Amendment on 27 June 2024
Resolved by Technical Committee on 30 January 2024

Cyber Resilience

Object of Amendment

Regulations for the Classification and Registry of Ships
Rules for the Survey and Construction of Steel Ships Parts A, B, D, O, P, PS, Q and X
Rules for Ballast Water Management Installations
Rules for High Speed Craft
Rules for the Survey and Construction of Passenger Ships
Rules for the Survey and Construction of Inland Waterway Ships
Rules for the Survey and Construction of Ships of Fibreglass Reinforced Plastics
Guidance for the Survey and Construction of Steel Ships Parts B and X
Guidance for Automatic and Remote Control Systems
Guidance for High Speed Craft
Guidance for the Survey and Construction of Inland Waterway Ships
Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use

Reason for Amendment

In April 2022, IACS adopted requirements related to the cyber resilience of on-board systems and equipment as IACS Unified Requirement (UR) E27 and requirements related to the cyber resilience of ships as IACS UR E26.

In September and November 2023, IACS respectively revised these URs as IACS UR E27(Rev.1) and E26(Rev.1) to clarify relevant survey requirements.

Accordingly, relevant requirements are amended based on IACS UR E27(Rev.1) and E26(Rev.1).

Outline of Amendment

The main contents of this amendment are as follows:

(1) Specifies requirements related to the cyber resilience of on-board systems and equipment in Chapter 4, Part X of the Rules for the Survey and Construction of Steel Ships.

(2) Specifies requirements related to the cyber resilience of ships in Chapter 5, Part X of the Rules for the Survey and Construction of Steel Ships.

(3) Specifies that the notation “Cyber Resilience” (abbreviated to CybR) is affixed to the classification characters of ships which have taken particular cyber resilience measures in Chapter 1, Part A of the Rules for the Survey and Construction of Steel Ships

(4) Specifies requirements related to approval of use of systems for which measures are taken to improve cyber resilience in Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use.

(5) Adds references to the Part X of the Rules for the Survey and Construction of Steel Ships established in December 2023 in accordance with IACS UR E22(Rev.3) on computer-based systems.

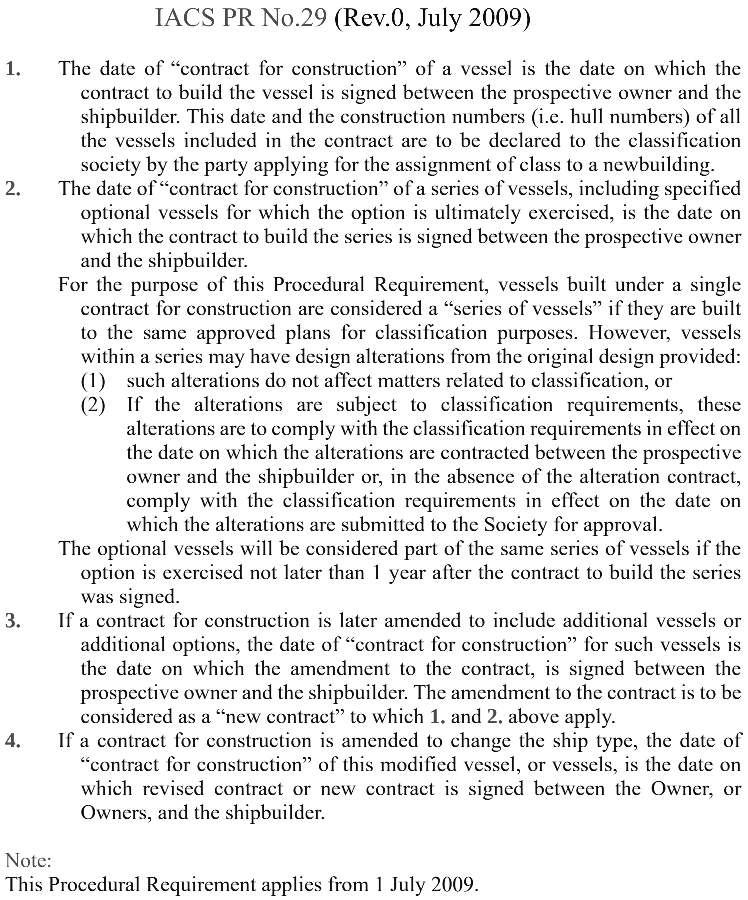
Effective Date and Application

This amendment applies to ships for which the date of contract for construction is on or after 1 July 2024.

ID: DD24-01

An asterisk (*) after the title of a requirement indicates that there is also relevant information in the corresponding Guidance.

Amended	Original	Remarks
REGULATIONS FOR THE CLASSIFICATION AND REGISTRY OF SHIPS **Chapter 2 CLASSIFICATION OF SHIPS** **2.1 Classification** **2.1.1 General*** Ships will be assigned a class and registered in the Classification Register defined in **2.1.5** when the ships have been surveyed for classification by the Society's Surveyors (hereinafter referred to as "the Surveyors") with regard to their hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, computer-based systems, stability and load lines in accordance with the rules for the survey and construction of ships provided separately (hereinafter referred to as "the Ship Rules") and found by the Society to be in compliance with the requirements of the Ship Rules. However, the Society may refuse the classification of ships regardless of the results of the survey in accordance with **1.4-3, Chapter 1 of the "Conditions of Service for Classification of ships and registration of installations"**. EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective	**REGULATIONS FOR THE CLASSIFICATION AND REGISTRY OF SHIPS** **Chapter 2 CLASSIFICATION OF SHIPS** **2.1 Classification** **2.1.1 General*** Ships will be assigned a class and registered in the Classification Register defined in **2.1.5** when the ships have been surveyed for classification by the Society's Surveyors (hereinafter referred to as "the Surveyors") with regard to their hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, stability and load lines in accordance with the rules for the survey and construction of ships provided separately (hereinafter referred to as "the Ship Rules") and found by the Society to be in compliance with the requirements of the Ship Rules. However, the Society may refuse the classification of ships regardless of the results of the survey in accordance with **1.4-3, Chapter 1 of the "Conditions of Service for Classification of ships and registration of installations"**.	Addition of rules which refer to new rules of Part X.

Amended	Original	Remarks
date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29.  IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part A GENERAL RULES	**Part A GENERAL RULES**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.2 Class Notations	**1.2 Class Notations**	
1.2.4 Hull Construction and Equipment, etc.* (**1** to **34** are omitted)	**1.2.4 Hull Construction and Equipment, etc.*** (**1** to **34** are omitted)	
35 For ships complying with the provisions of **Chapter 4** and **5, Part X**, the notation of “*Cyber Resilience*” (abbreviated to *CybR*) is affixed to the Classification Characters	(Newly added)	Addition of Notation.
36 Unless otherwise specified above, for ships deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	**35** Unless otherwise specified above, for ships deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29.		

Amended	Original	Remarks
IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part B CLASS SURVEYS	**Part B CLASS SURVEYS**	
Chapter 2 CLASSIFICATION SURVEYS	**Chapter 2 CLASSIFICATION SURVEYS**	
2.1 Classification Survey during Construction	**2.1 Classification Survey during Construction**	
2.1.1 General **1** In the Classification Survey during Construction, the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, computer-based systems, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in the Rules.	**2.1.1 General** **1** In the Classification Survey during Construction, the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in the Rules.	Addition of rules which refer to new rules of Part X.
2.1.6 Documents to be Maintained On Board* **1** At the completion of a classification survey, the Surveyor confirms that the finished versions of the following applicable drawings, plans, manuals, lists, etc., are on board. (1) Documents approved by the Society or their copies ((a) to (t) are omitted）	**2.1.6 Documents to be Maintained On Board*** **1** At the completion of a classification survey, the Surveyor confirms that the finished versions of the following applicable drawings, plans, manuals, lists, etc., are on board. (1) Documents approved by the Society or their copies ((a) to (t) are omitted）	
(u) Zones and conduit diagram (**2.2.3-3(4), Part X**)	(Newly added)	Addition of drawings kept onboard because E26(Rev.1) was incorporated.
(v) Cyber security design description (**2.2.3-3(5), Part X**)	(Newly added)	
(w) Vessel asset inventory (**2.2.3-3(6), Part X**)	(Newly added)	
(x) Risk assessment for the exclusion of computer-based systems (**2.2.3-3(7), Part X**)	(Newly added)	
(y) Description of compensating countermeasures	(Newly added)	

Amended	Original	Remarks
(2.2.3-3(8), Part X)		
(z) Ship cyber resilience test procedure (**2.2.3-4(2), Part X**)	(Newly added)	
（(2) and (3) are omitted）	（(2) and (3) are omitted）	
2.2 Classification Survey of Ships Not Built under Survey	**2.2 Classification Survey of Ships Not Built under Survey**	
2.2.1 General*	**2.2.1 General***	
1 In the Classification Survey of ships not built under the Society's survey, the actual scantlings of main parts of the ship are to be measured in addition to such examination of the hull and equipment, machinery, fire protection and detection, means of escape, fire fighting system, electrical installations, computer-based systems, stability and load lines as required for the Special Survey corresponding to the ship's age in order to ascertain that they meet the relevant requirements in the Rules.	**1** In the Classification Survey of ships not built under the Society's survey, the actual scantlings of main parts of the ship are to be measured in addition to such examination of the hull and equipment, machinery, fire protection and detection, means of escape, fire fighting system, electrical installations, stability and load lines as required for the Special Survey corresponding to the ship's age in order to ascertain that they meet the relevant requirements in the Rules.	Addition of rules which refer to new rules of Part X.

