 1 (4) (A) Ch 2, 405. 1 (4) (C)
Ship cyber security and resilience program	Recovery plans	Ch 2, 405. 1 (5)
Backup and restore capability (Ch 2, 405. 2)		
CBS security capabilities	System backup (#26) System recovery and reconstitution (#27)	Ch 3, 401.
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	Ch 3, 301. 3 Ch 3, 301. 4 Ch 3, 301. 8
Vessel design documentation	Ship cyber resilience test procedure	Ch 2, 405. 2 (4) (C)
Ship cyber security and resilience program	Recovery plan	Ch 2, 405. 2 (5)
Controlled shutdown, reset, restore and restart (Ch 2, 405. 3)		
CBS security capabilities	System recovery and reconstitution (#27)	Ch 3, 401.
CBS documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	Ch 3, 301. 3 Ch 3, 301. 4 Ch 3, 301. 8
Vessel design documentation	Design description Ship cyber resilience test procedure	Ch 2, 405. 3 (4) (A) Ch 2, 405. 3 (4) (C)
Ship cyber security and resilience program	Recovery plans	Ch 2, 405. 3 (5)
Risk assessment for exclusion of CBS from the application of requirements (Ch 1, Sec 3)		
CBS security capabilities		
CBS documentation		
Vessel design documentation	Risk assessment for the exclusion of CBSs	Ch 2, 202. 1 (1) (D)
Ship cyber security and resilience program		

GUIDANCE FOR CYBER RESILIENCE OF SHIPS AND SYSTEMS