Amended	Original	Remarks
Chapter 3 ANNUAL SURVEYS	**Chapter 3 ANNUAL SURVEYS**	
3.2 Annual Surveys for Hull, Equipment, Fire Extinction, Computer-based Systems and Fittings	**3.2 Annual Surveys for Hull, Equipment, Fire Extinction and Fittings**	Addition of rules which refer to new rules of Part X.
(Omiited)	(Omitted)	
3.9 Special Requirements for Ships Affixed with the Notation "*CybR*"	**(Newly added)**	Addition of requirement of annual survey because E26(Rev.1) was incorporated.
3.9.1 General In addition to the requirements of **3.2** and **3.3**, the requirements of **3.9** apply to the Annual Surveys of ships affixed with the notation "*CybR*".	**(Newly added)** .	
3.9.2 Ship Cyber Security and Resilience Program **1** At Annual Surveys for ships affixed with the notation "*CybR*", a ship cyber security and resilience program is to be submitted to the Society by the first Annual Survey and verified by the Society in accordance with **2.2.3-5(7), Part X**. **2** At the completion of Annual Surveys, the surveyor is to confirm that the ship cyber security and resilience program is kept on board. **3** Change of vessel management company will require a new verification of the Ship cyber security and resilience program.	**(Newly added)**	
3.9.3 Surveys At Annual Surveys for ships affixed with the notation "*CybR*", the items specified in **Table B3.12** are to be examined.	**(Newly added)**	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended		Remarks
Table B3.12 Special Requirements for Ships Affixed with the Notation "*CybR*"		Addition of Table which was extracted requirement of "First annual survey" specified in UR E26(Rev. 1) 4.
Item	Examination	
1 Ship cyber security and resilience program (First Annual Survey)	(1) In accordance with the documents for management of change **and,** hardware and software modifications specified in **5.4.2(1)(d)iv), Part X,** confirm the following: (a) Vessel asset inventory is updated and completed at delivery. (b) Computer-based systems in the scope of applicability of this Chapter are correctly represented by the vessel asset inventory. (c) Software of the computer-based systems in the scope of applicability of this Chapter has been kept updated, e.g. by vulnerability scanning or by checking the software versions of computer-based systems while switched on. (2) In accordance with the documents for the management of security zone boundary devices specified in **5.4.3(1)(d)iv), Part X,** confirm that the zones and conduit diagram has been kept updated and **security zone boundaries are managed.** (3) In accordance with the documents for management of anti-malware specified in **5.4.3(3)(d)iv), Part X,** confirm the following: (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. (4) In accordance with the documents for the management of access and confidential information specified in **5.4.3(4)(d)iv), Part X,** confirm the following: (a) Personnel are authorized to access the computer-based systems in accordance with their responsibilities. (b) Only authorised devices are connected to the computer-based systems. (c) Visitors are given access to the computer-based systems according to relevant policies and procedures. (d) Physical access controls are maintained and applied.	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended				Remarks
		(e) Credentials, keys, secrets, certificates, relevant computer-based system documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures. (5) In accordance with the documents for the management of remote access and communication specified in **5.4.3(6)(d)iv), Part X,** confirm the following: (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. (6) In accordance with the documents for the management of mobile and portable devices specified in **5.4.3(7)(d)iv), Part X,** confirm the following: (a) The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures. (b) Only authorized devices are connected to the computer-based systems. (c) Means to restrict use of physical interface ports are implemented as per approved design documentation. (7) In accordance with the documents for the management activities to detect anomalies in the computer-based systems and networks specified in **5.4.4(1)(d)iv), Part X,** confirm that the computer-based systems are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the computer-based systems. (8) In accordance with the documents for the management activities to verify correct operation of the security functions in the computer-based systems and networks specified in **5.4.4(2)(d)iv), Part X,** confirm that the security functions in the computer-based systems are periodically tested or verified. (9) In accordance with incident response plans specified in **5.4.5(1)(d)iv), Part X,** confirm the following: (a) The incident response plans are available for the responsible personnel onboard.		

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended				Remarks
		(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. (10) In accordance with incident recovery plans specified in **5.4.6(1)(d)iv), Part X,** confirm the following: (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 computer-based systems have been taken in accordance with the policies and procedures. (d) Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.		
	2 Ship cyber security and resilience program (Subsequent Annual Survey)	(1) In accordance with presenting records or other documented evidence described in the Ship cyber security and resilience program specified in **-1** above, confirm the implementation of the program upon request by the Society.		

Amended	Original	Remarks
Chapter 4 INTERMEDIATE SURVEYS	**Chapter 4 INTERMEDIATE SURVEYS**	Addition of requirement of intermendiate survey because E26(Rev.1) was incorporated.
4.2 Intermediate Surveys for Hull, Equipment, Fire Extinction, Computer-based Systems and Fittings	**4.2 Intermediate Surveys for Hull, Equipment, Fire Extinction and Fittings**	
(Omitted)	(Omitted)	
4.9 Special Requirements for Ships Affixed with the Notation “*CybR*”	**(Newly added)**	
4.9.1 General In addition to the requirements of **4.2** to **4.3**, the requirements of **4.9** apply to the Intermediate Surveys of ships affixed with the notation “*CybR*”.	**(Newly added)**	
4.9.2 Surveys At Intermediate Surveys of ships affixed with the notation “*CybR*”, the examinations specified in **3.9.2** are to be carried out.	**(Newly added)**	substantially, it is no difference from subsequent annual survey.

Amended	Original	Remarks
Chapter 5 SPECIAL SURVEYS	**Chapter 5 SPECIAL SURVEYS**	Addition of requirement of special survey because E26(Rev.1) was incorporated.
5.2 Special Surveys for Hull, Equipment, Fire Extinction, Computer-based Systems and Fittings	**5.2 Special Surveys for Hull, Equipment, Fire Extinction and Fittings**	
(Omitted)	(Omitted)	
5.9 Special Requirements for Ships Affixed with the Notation "*CybR*"	**(Newly added)**	
5.9.1 General In addition to the requirements of **5.2** to **5.3**, the requirements of **5.9** apply to the Special Surveys of ships affixed with the notation "*CybR*".	**(Newly added)**	
5.9.2 Surveys At Special Surveys of ships affixed with the notation "*CybR*", examinations specified in **3.9.2** and examinations specified in **Table B5.32** are to be carried out in accordance with ship cyber resilience test procedure specified in **2.2.3-4(2), Part X**.	**(Newly added)**	

Amended-Original Requirements Comparison Table (Cyber Resilience)

<table>
<tr><th>Amended</th><th>Remarks</th></tr>
<tr><td>

Table B5.32 Special Requirements for Ships Affixed with the Notation "*CybR*"

<table>
<tr><th>Item</th><th>Examination</th></tr>
<tr><td colspan="2">Security requirements for "Identify"</td></tr>
<tr><td>1 Vessel asset inventory(<b>5.4.2(1), Part X</b>)</td><td>(1) Vessel asset inventory is updated and completed at delivery
(2) Computer-based systems in the scope of applicability of <b>Chapter 5, Part X</b> are correctly represented by the vessel asset inventory
(3) Software of the computer-based systems in the scope of applicability of <b>Chapter 5, Part X</b> has been kept updated, e.g. by vulnerability scanning or by checking the software versions of computer-based systems while switched on.</td></tr>
<tr><td colspan="2">Security requirements for "Protect"</td></tr>
<tr><td><b>2</b> Security zones and network segmentation <b>(5.4.3(1), Part X)</b></td><td>(1) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.
(2) Security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.</td></tr>
<tr><td><b>3</b> Network protection safeguards <b>(5.4.3(2), Part X)</b>(1), (2)</td><td>(1) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.
(2) Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests are to cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network)
(3) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the computer-based systems have been removed or prohibited in accordance with hardening guidelines provided by the suppliers.</td></tr>
<tr><td><b>4</b> Antivirus, antimalware, antispam and other protections from malicious code <b>(5.4.3(3), Part X)</b>(2)</td><td>(1) Approved anti-malware software or other compensating countermeasures is effective (test e.g., with a trustworthy anti-malware test file)</td></tr>
<tr><td><b>5</b> Wireless communication(<b>5.4.3(5), Part X</b>)(2)</td><td>(1) Only authorised devices can access the wireless network.
(2) Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).</td></tr>
</table>

</td><td>Addition of Table which was extracted requirement of "Commissioning phase" specified in UR E26(Rev. 1) 4.</td></tr>
</table>

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended				Remarks
	6 Remote access control and communication with untrusted networks **(5.4.3(6), Part X)**	(1) Communication with untrusted networks is secured in accordance with **4.4.3, Part X** and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool). (2) Remote access requires multifactor authentication of the remote user. (3) A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established. (4) Remote connections must be explicitly accepted by responsible personnel on board. (5) Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity. (6) Remote sessions are logged (see No.**13** in **Table X4.1, Part X**). (7) Instructions or procedures are provided by the respective product suppliers (see **4.4.1(3), Part X**)		
	7 Use of mobile and portable devices **(5.4.3(7), Part X)**	(1) Use of mobile and portable devices is restricted to authorised users. (2) Interface ports can only be used by specific device types. (3) Files cannot be transferred to the system from such devices. (4) Files on such devices will not be automatically executed (by disabling autorun). (5) Network access is limited to specific MAC or IP addresses. (6) Unused interface ports are disabled. (7) Unused interface ports are physically blocked.		
	Security requirement for the "Detect"			
	8 Network operation monitoring **(5.4.4(1), Part X)**(1), (2)	(1) Test that disconnected network connections will activate alarm and that the event is recorded. (2) Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test specified in **-11.** (3) Demonstrate that the computer-based system will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also **5.4.3(2)(d)iii), Part X**) (4) Demonstrate generation of audit records (logging of security-related events) (5) If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the computer-based systems.		
	Security requirements for "Respond"			
	9 Local, independent and/or manual operation **(5.4.5(2), Part X)**(1), (2)	(1) The required local controls needed for safety of the ship can be operated independently of any remote or automatic control systems. The tests are to be carried out by disconnecting all networks from the local control system to other systems/devices.		
	10 Network isolation **(5.4.5(3), Part X)**(1), (2)	(1) By disconnecting all networks traversing security zone boundaries, that the computer-based systems in the security zone will maintain adequate operational functionality without network communication with other security zones or networks.		

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended		Remarks
11 Fallback to a minimal risk condition (**5.4.5(4), Part X**)(1), (2)	(1) Respond to cyber incidents in a safe manner (as per **5.4.5(4)(d)i)**), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests are to at least include denial of service (DoS) attacks and may be done together with related test specified in **-8**.	
Security requirements for “Recover”		
12 Backup and restore capability (**5.4.6(2), Part X**)(1), (2)	(1) The procedures and instructions for backup and restore provided by the suppliers for computer-based systems.	
13 Controlled shutdown, reset, restore and restart (**5.4.6(3), Part X**)(1), (2)	(1) Manuals or procedures are established for shutdown, reset and restore of the computer-based systems.	

Notes:

1 Subject to modifications of the computer-based systems, the tests are carried out.

2 The tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-3(2), Part X**

Amended	Original	Remarks
Chapter 10 SURVEYS FOR STEEL BARGES	**Chapter 10 SURVEYS FOR STEEL BARGES**	
10.2 Classification Survey during Construction	**10.2 Classification Survey during Construction**	
10.2.1 General In the Classification Survey during Construction, it is to be confirmed that hull structure, hull equipment, machinery, fire protection, fire extinguishing systems, electrical installations, computer-based systems, stability and load lines of the barge comply with the relevant requirements specified in **Part Q**.	**10.2.1 General** In the Classification Survey during Construction, it is to be confirmed that hull structure, hull equipment, machinery, fire protection, fire extinguishing systems, electrical installations, stability and load lines of the barge comply with the relevant requirements specified in **Part Q**.	Addition of rules which refer to new rules of Part X. (the same as follow)
10.3 Classification Survey of Barges Not Built under Survey	**10.3 Classification Survey of Barges Not Built under Survey**	
10.3.1 General **1** In the Classification Survey of barges not built under the Society's survey, the actual scantlings of main structures of the barge are to be measured in addition to such examinations of the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, computer-based systems, stability and load lines as required for Special Surveys corresponding to the barge's age in order to ascertain that they meet the relevant requirements in the Rules	**10.3.1 General** **1** In the Classification Survey of barges not built under the Society's survey, the actual scantlings of main structures of the barge are to be measured in addition to such examinations of the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, stability and load lines as required for Special Surveys corresponding to the barge's age in order to ascertain that they meet the relevant requirements in the Rules	
10.4 Annual Survey	**10.4 Annual Survey**	
10.4.2 Annual Survey for Hull, Equipment, Computer-based Systems and Fire Extinction* (Omitted)	**10.4.2 Annual Survey for Hull, Equipment and Fire Extinction*** (Omitted)	

Amended	Original	Remarks
10.5 Intermediate Survey	**10.5 Intermediate Survey**	
10.5.2 Intermediate Survey for Hull, Equipment, Computer-based Systems and Fire Extinction* (Omitted)	**10.5.2 Intermediate Survey for Hull, Equipment and Fire Extinction*** (Omitted)	
10.6 Special Surveys	**10.6 Special Surveys**	
10.6.2 Special Survey for Hull, Equipment, Computer-based Systems and Fire Extinction* (Omitted)	**10.6.2 Special Survey for Hull, Equipment and Fire Extinction*** (Omitted)	

Amended	Original	Remarks
Chapter 12 SURVEYS FOR MOBILE OFFSHORE DRILLING UNITS AND SPECIAL PURPOSE BARGES	**Chapter 12 SURVEYS FOR MOBILE OFFSHORE DRILLING UNITS AND SPECIAL PURPOSE BARGES**	
12.2 Classification Survey during Construction	**12.2 Classification Survey during Construction**	
12.2.1 General* **1** In the Classification Survey during Construction, surveys are to be carried out on hull construction, equipment, machinery, construction of fire protection, means of escape, fire extinguishing systems, electrical installations, computer-based systems, stability and load lines in order to ascertain that they meet the relevant requirements of **Part P**.	**12.2.1 General*** **1** In the Classification Survey during Construction, surveys are to be carried out on hull construction, equipment, machinery, construction of fire protection, means of escape, fire extinguishing systems, electrical installations, stability and load lines in order to ascertain that they meet the relevant requirements of **Part P**.	Addition of rules which refer to new rules of Part X. (the same as follow)
12.2.3 Presence of Surveyor* **1** During the Classification Survey, the presence of the Surveyor is required at the following stages of the work in relation to hull construction, equipment, machinery, electrical installations and computer-based systems. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where the Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. ((1) to (7) are omitted)	**12.2.3 Presence of Surveyor*** **1** During the Classification Survey, the presence of the Surveyor is required at the following stages of the work in relation to hull construction, equipment, machinery and electrical installations. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where the Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. ((1) to (7) are omitted)	
12.2.7 Classification Survey of Units Not Built under Survey* **1** In the Classification Survey of units not built under the Society's survey, the actual scantlings of main parts of the units are to be measured in addition to such examination of the hull, equipment, machinery, fire protection, means of escape, fire fighting system, electrical installations, computer-based	**12.2.7 Classification Survey of Units Not Built under Survey*** **1** In the Classification Survey of units not built under the Society's survey, the actual scantlings of main parts of the units are to be measured in addition to such examination of the hull, equipment, machinery, fire protection, means of escape, fire fighting system, electrical installations, stability and load	

Amended	Original	Remarks
systems, stability and load lines as required for the Special Survey corresponding to the units' age in order to ascertain that they meet the relevant requirements in **Part P**.	lines as required for the Special Survey corresponding to the units' age in order to ascertain that they meet the relevant requirements in **Part P**.	
12.3 Annual Surveys	**12.3 Annual Surveys**	
12.3.2 Annual Surveys for Hull, Equipment, Fire Extinguishing Systems, Computer-based Systems, and Fittings* **2** Annual Surveys for hulls, equipment, fire extinguishing systems, computer-based systems, and fittings At Annual Surveys, the following surveys are to be carried out as far as practicable, in addition to the relevant survey items specified in **3.2.2** through **3.2.7** corresponding to hull structure, equipment, purpose, etc. Close-up surveys using remote inspection techniques (RIT) may be accepted subject to prior special consideration by the surveyor. In such cases, the close-up surveys using RIT is to be carried out under the direction, and in the presence, of the surveyor. ((1) to (3) are omitted)	**12.3.2 Annual Surveys for Hull, Equipment, Fire Extinguishing Systems, and Fittings*** **2** Annual Surveys for hulls, equipment, fire extinguishing systems and fittings At Annual Surveys, the following surveys are to be carried out as far as practicable, in addition to the relevant survey items specified in **3.2.2** through **3.2.7** corresponding to hull structure, equipment, purpose, etc. Close-up surveys using remote inspection techniques (RIT) may be accepted subject to prior special consideration by the surveyor. In such cases, the close-up surveys using RIT is to be carried out under the direction, and in the presence, of the surveyor. ((1) to (3) are omitted)	
12.4 Intermediate Surveys	**12.4 Intermediate Surveys**	
12.4.2 Intermediate Surveys for Hull, Equipment, Fire Extinguishing Systems, Computer-based Systems, and Fittings* (Omitted)	**12.4.2 Intermediate Surveys for Hull, Equipment, Fire Extinguishing Systems, and Fittings*** (Omitted)	
12.5 Special Surveys	**12.5 Special Surveys**	
12.5.2 Special Surveys for Hull, Equipment, Fire	**12.5.2 Special Surveys for Hull, Equipment, Fire**	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
Extinguishing Systems, Computer-based Systems, and Fittings* (Omitted)	**Extinguishing Systems, and Fittings*** (Omitted)	

Amended	Original	Remarks
Chapter 14 SURVEY FOR FLOATING OFFSHORE FACILITIES FOR CRUDE OIL/PETROLEUM GAS PRODUCTION, STORAGE AND OFFLOADING **14.2 Classification Surveys** **14.2.1 General** At Classification Surveys during construction, the hull, equipment, fire protection and detection means, means of escape, fire extinction means, machinery, electrical installations, computer-based systems etc. are to be examined in detail in order to ascertain that they meet the relevant requirements given in **Part PS**. **14.2.3 Presence of Surveyors** **1** At Classification Surveys during construction, the presence of a surveyor is required at all stages of the work on hull construction, equipment, machinery, electrical installations and computer-based systems in cases where the tests, examinations or inspections specified in **2.1** and **14.2.4** to **14.2.8** are carried out and in cases where the submitted plans and documents regarding tests, examinations or inspections specified in **14.2.2** are verified by the Society. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where a surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate. **14.2.10 Classification Surveys of Floating Offshore Facilities Not Built under Survey** **1** During the Classification Surveys of Floating Offshore	**Chapter 14 SURVEY FOR FLOATING OFFSHORE FACILITIES FOR CRUDE OIL/PETROLEUM GAS PRODUCTION, STORAGE AND OFFLOADING** **14.2 Classification Surveys** **14.2.1 General** At Classification Surveys during construction, the hull, equipment, fire protection and detection means, means of escape, fire extinction means, machinery, electrical installations, etc. are to be examined in detail in order to ascertain that they meet the relevant requirements given in **Part PS**. **14.2.3 Presence of Surveyors** **1** At Classification Surveys during construction, the presence of a surveyor is required at all stages of the work on hull construction, equipment, machinery and electrical installations in cases where the tests, examinations or inspections specified in **2.1** and **14.2.4** to **14.2.8** are carried out and in cases where the submitted plans and documents regarding tests, examinations or inspections specified in **14.2.2** are verified by the Society. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where a surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate. **14.2.10 Classification Surveys of Floating Offshore Facilities Not Built under Survey** **1** During the Classification Surveys of Floating Offshore	Addition of rules which refer to new rules of Part X. (the same as follow)

Amended	Original	Remarks
Facilities not built under Society surveys, the actual scantlings of the main parts of Floating Offshore Facilities are to be measured in addition to the examination of the main structures, equipment, machinery, fire protection, means of escape, fire extinguishing arrangements, electric installations, computer-based systems, stability, etc. in order to ascertain that they meet the relevant requirements given in **Part PS** as required for the Special Survey corresponding to the age, kind and purpose of the Floating Offshore Facilities.	Facilities not built under Society surveys, the actual scantlings of the main parts of Floating Offshore Facilities are to be measured in addition to the examination of the main structures, equipment, machinery, fire protection, means of escape, fire extinguishing arrangements, electric installations, stability, etc. in order to ascertain that they meet the relevant requirements given in **Part PS** as required for the Special Survey corresponding to the age, kind and purpose of the Floating Offshore Facilities.	

Amended	Original	Remarks
Chapter 15 SURVEYS FOR WORK-SHIPS	**Chapter 15 SURVEYS FOR WORK-SHIPS**	
15.2 Classification Surveys during Construction	**15.2 Classification Surveys during Construction**	
15.2.1 General **1** In Classification Surveys During Construction, surveys are to be carried out on the hull construction, equipment, machinery, fire protection, means of escape, fire extinguishing systems, electrical installations, computer-based systems, stability and load lines in order to ascertain that they meet the relevant requirements of **Part O**.	**15.2.1 General** **1** In Classification Surveys During Construction, surveys are to be carried out on the hull construction, equipment, machinery, fire protection, means of escape, fire extinguishing systems, electrical installations, stability and load lines in order to ascertain that they meet the relevant requirements of **Part O**.	Addition of rules which refer to new rules of Part X. (the same as follow)
15.2.3 Presence of Surveyor* **1** During the Classification Surveys, with respect to the stages of work related to hull construction, equipment, machinery, electrical installations and computer-based systems the presence of a Surveyor is required at the following stages in addition to those specified in **2.1.4**. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where a Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. (1) When performance tests, including the tests specified in **1.5** of **Annex 4.4.2-3, Part O**, are carried out on work-related installations (2) For ships with a dynamic positioning system, as specified in **12.2.3(6)**	**15.2.3 Presence of Surveyor*** **1** During the Classification Surveys, with respect to the stages of work related to hull construction, equipment, machinery and electrical installations, the presence of a Surveyor is required at the following stages in addition to those specified in **2.1.4**. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where a Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. (1) When performance tests, including the tests specified in **1.5** of **Annex 4.4.2-3, Part O**, are carried out on work-related installations (2) For ships with a dynamic positioning system, as specified in **12.2.3(6)**	
15.3 Annual Surveys	**15.3 Annual Surveys**	
15.3.2 Annual Surveys for Hull, Equipment, Fire	**15.3.2 Annual Surveys for Hull, Equipment, Fire**	

Amended	Original	Remarks
Extinguishing Systems, Computer-based Systems and Fittings*	**Extinguishing Systems, and Fittings***	
(Omitted)	(Omitted)	
15.4 Intermediate Surveys	**15.4 Intermediate Surveys**	
15.4.2 Intermediate Surveys for Hull, Equipment, Fire Extinction, Computer-based Systems and Fittings	**15.4.2 Intermediate Surveys for Hull, Equipment, Fire Extinction and Fittings**	
(Omitted)	(Omitted)	
15.5 Special Surveys	**15.5 Special Surveys**	
15.5.2 Special Surveys for Hull, Equipment, Fire Extinguishing Systems, Computer-based Systems and Fittings	**15.5.2 Special Surveys for Hull, Equipment, Fire Extinguishing Systems and Fittings**	
(Omitted)	(Omitted)	
EFFECTIVE DATE AND APPLICATION 1. The effective date of the amendments is 1 July 2024. 2. Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) 1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all		

Amended	Original	Remarks
the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part D MACHINERY INSTALLATIONS	**Part D MACHINERY INSTALLATIONS**	
Chapter 18 AUTOMATIC AND REMOTE CONTROL	**Chapter 18 AUTOMATIC AND REMOTE CONTROL**	
18.1 General	**18.1 General**	
18.1.1 Scope* (-1 and -2 are omitted.) (Deleted)	**18.1.1 Scope*** (-1 and -2 are omitted.) **3** Computer based systems, including the hardware and software which constitute such systems, are to be in accordance with **Chapters 1, 2 and 3, Part X** in addition to those specified in **-1** and **-2** above and throughout the rest of this chapter for design, construction, commissioning, maintenance, etc.	Reference was deleted. Annex 18.1.1, Part D transfer to part X in previous amendment (Computer based systems, December 2023).
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement		

Amended	Original	Remarks
(PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS **Part O WORK-SHIPS** **Chapter 2 DREDGERS** **2.8 Computer-based Systems** **2.8.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS** **Part O WORK-SHIPS** **Chapter 2 DREDGERS** **(Newly added)** **(Newly added)**	Addition of rules which refer to new rules of Part X. (the same as follow)
Chapter 3 CRANE SHIPS **3.8 Computer-based Systems** **3.8.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**Chapter 3 CRANE SHIPS** **(Newly added)** **(Newly added)**	
Chapter 4 VESSELS ENGAGED IN TOWING OPERATIONS **4.8 Computer-based Systems**	**Chapter 4 VESSELS ENGAGED IN TOWING OPERATIONS** **(Newly added)**	

Amended	Original	Remarks
4.8.1 General Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**(Newly added)**	
Chapter 5 PUSHER TUGS **5.8 Computer-based Systems** **5.8.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**Chapter 5 PUSHER TUGS** **(Newly added)** **(Newly added)**	
Chapter 6 FIRE FIGHTING VESSELS **6.8 Computer-based Systems** **6.8.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**Chapter 6 FIRE FIGHTING VESSELS** **(Newly added)** **(Newly added)**	
Chapter 7 OFFSHORE SUPPLY VESSELS **7.8 Computer-based Systems** **7.8.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**Chapter 7 OFFSHORE SUPPLY VESSELS** **(Newly added)** **(Newly added)**	

Amended	Original	Remarks
Chapter 8 ANCHOR HANDLING VESSELS	**Chapter 8 ANCHOR HANDLING VESSELS**	
8.8 Computer-based Systems	**(Newly added)**	
8.8.1 General Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**(Newly added)**	
Chapter 9 VESSELS ENGAGED IN LAYING OBJECTS ON THE SEABED	**Chapter 9 VESSELS ENGAGED IN LAYING OBJECTS ON THE SEABED**	
9.8 Computer-based Systems	**(Newly added)**	
9.8.1 General Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**(Newly added)**	
Chapter 10 OIL RECOVERY VESSELS	**Chapter 10 OIL RECOVERY VESSELS**	
10.10 Computer-based Systems	**(Newly added)**	
10.10.1 General Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**(Newly added)**	

Amended	Original	Remarks
Chapter 11 WIND TURBINE INSTALLATION SHIPS **11.16 Computer-based Systems** **11.16.1 General** Computer-based systems are to be in accordance with relevant requirements in **Part X**.	**Chapter 11 WIND TURBINE INSTALLATION SHIPS** **(Newly added)** **(Newly added)**	
Annex 4.4.2-3 TOWING WINCH EMERGENCY RELEASE SYSTEMS **1.4 Emergency Release System Requirements** **1.4.2 Operational Requirements** **8** Computer based systems that operate or may affect the control of emergency release systems are to meet the requirements for Category III systems in accordance with **Chapters 1, 2** and **3, Part X**. EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * "contract for construction" is defined in the latest version of IACS Procedural Requirement	**Annex 4.4.2-3 TOWING WINCH EMERGENCY RELEASE SYSTEMS** **1.4 Emergency Release System Requirements** **1.4.2 Operational Requirements** **8** Computer based systems that operate or may affect the control of emergency release systems are to meet the requirements for Category III systems in accordance with **18.1.1-3, Part D**.	Addition of rules which refer to new rules of Part X.

Amended	Original	Remarks
(PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS **Part P MOBILE OFFSHORE DRILLING UNITS AND SPECIAL PURPOSE BARGES** **Chapter 1 GENERAL** **1.1 General** **1.1.1 Application** **1** The requirements in this Part apply to the materials, welding, stability, hull construction, equipment, positioning systems, machinery installations, electrical installations, computer-based systems, fire protection and detection system, fire extinguishing systems, means of escape and load lines of mobile offshore drilling units and special purpose barges, etc., notwithstanding the requirements in other Parts. The mobile offshore drilling units and special purpose barges, etc., (hereinafter referred to as “units” in this Part) are steel-made ships and floating structures, and those are generally positioned for a long period of time or semi-permanently at a specific sea area, or fixed at a specific sea area.	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS** **Part P MOBILE OFFSHORE DRILLING UNITS AND SPECIAL PURPOSE BARGES** **Chapter 1 GENERAL** **1.1 General** **1.1.1 Application** **1** The requirements in this Part apply to the materials, welding, stability, hull construction, equipment, positioning systems, machinery installations, electrical installations, fire protection and detection system, fire extinguishing systems, means of escape and load lines of mobile offshore drilling units and special purpose barges, etc., notwithstanding the requirements in other Parts. The mobile offshore drilling units and special purpose barges, etc., (hereinafter referred to as “units” in this Part) are steel-made ships and floating structures, and those are generally positioned for a long period of time or semi-permanently at a specific sea area, or fixed at a specific sea area.	Addition of rules which refer to new rules of Part X. (the same as follow)

Amended	Original	Remarks
Chapter 19 COMPUTER-BASED SYSTEMS	**(Newly added)**	
19.1 General	**(Newly added)**	
19.1.1 Application Computer-based systems are to be in accordance with **Part X.**	**(Newly added)**	
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * "contract for construction" is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on		

Amended	Original	Remarks
the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS **Part PS FLOATING OFFSHORE FACILITIES FOR CRUDE OIL/PETROLEUM GAS PRODUCTION, STORAGE AND OFFLOADING** **Chapter 1 GENERAL** **1.1 General** **1.1.1 Application*** **1** The requirements given in this **Part PS** apply to the materials, welding, stability, hull construction, equipment, positioning systems, machinery installations, electrical installations, computer-based systems, fire protection and detection system, fire extinguishing systems, means of escape and load lines of the floating offshore facilities (hereinafter referred to as "Floating Offshore Facility" defined in **1.2.1**), not primarily intended for the transport of cargo, which are positioned at a specific oil producing sea areas permanently or for long periods of time, and also fitted with systems for the production, storage and offloading of crude oil/petroleum gases, notwithstanding the provisions specified in other Parts.	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS** **Part PS FLOATING OFFSHORE FACILITIES FOR CRUDE OIL/PETROLEUM GAS PRODUCTION, STORAGE AND OFFLOADING** **Chapter 1 GENERAL** **1.1 General** **1.1.1 Application*** **1** The requirements given in this **Part PS** apply to the materials, welding, stability, hull construction, equipment, positioning systems, machinery installations, electrical installations, fire protection and detection system, fire extinguishing systems, means of escape and load lines of the floating offshore facilities (hereinafter referred to as "Floating Offshore Facility" defined in **1.2.1**), not primarily intended for the transport of cargo, which are positioned at a specific oil producing sea areas permanently or for long periods of time, and also fitted with systems for the production, storage and offloading of crude oil/petroleum gases, notwithstanding the provisions specified in other Parts.	Addition of rules which refer to new rules of Part X. (the same as follow)
Chapter 10 COMPUTER-BASED SYSTEMS	**(Newly added)**	

Amended	Original	Remarks
10.1 General	**(Newly added)**	
10.1.1 Application* Computer-based systems are to be in accordance with **Part X.**	**(Newly added)**	
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the		

Amended	Original	Remarks
option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part Q STEEL BARGES	**Part Q STEEL BARGES**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.1 General	**1.1 General**	
1.1.1 Application*	**1.1.1 Application***	
1 The requirements in this Part are to be applied to the hull construction, equipment and machinery (including electrical equipment and computer-based systems, hereinafter referred to as “machinery”) of steel barges (hereinafter referred to as “barges”), notwithstanding the requirements specified in other Parts (except those in **Chapter 1, Part A** as well as **Part K**, **Part L**, **Part M**, **Part N**, **Part R**, **Part S**, **Part U**, **Part V** and **Part X**).	**1** The requirements in this Part are to be applied to the hull construction, equipment and machinery (including electrical equipment, hereinafter referred to as “machinery”) of steel barges (hereinafter referred to as “barges”), notwithstanding the requirements specified in other Parts (except those in **Chapter 1, Part A** as well as **Part K**, **Part L**, **Part M**, **Part N**, **Part R**, **Part S**, **Part U** and **Part V**).	Addition of rules which refer to new rules of Part X. (the same as follow)
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29.		

Amended	Original	Remarks
IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part X COMPUTER-BASED SYSTEMS	**Part X COMPUTER-BASED SYSTEMS**	
Chapter 1 INTRODUCTION	**Chapter 1 INTRODUCTION**	
1.1 General	**1.1 General**	
1.1.1 Scope This Part applies to computer-based systems. Details of the scope of application are to be in accordance with **Chapter 3** and subsequent chapters.	**1.1.1 Scope** This Part applies to computer-based systems, including the hardware and software which constitute such systems.	Amended to refer to each Chapters, because Chapter 3, 4, and 5 are applicable differently.

Amended	Original	Remarks
Chapter 2 PLANS, DOCUMENTS AND TESTS	**Chapter 2 PLANS, DOCUMENTS AND TESTS**	
2.1 Submission of Plans and Documents	**2.1 Submission of Plans and Documents**	
2.1.1 Submission of Plans and Documents The following drawings and data are, in principle, to be submitted. (1) Plans and documents for approval: (a) Plans and documents for computer-based systems subject to **Chapter 3** that are required to be submitted for approval purposes are specified in **2.2.1** according to system category. Summaries of said plans and documents are shown in **Tables X2.1** and **X2.2**. However, for computer-based systems approved for use in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**, plans and documents submitted for the approval of use may be reutilized.	**2.1.1 Submission of Plans and Documents** The following drawings and data are, in principle, to be submitted. (1) Plans and documents for approval: (a) Plans and documents for computer-based systems subject to **Chapter 3** that are required to be submitted for approval purposes are specified in **2.2.1** and **2.2.2** according to system category. Summaries of said plans and documents are shown in **Tables X2.1** and **X2.2**. However, submission of plans and documents may be omitted in accordance with **2.1.2-6, Part B** for computer-based systems approved for use in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**.	
(b) Plans and documents for computer-based systems subject to **Chapter 4** that are required to be submitted for approval purposes are specified in **4.4.1(1), (2), (3), (4)** and **(6)**. Summaries of said plans and documents are shown in **Table X2.3**. However, for computer-based systems approved for use in accordance with **Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**, where appropriate "Test Reports" specified in **4.4.1(10)** are submitted, plans and documents submitted for the approval	(Newly added)	Approval documents which required submission specified in E27(Rev.1), were extracted, and consolidate to chapter 2.

Amended	Original	Remarks
of use may be reutilized except for "Computer-based Systems Asset Inventory" specified in **4.4.1(1)** and "Topology Diagram" specified in **4.4.1(2)**.		
(c) Plans and documents for computer-based systems subject to **Chapter 5** that are required to be submitted for approval purposes are specified in **2.2.3-3(4), (5), (6), (7)** and **(8)**. Summary of plans and documents with related actions are shown in **Table X2.4**. Summary of requirements and related plans and documents are shown in **Table X2.5**.	(Newly added)	Approval documents which required submission specified in E26(Rev.1), were extracted, and consolidate to chapter 2.
(d) Other plans and documents considered necessary by the Society	(b) Other plans and documents considered necessary by the Society	
(2) Plans and documents for reference:	(2) Plans and documents for reference:	
(a) Plans and documents for computer-based systems subject to **Chapter 3** that are required to be submitted for reference purposes are specified in **2.2.1** according to system category. Summaries of said plans and documents are shown in **Tables X2.1** and **X2.2**. However, for computer-based systems approved for use in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**, plans and documents submitted for the approval of use may be reutilized except for the "list of system categorisations" specified in **2.2.1-3(3)**.	(a) Plans and documents for computer-based systems subject to **Chapter 3** that are required to be submitted for reference purposes are specified in **2.2.1** and **2.2.2** according to system category. Summaries of said plans and documents are shown in **Tables X2.1** and **X2.2**. However, submission of plans and documents may be omitted in accordance with **2.1.2-6, Part B** for computer-based systems approved for use in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use,** except for the "list of system categorisations" specified in **2.2.2-3**.	
(b) Plans and documents for computer-based systems subject to **Chapter 4** that are required to be submitted for reference purposes are specified in **4.4.1(5), (7), (8)** and **(9)**. Summaries of said	(Newly added)	Approval documents which required submission specified in E27(Rev.1), were

Amended	Original	Remarks
plans and documents are shown in **Table X2.3**. However, for computer-based systems approved for use in accordance with **Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**, where appropriate "Test Reports" specified in **4.4.1(10)** are submitted, plans and documents submitted for the approval of use may be reutilized.		extracted, and consolidate to chapter 2.
(c) Other plans and documents considered necessary by the Society	(b) Other plans and documents considered necessary by the Society	

Amended	Remarks
Table X2.1 System Supplier's Plans and Documents to be Submitted ~~by System Suppliers~~(Related to **Chapter 3 COMPUTER-BASED SYSTEMS**)	Editorial correction.

#	Referenced requirements	Plans and documents	Category I		Categories II and III	
			Reference	Approval	Reference	Approval
1	**2.2.1-~~1~~2(1)** and **3.4.2-1**	Quality plan (and quality manual)	-	-	-	○
2	**2.2.1-~~3~~2(3)** and **3.4.2-3**	System descriptions (System specification and design)	○*	-	-	○
3	**2.2.1-~~4~~2(4)** and **3.4.2-4**	Environmental compliance	○*	-	○	-
4	**2.2.1-~~5~~2(5)** and **3.4.2-5**	Software test report	-	-	○*	-
5	**2.2.1-~~6~~2(6)** and **3.4.2-6**	System test report	-	-	○*	-
6	**2.2.1-~~7~~2(7)** and **3.4.2-7**	FAT program	-	-	-	○
7	**2.2.1-~~7~~2(7)** and **3.4.2-7**	FAT report	-	-	○	-
8	**2.2.1-~~7~~2(7)** and **3.4.2-7**	Additional FAT documentation (e.g. user manuals)	-	-	○*	-
9	**2.2.1-~~8~~2(8)** and **3.4.2-8**	Change management procedure	-	-	-	○

(Notes)

Approval: Plans and documents to be submitted for approval

Reference: Plans and documents to be submitted for reference

○ : Submission required

○*: Submission required only when deemed necessary by the Society or its surveyor

See **3.3.1** for information on system categories

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X2.2 Systems Integrator's Plans and Documents to be Submitted ~~by Systems Integrators~~(Related to **Chapter 3 COMPUTER-BASED SYSTEMS**)	Editorial correction.

#	Referenced requirements	Plans and documents	Category I		Categories II and III	
			Reference	Approval	Reference	Approval
1	**2.2.~~2~~1-~~2~~3(2)** and **3.4.3-2**	Quality plan	-	-	-	○*
2	**2.2.~~2~~1-3(3)** and **3.4.3-3**	List of system categorisations	For reference (regardless of category) ○			
3	**2.2.~~2~~1.43(4)** and **3.4.3-4**	Risk assessment report (For determining system category)	For reference (regardless of category) ○*			
4	**2.2.~~2~~1-~~5~~3(5)** and **3.4.3-5**	Vessel's system architecture	○*	-	○*	-
5	**2.2.~~2~~1-~~6~~3(6)** and **3.4.3-6**	SAT program	-	-	-	○
6	**2.2.~~2~~1-~~6~~3(6)** and **3.4.3-6**	SAT report	-	-	○	-
7	**2.2.~~2~~1-~~7~~3(7)** and **3.4.3-7**	SOST program	-	-	-	○
8	**2.2.~~2~~1-~~7~~3(7)** and **3.4.3-7**	SOST report	-	-	○	-
9	**2.2.~~2~~1-~~8~~3(8)** and **3.4.3-8**	Change management procedure	-	-	-	○*

(Notes)

Approval: Plans and documents to be submitted for approval

Reference: Plans and documents to be submitted for reference

○ : Submission required

○*: Submission required only when deemed necessary by the Society or its surveyor

See **3.3.1** for information on system categories

Amended	Remarks
Table X2.3 Supplier’s Plans and Documents to be Submitted (Related to **Chapter 4 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT**)	E27(Rev.1) Appendix II

#	Document (Referenced requirements)	Requirements （Referenced requirements）	Reference	Approval
1	Computer-based system asset inventory **(4.4.1(1))**	To be incorporated in vessel asset inventory **(5.4.2(1))**	-	○$^{(1), (2)}$
2	Topology diagrams **(4.4.1(2))**	Enabling system integrator to design security zones and conduits **(5.4.3(1))**	-	○$^{(1), (2)}$
3	Description of security Capabilities **(4.4.1(3))**	Required security capabilities **(4.4.2)**	-	○$^{(1)}$
		Additional security capabilities, if applicable **(4.4.3)**		
4	Test procedure for security Capabilities **(4.4.1(4))**	Required security capabilities **(4.4.2)**	-	○$^{(1)}$
		Additional security capabilities, if applicable **(4.4.3)**		
5	Security configuration Guidelines **(4.4.1(5))**	Network and security configuration settings **(No.29 in Table X4.1)**	○$^{(1)}$	-
6	Secure development lifecycle **(4.4.1(6))**	Secure development lifecycle requirements **(4.5)**	-	○$^{(1)}$
7	Plans for maintenance and Verification **(4.4.1(7))**	Security functionality verification **(No.19 in Table X4.1)**	○$^{(1)}$	-
8	Information supporting incident response and recovery plans **(4.4.1(8))**	Auditable events **(No.13 in Table X4.1)**	○$^{(1)}$	-
		Deterministic output **(No.20 in Table X4.1)**		
		System backup **(No.26 in Table X4.1)**		
		System recovery and reconstitution **(No.27 in Table X4.1)**		
9	Management of change plan **(4.4.1(9))**	Management of change process **(Chapter 3)**	○$^{(1)}$	-
10	Test reports	Configuration of security capabilities and hardening	○$^{(2)}$	-

<table>
<tr><th>Amended</th><th>Remarks</th></tr>
<tr><td>
<table>
<tr><td></td><td><b>(4.4.1(10))</b></td><td><b>(4.4.1(5)</b> and <b>4.5.8)</b></td><td></td><td></td></tr>
</table>
(Notes)
Approval: Plans and documents to be submitted for approval
Reference: Plans and documents to be submitted for reference
○: Submission required
(1): Submitted when type approval has not been obtained in accordance with <b>Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use</b>
(2): Submitted when type approval has been obtained in accordance with <b>Chapter 10, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use</b>
</td><td></td></tr>
</table>

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X2.4 Systems Integrator’s or Shipowner’s Plans and Documents to be Submitted (Related to **Chapter 5 CYBER RESILIENCE OF SHIPS**)	E26(Rev.1) Appendix I

#	Document (Referenced requirements)	Systems integrator			Shipowner			
		Design	Construction	Commissioning	Operation	1st AS	AS/IS	SS
1	Approved supplier documentation (2.2.3)	-	Maintain	Maintain	Maintain	-	-	-
2	Zones and conduit diagram (**2.2.3-3(4)**)	Submit	Maintain	Maintain	Maintain	-	-	-
3	Cyber security design description (**2.2.3-3(5)**)	Submit	Maintain	Maintain	Maintain	-	-	-
4	Vessel asset inventory (**2.2.3-3(6)**)	Submit	Maintain	Maintain	Maintain	-	-	-
5	Risk assessment for the exclusion of computer-based systems (**2.2.3-3(7)**)*	Submit	Maintain	Maintain	Maintain	-	-	-
6	Description of compensating countermeasures (**2.2.3-3(8)**)*	Submit	Maintain	Maintain	Maintain	-	-	-
7	Ship cyber resilience test procedure (**2.2.3-4(2)**)	-	Submit	Demon-strate	Maintain	-	-	Demon-strate
8	Ship cyber security and resilience program (**2.2.3-5(7)**) - Management of change (MoC) (**5.4.2(1)(d)iv)**) - Management of software updates (**5.4.2(1)(d)iv)**) - Management of firewalls (**5.4.3(1)(d)iv)**) - Management of	-	-	-	Maintain	Submit	Demon-strate	-

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks

	malware protection (5.4.3(3)(d)iv)) - Management of access control （5.4.3(4)(d)iv）） - Management of access control （5.4.3(4)(d)iv）） - Management of remote access （5.4.3(6)(d)iv）） - Management of mobile and portable devices （5.4.3(7)(d)iv）） - Detection of security anomalies （5.4.4(1)(d)iv）） - Verification of security functions （5.4.4(2)(d)iv）） - Incident response plans（5.4.5(1)(d)iv）） - Recovery plans （5.4.6(1)(d)iv））							

(Notes)

*：If applicable

Submit: The stakeholder is to submit the document to the Society for verification and approval of compliance with requirements in **Chapter 5**.

Maintain: The stakeholder is to keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records are to be submitted to the Society as per **Table X2.2**.

Demonstrate: The stakeholder is to demonstrate compliance to the Society in accordance with the approved document.

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
1st AS：First Annual Survey AS/IS：Subsequent Annual Survey/Intermediate survey SS：Special Survey	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X2.5 Summary of Requirements and Documents (Related to **Chapter 5 CYBERESILIENCE OF SHIPS**)	E26(Rev.1) Appendix II

Vessel asset inventory (5.4.2(1))		
Computer-based system security capabilities	Provide documentation of product security updates Provide documentation of dependent component security updates Provide security updates	4.5.3 4.5.4 4.5.5

Computer-based system documentation	Computer-based system asset inventory
	Management of change plan
		4.4.1(1)
		4.4.1(9)

Vessel design documentation	Vessel asset inventory	5.4.2(1)(d)i)
Ship cyber security and resilience program	Management of change	5.4.2(1)(d)iv)
	Management of software updates	5.4.2(1)(d)iv)
Security zones and network segmentation (5.4.3(1))		
Computer-based system security capabilities	-	-
Computer-based system documentation	Topology diagrams	4.4.1(2)

Vessel design documentation	Zones and conduit diagram
	Design description
	Ship cyber resilience test procedure
		5.4.3(1)(d)i)
		5.4.3(1)(d)i)
		5.4.3(1)(d)iii)

Ship cyber security and resilience program	Management of security zone boundary devices (e.g., firewalls)	5.4.3(1)(d)iv)
Network protection safeguards (5.4.3(2))		
Computer-based system security capabilities	Denial of service (DoS) protection Deterministic output	No.24 in **Table X4.1** No.20 in **Table X4.1**

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)

Vessel design documentation	Ship cyber resilience test procedure	5.4.3(2)(d)iii)
Ship cyber security and resilience program	-	-
Antivirus, antimalware, antispam and other protections from malicious code (5.4.3(3))		
Computer-based system security capabilities	Malicious code protection	No.18 in **Table X4.1**

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.3(3)(d)i)
		5.4.3(3)(d)iii)

Ship cyber security and resilience program	Management of malware protection	5.4.3(3)(d)iv)

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended			Remarks
Access control (5.4.3(4))			
Computer-based system security capabilities	Human user ID and authorisation Account management Identifier management Authenticator management Authorisation enforcement	No.1 in Table X4.1 No.2 in Table X4.1 No.3 in Table X4.1 No.4 in Table X4.1 No.8 in Table X4.1	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.3(4)(d)i)
		5.4.3(4)(d)iii)	

Ship cyber security and resilience program	Management of confidential information	5.4.3(4)(d)iv)	
	Management of logical and physical access	5.4.3(4)(d)iv)	
Wireless communication (5.4.3(5))			
Computer-based system security capabilities	Wireless access management Wireless use control	No.5 in Table X4.1 No.8 in Table X4.1	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.3(5)(d)i)
		5.4.3(5)(d)iii)	

Ship cyber security and resilience program	-	-	
Remote access control and communication with untrusted networks (5.4.3(6))			
Computer-based system security capabilities	Multifactor authentication Process / device ID and authorisation Unsuccessful login attempts System use notification Access via untrusted networks Explicit access request approval Remote session termination Cryptographic integrity protection Input validation Session integrity Invalidation of session ID	No.31 in Table X4.2 No.32 in Table X4.2 No.33 in Table X4.2 No.34 in Table X4.2 No.35 in Table X4.2 No.36 in Table X4.2 No.37 in Table X4.2 No.38 in Table X4.2 No.39 in Table X4.2 No.40 in Table X4.2 No.41 in Table X4.2	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.3(6)(d)i)
		5.4.3(6)(d)iii)	

Amended	Remarks

Ship cyber security and resilience program	Management of remote access and communication with/via untrusted networks	5.4.3(6)(d)iv)
Use of mobile and portable devices (5.4.3(7))		
Computer-based system security capabilities	Use control for portable devices	No.10 in Table X4.1

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.3(7)(d)i)
		5.4.3(7)(d)iii)

Ship cyber security and resilience program	Management of mobile and portable devices	5.4.3(7)(d)iv)
Network operation monitoring (5.4.4(1))		
Computer-based system security capabilities	Use control for portable devices Auditable events Denial of service (DoS) protection Alarm excessive bandwidth use	No.10 in Table X4.1 No.13 in Table X4.1 No.24 in Table X4.1 3.7.2-1.

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
		4.4.1(3)
		4.4.1(4)

Vessel design documentation	Ship cyber resilience test procedure	5.4.4(1)(d)iii)
Ship cyber security and resilience program	Incident response plans	5.4.4(1)(d)iv)
Verification and diagnostic functions of computer-based system and networks (5.4.4(2))		
Computer-based system security capabilities	Security function verification	No.19 in Table X4.1

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Plans for maintenance and verification
		4.4.1(3)
		4.4.1(4)
		4.4.1(7)

Vessel design documentation	Ship cyber resilience test procedure	5.4.4(2)(d)iii)
Ship cyber security and resilience program	Verification of security functions	5.4.4(2)(d)iv)
Incident response plan (5.4.5(1))		
Computer-based system security capabilities	-	-
Computer-based system documentation	Description of security capabilities Test procedure for security capabilities Information supporting incident response and recovery plans	4.4.1(8)

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.5(1)(d)i)
		5.4.5(1)(d)iii)

Ship cyber security and resilience program	Incident response plans	5.4.5(1)(d)iv)

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended			Remarks
Local, independent and/or manual operation (**5.4.5(2)**)			
Computer-based system security capabilities	-	-	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.5(2)(d)i)
		5.4.5(2)(d)iii)	

Ship cyber security and resilience program	Incident response plans	**5.4.5(2)(d)iv)**	
Network isolation (**5.4.5(3)**)			
Computer-based system security capabilities	-	-	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.5(3)(d)i)
		5.4.5(3)(d)iii)	

Ship cyber security and resilience program	Incident response plans	**5.4.5(3)(d)iv)**	
Fallback to a minimal risk condition (**5.4.5(4)**)			
Computer-based system security capabilities	Deterministic output	No.**20** in **Table X4.1**	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.5(4)(d)i)
		5.4.5(4)(d)iii)	

Ship cyber security and resilience program	Incident response plans	**5.4.5(4)(d)iv)**	
Recovery plan (**5.4.6(1)**)			
Computer-based system security capabilities	-	-	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Design description	**5.4.6(1)(d)i)**	

Amended			Remarks
	Ship cyber resilience test procedure	**5.4.6(1)(d)iii)**	
Ship cyber security and resilience program	Recovery plans	**5.4.6(1)(d)iv)**	
Backup and restore capability (**5.4.6(2)**)			
Computer-based system security capabilities	System backup System recovery and reconstitution	No.26 in **Table X4.1** No.27 in **Table X4.1**	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Ship cyber resilience test procedure	**5.4.6(2)(d)iii)**	
Ship cyber security and resilience program	Recovery plan	**5.4.6(2)(d)iv)**	
Controlled shutdown, reset, restore and restart (**5.4.6(3)**)			
Computer-based system security capabilities	System recovery and reconstitution	No.27 in **Table X4.1**	

Computer-based system documentation	Description of security capabilities
	Test procedure for security capabilities
	Information supporting incident response and recovery plans
		4.4.1(3)
		4.4.1(4)
		4.4.1(8)	

Vessel design documentation	Design description
	Ship cyber resilience test procedure
		5.4.6(3)(d)i)
		5.4.6(3)(d)iii)	

Ship cyber security and resilience program	Recovery plans	**5.4.6(3)(d)iv)**	
Risk assessment for exclusion of computer-based system from the application of requirements (**5.5**)			
Computer-based system security capabilities	-	-	
Computer-based system documentation	-	-	
Vessel design documentation	Risk assessment for the exclusion of computer-based systems	**5.5**	
Ship cyber security and resilience program	-	-	

Amended	Original	Remarks
2.2 Tests	**2.2 Tests**	
2.2.1 Tests (Related to Chapter 3 COMPUTER BASED SYSTEMS**)**		Editorial correction.
1 Computer-based systems subject to **Chapter 3** are to be verified by the Society in accordance with **-2** and **-3** based on their system category. A summary of the tests to be witnessed and verified by Society surveyors are shown in **Table X2.6**.	Computer-based systems subject to **Chapter 3** are to be verified by the Society in accordance with **2.2.1** and **2.2.2** based on their system category. A summary of the tests to be witnessed and verified by Society surveyors are shown in **Table X2.3**.	
2 Verification Items for System Suppliers	**2.2.1 Verification Items for System Suppliers**	
(1) Quality plan (and quality manual) (see **3.4.2-1**) (a) Category I: This requirement is not applicable. (hereafter referred to as “N/A” in this Chapter) (b) Categories II and III: i) Quality plan (and quality manual) are to be submitted for approval. ii) Quality plan (and quality manual) are to be made available during FAT.	-1. Quality plan (and quality manual) (see **3.4.2-1**) (1) Category I: This requirement is not applicable. (hereafter referred to as “N/A” in this Chapter) (2) Categories II and III: (a) Quality plan (and quality manual) are to be submitted for approval. (b) Quality plan (and quality manual) are to be made available during FAT.	
(2) Unique identification of systems and software (see **3.4.2-2**) (a) Category I: N/A (b) Categories II and III: Application of the identification system is verified as a part of the FAT (see **3.4.2-7**) and SAT (see **3.4.3-6**)	-2. Unique identification of systems and software (see **3.4.2-2**) (1) Category I: N/A (2) Categories II and III: Application of the identification system is verified as a part of the FAT (see **3.4.2-7**) and SAT (see **3.4.3-6**)	
(3) System description (System specification and design) (see **3.4.2-3**) (a) Category I: The system description documentation is to be submitted for reference when deemed necessary by the Society. (b) Categories II and III: The system description documentation is to be submitted for approval.	-3. System description (System specification and design) (see **3.4.2-3**) (1) Category I: The system description documentation is to be submitted for reference when deemed necessary by the Society. (2) Categories II and III: The system description documentation is to be submitted for approval.	
(4) Environmental compliance of hardware components	-4. Environmental compliance of hardware components	

Amended	Original	Remarks
(see **3.4.2-4**)	(see **3.4.2-4**)	
(a) Category I: Environmental tests may be omitted. However, certificates issued in accordance with **Chapter 1, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use** or documents proving the passing of the environmental tests specified in **18.7.1(1), Part D** are to be submitted for reference when deemed necessary by Society (see **3.3.2**).	(1) Category I: Environmental tests may be omitted. However, certificates issued in accordance with **Chapter 1, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use** or documents proving the passing of the environmental tests specified in **18.7.1(1), Part D** are to be submitted for reference when deemed necessary by Society (see **3.3.2**).	
(b) Categories II and III: Certificates issued in accordance with **Chapter 1, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use** or documents proving the passing of the environmental tests specified in **18.7.1(1), Part D** are to be submitted for reference.	(2) Categories II and III: Certificates issued in accordance with **Chapter 1, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use** or documents proving the passing of the environmental tests specified in **18.7.1(1), Part D** are to be submitted for reference.	
(5) Software code creation, parameterisation, and testing (see **3.4.2-5**)	-5. Software code creation, parameterisation, and testing (see **3.4.2-5**)	
(a) Category I: N/A	(1) Category I: N/A	
(b) Categories II and III: Software test report is to be submitted for reference when deemed necessary by the Surveyor.	(2) Categories II and III: Software test report is to be submitted for reference when deemed necessary by the Surveyor.	
(6) Internal system testing before FAT (see **3.4.2-6**)	-6. Internal system testing before FAT (see **3.4.2-6**)	
(a) Category I: N/A	(1) Category I: N/A	
(b) Categories II and III:	(2) Categories II and III:	
i) Internal system test report is to be available during survey (FAT).	(a) Internal system test report is to be available during survey (FAT).	
ii) Internal system test report is to be submitted for reference when deemed necessary by the Surveyor.	(b) Internal system test report is to be submitted for reference when deemed necessary by the Surveyor.	
(7) FAT before installation on board (see **3.4.2-7**)	-7. FAT before installation on board (see **3.4.2-7**)	
(a) Category I: N/A	(1) Category I: N/A	

Amended	Original	Remarks
(b) Categories II and III:	(2) Categories II and III:	
i) The FAT program is to be submitted for approval before the test.	(a) The FAT program is to be submitted for approval before the test.	
ii) The FAT is to be witnessed by the Surveyor.	(b) The FAT is to be witnessed by the Surveyor.	
iii) The FAT report is to be submitted for reference.	(c) The FAT report is to be submitted to the Society branch office in charge for reference.	
iv) Additional FAT documentation (e.g. user manuals and internal system test reports specified in **-6**) is to be made available during the FAT.	(d) Additional FAT documentation (e.g. user manuals and internal system test reports specified in **-6**) is to be made available during the FAT.	
v) Additional FAT documentation (e.g. user manuals and internal system test reports specified in **-6**) may be required for reference when deemed necessary by the Surveyor.	(e) Additional FAT documentation (e.g. user manuals and internal system test reports specified in **-6**) is to be submitted for reference when deemed necessary by the Surveyor.	
(8) Secure and controlled software installation on the vessel (see **3.4.2-8**)	-8. Secure and controlled software installation on the vessel (see **3.4.2-8**)	
(a) Category I: N/A	(1) Category I: N/A	
(b) Categories II and III: The change management procedure is to be submitted for approval. The change management procedure may be included in quality plan (and quality manual).	(2) Categories II and III: The change management procedure is to be submitted for approval. The change management procedure may be included in quality plan (and quality manual).	
3 Verification Items for Systems Integrators	**2.2.2 Verification Items for Systems Integrators**	
(1) Appointed systems integrator (see **3.5.1-1**) The Society is to be informed in a timely manner by owners about the systems integrators appointed to be responsible for implementing any changes to the systems in conjunction with system suppliers.	-1. Appointed systems integrator (see **3.5.1-1**) The Society is to be informed in a timely manner by owners about the systems integrators appointed to be responsible for implementing any changes to the systems in conjunction with system suppliers.	
(2) Quality plan (see **3.4.3-2**)	-2. Quality plan (see **3.4.3-2**)	
(a) Category I: N/A	(1) Category I: N/A	
(b) Categories II and III:	(2) Categories II and III:	
i) Quality plan is to be made available for verification by the Surveyor during surveys	(a) Quality plan is to be made available for verification by the Surveyor during surveys	

Amended	Original	Remarks
(SAT/SOST). ii) Quality plan is to be submitted for the approval when deemed necessary by the Society.	(SAT/SOST). (b) Quality plan is to be submitted for the approval when deemed necessary by the Society.	
(3) Determining the category of the system in question (see **3.4.3-3**) The categories for the different systems are to be documented in the list of system categorisations and submitted for reference.	-3. Determining the category of the system in question (see **3.4.3-3**) The categories for the different systems are to be documented in the list of system categorisations and submitted for reference.	
(4) Risk assessment of the system (see **3.4.3-4**) Risk assessment report may be required for reference when deemed necessary by the Society.	-4. Risk assessment of the system (see **3.4.3-4**) Risk assessment report is to be submitted for approval when deemed necessary by the Society.	
(5) Define the vessel's system architecture (see **3.4.3-5**) The vessel's system architecture is to be submitted for reference when deemed necessary by the Society.	-5. Define the vessel's system architecture (see **3.4.3-5**) The vessel's system architecture is to be submitted for reference when deemed necessary by the Society.	
(6) System acceptance test (SAT) on board the vessel (see **3.4.3-6**) (a) Category I: N/A (b) Categories II and III: i) The SAT program is to be submitted to the Surveyor for approval before the test. ii) The SAT is to be witnessed by the Surveyor. iii) The SAT report is to be submitted to the Society for reference.	-6. System acceptance test (SAT) on board the vessel (see **3.4.3-6**) (1) Category I: N/A (2) Categories II and III: (a) The SAT program is to be submitted to the Surveyor for approval before the test. (b) The SAT is to be witnessed by the Surveyor. (c) The SAT report is to be submitted to the Surveyor for reference.	
(7) SOST at the vessel level (see **3.4.3-7**) (a) Category I: N/A (b) Categories II and III: i) The SOST program is to be submitted to the Surveyor for approval before the test. ii) The SOST is to be witnessed by the Surveyor. iii) The SOST report is to be submitted to the Society for reference.	-7. SOST at the vessel level (see **3.4.3-7**) (1) Category I: N/A (2) Categories II and III: (a) The SOST program is to be submitted to the Surveyor for approval before the test. (b) The SOST is to be witnessed by the Surveyor. (c) The SOST report is to be submitted to the Surveyor for reference.	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
(8) Change management (see **3.4.3-8**) (a) Category I: N/A (b) Categories II and III: The change management procedure is to be submitted for approval when deemed necessary by the Society.	-8. Change management (see **3.4.3-8**) (1) Category I: N/A (2) Categories II and III: The change management procedure is to be submitted for approval when deemed necessary by the Society.	

Amended	Remarks

Table X2.~~3~~6 Test Witnessing and Verifying

Editorial correction.

Referenced requirements	Verification details	Responsible party	Category I	Category II and III
2.2.1-~~7~~2(7) and **3.4.2-7**	Witness FAT	System supplier	-	○
2.2.~~2~~1-~~6~~3(6) and **3.4.3-6**	Witness SAT	Systems integrator	-	○
2.2.~~2~~1-~~7~~3(7) and **3.4.3-7**	Witness SOST	Systems integrator	-	○
3.6.12	Verification of changes	Systems integrator	-	○

(Notes)

○: Test required to be witnessed and verified by a Society surveyor

See **3.3.1** for information on system categories

2.2.2 Tests (Related to Chapter 4 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT)

1 Computer-based systems subject to **Chapter 4** are to be subjected to survey and factory acceptance testing as specified in **-2** to **-5**.

2 General survey items

E27(Rev.1) 6.3.1

The supplier is to demonstrate that design, construction, and internal testing has been completed. It is to also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This is to be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (**4.4.1(1)**) and the topology diagrams (**4.4.1(2)**).

3 Test of security capabilities

E27(Rev.1) 6.3.2

The supplier is to test the required security capabilities on the system to be delivered. The tests are to be carried out in accordance with the approved test procedure in **4.4.1(4)** and be witnessed/accepted by a surveyor. The tests are to provide the 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

E27(Rev.1) 6.3.3

The supplier is to test/demonstrate for a surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in **4.4.1(5)**. This demonstration may be carried out in conjunction with testing of the security capabilities. The security settings are to be documented in a report, e.g. a ship-specific instance of the configuration guidelines.

5 Secure development lifecycle

E27(Rev.1) 6.3.4

The supplier is to, in accordance with documentation in **4.4.1(6)**, demonstrate compliance with requirements for secure

Amended	Remarks
development lifecycle in **4.5**.	
(1) Controls for private keys (*IEC* 62443-4-1/SM-8) This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity. The supplier is to present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access. The policies and procedures are to address roles, responsibilities and work processes. The technical controls are to include e.g. physical access restrictions and cryptographic hardware (e.g. Hardware security module) for storage of the private key.	E27(Rev.1) 6.3.4.1
(2) Security update documentation (*IEC* 62443-4-1/SUM-2) The supplier is to 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 are to include the items listed in **4.5.3**.	E27(Rev.1) 6.3.4.2
(3) Dependent component security update documentation (*IEC* 62443-4-1/SUM-3) The supplier is to present management system documentation, as required by **4.5.4**, 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 is to address how to manage risks related to not applying the updated acquired software.	E27(Rev.1) 6.3.4.3
(4) Security update delivery (*IEC* 62443-4-1/SUM-4) The supplier is to present management system documentation, as required by **4.5.5**, 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.	E27(Rev.1) 6.3.4.4
(5) Product defence in depth (*IEC* 62443-4-1/SG-1) The supplier is to present management system documentation, as required by **4.5.6**, 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 computer-based system during installation, maintenance and operation. Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.	E27(Rev.1) 6.3.4.5
(6) Defence in depth measures expected in the environment (*IEC* 62443-4-1/SG-2) The supplier is to present management system documentation, as required by **4.5.7**, 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.	E27(Rev.1) 6.3.4.6
(7) Security hardening guidelines (*IEC* 62443-4-1/SG-3) The supplier is to present management system documentation, as required by **4.5.8**, substantiating that a process is	E27(Rev.1) 6.3.4.7

Amended	Remarks
established in the organization to ensure that hardening guidelines are produced for the system. The guidelines are to specify how to reduce vulnerabilities in the system by removal/prohibiting/disabling of unnecessary software, accounts, services, etc.	
2.2.3 Tests (Related to Chapter 5 CYBER RESILIENCE OF SHIPS**)**	E26(Rev.1) 5.
1 Computer-based systems subject to **Chapter 5** are to be subjected to tests for demonstration of compliance as specified in **-2** to **-5**.	
2 General	
(1) Evaluation of compliance with requirements in **Chapter 5** is to be carried out by the Society by assessment of documentation and survey in the relevant phases as specified in the following subsections.	
(2) Documentation to be submitted by suppliers to the Society is specified in **Chapter 4**. The approved versions of this documentation is also to be provided by the suppliers to the systems integrator as specified in **4.6.2**.	
(3) Documents to be provided by the systems integrator are listed in **2.2.3-3** and **-4**.	
(4) Documents to be provided by the shipowner are listed in **2.2.3-5**.	
(5) Upon delivery of the ship, the systems integrator is to provide below documentation to the shipowner:	
(a) Documentation of the computer-based systems provided by the suppliers (see **4.6.2**)	
(b) Documentation produced by the systems integrator (see **2.2.3-3** and **-4**)	
3 During design and construction phases	E26(Rev.1) 5.1
(1) The supplier is to demonstrate compliance to the Society by following the certification process specified in **4.6**.	
(2) The systems integrator is to demonstrate compliance by submitting documents in the following subsections to the Society for assessment.	
(3) During the design and construction phases, modifications to the design are to be carried out in accordance with the management of change (MoC) requirements in **3.6**.	
(4) The content of “Zones and conduit diagram” is specified in **5.4.3(1)(d)i)**.	E26(Rev.1) 5.1.1
(5) The content of “Cyber security design description (CSDD)” is specified in subsections “Design phase” for each requirement in **5.4**.	E26(Rev.1) 5.1.2
(6) The content of “Vessel asset inventory” is specified in **5.4.2(1)**.	E26(Rev.1) 5.1.3
(7) The content of “Risk assessment for the exclusion of computer-based systems” is specified in **5.5**.	E26(Rev.1) 5.1.4
(8) If any computer-based system in the scope of applicability of this Chapter has been approved with compensating countermeasures in lieu of a requirement in **Chapter 4**, “Description of compensating countermeasures” is to specify the respective computer-based system, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also **4.4.1(3)** requiring that the supplier describes such compensating countermeasures in the system documentation.	E26(Rev.1) 5.1.5

Amended	Remarks
4 Upon ship commissioning (1) Before final commissioning of the ship, the systems integrator is to: (a) Submit updated design documentation to the Society (as-built versions of the documents in **2.2.3-3**). (b) Submit Ship cyber resilience test procedure to the Society describing how to demonstrate compliance with **Chapter 5** by testing and/or analytic evaluation. (c) Carry out testing, witnessed by the Society, in accordance with the approved Ship cyber resilience test procedure.	E26(Rev.1) 5.2
(2) Ship cyber resilience test procedure (a) The content of this document is specified for the Commissioning phase in each subsection “Demonstration of compliance” in **5.4**. (b) For each computer-based system, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each computer-based system (see **Chapter 4**). Testing of such security functions may be omitted if specified in the respective subsection "Commissioning phase" in **5.4**, on the condition that these security functions have been successfully tested during the certification of the computer-based system as per **Chapter 4**. Nevertheless, all tests are to be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the computer-based system after the certification process. (c) The Ship cyber resilience test procedure is also to specify how to test any compensating countermeasures described in **2.2.3-3(8)**. (d) The Ship cyber resilience test procedure is to include means to update status and record findings during the testing, and specify the following information: i) Necessary test setup (i.e. to ensure the test can be repeated with the same expected result) ii) Test equipment iii) Initial condition(s) iv) Test methodology, detailed test steps v) Expected results and acceptance criteria (e) Before submitting the Ship cyber resilience test procedure to the Society, the systems integrator is to verify that the information is updated and placed under change management; that it is aligned with the latest configurations of computer-based systems and networks connecting such systems together onboard the ship and to other computer-based systems not onboard (e.g., ashore); and that the tests documented are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of computer-based systems and networks onboard.	E26(Rev.1) 5.2.1

Amended	Remarks
(f) The systems integrator is to 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 is to be carried out on board in accordance with the approved Ship cyber resilience test procedure after other commissioning activities for the computer-based systems are completed. The Society may request execution of additional tests.	
5 During the operational life of the ship (1) After the ship has been delivered to the shipowner, the shipowner is to manage technical and organisational security countermeasures by establishing and implementing processes as specified in **Chapter 5**. (2) Modifications to the computer-based systems in scope of applicability of **Chapter 5** are to be carried out in accordance with the management of change (MoC) requirements in **3.6**. This includes keeping documentation of the computer-based systems up to date. (3) The shipowner, with the support of suppliers, is to keep the Ship cyber resilience test procedure up to date and aligned with the computer-based systems onboard the ship and the networks connecting such systems to each other and to other computer-based systems not onboard (e.g. ashore). The shipowner is to update the Ship cyber resilience test procedure considering the changes occurred on computer-based systems and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment. (4) The shipowner is to prepare and implement operational procedures, provide periodic training and carry out drills for the onboard personnel and other concerned personnel ashore to familiarize them with the computer-based systems onboard the ship and the networks connecting such systems to each other and to other computer-based systems not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements. (5) The shipowner, with the support of supplier, is to keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of computer-based systems onboard the ship and the networks connecting such systems. (6) The shipowner is to retain onboard a copy of results of execution of tests and an updated Ship cyber resilience test procedure and make them available to the Society.	E26(Rev.1) 5.3
(7) First Annual Survey (a) In due time before the first Annual Survey of the ship, the shipowner is to submit to the Society a Ship cyber security and resilience program documenting management of cyber security and cyber resilience of the computer-based systems in the scope of applicability of **Chapter 5**. (b) The Ship cyber security and resilience program are to include policies, procedures, plans and/or other information documenting the processes/activities specified in subsections "Demonstration of compliance" in **5.4**.	E26(Rev.1) 5.3.1

Amended	Remarks
(c) After the Society has approved the Ship cyber security and resilience program, the shipowner is to in the first Annual Survey demonstrate compliance by presenting records or other documented evidence of implementation of the processes described in the approved Ship cyber security and resilience program. (d) Change of vessel management company will require a new verification of the Ship cyber security and resilience program.	
(8) Subsequent Annual Surveys In the subsequent Annual Surveys of the ship, the shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program.	E26(Rev.1) 5.3.2
(9) Special Survey Upon renewal of the ship's *Certificate of Classification*, the shipowner is to carry out testing witnessed by the Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards are to be demonstrated at Special Survey whereas other need only be carried out upon request by the Society based on modifications to the computer-based systems as specified in subsections "Operation phase" in **5.4**.	E26(Rev.1) 5.3.3

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
Chapter 3 COMPUTER-BASED SYSTEMS **3.2 Approval of Systems and Components** **3.2.2 Approval of Use for Computer-based Systems** **1** Computer-based systems that are routinely manufactured and include standardised software functions may be approved in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**. Hardware is to be documented according to **2.2.1-2(4).** The approval of use consists of two main verification activities: (1) assessment of type-specific documentation, and (2) survey and testing of the standardised functions.	**Chapter 3 COMPUTER-BASED SYSTEMS** **3.2 Approval of Systems and Components** **3.2.2 Approval of Use for Computer-based Systems** **1** Computer-based systems that are routinely manufactured and include standardised software functions may be approved in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**. Hardware is to be documented according to **2.2.1-4.** The approval of use consists of two main verification activities: (1) assessment of type-specific documentation, and (2) survey and testing of the standardised functions.	E22(Rev.3) was incorporated. Editorial correction.

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X3.2 Quality Management Systems (see below)	Editorial correction.

Table X3.2 Quality Management Systems

Area		Role	
#	Topic	System supplier	Systems integrator
1	Responsibilities and competency of the staff	~~×~~○	~~×~~○
2	The complete life cycle of the delivered software and associated hardware	~~×~~○	~~×~~○
3	Specific procedure for unique identification of a computer-based system, its components and versions	~~×~~○	-
4	Creation and update of the vessel's system architecture	-	~~×~~○
5	Organisation set in place for the acquisition of software and related hardware from suppliers	~~×~~○	~~×~~○
6	Organisation set in place for software code writing and verification	~~×~~○	-
7	Organisation set in place for system validation before integration in the vessel	~~×~~○	-
8	Specific procedure for conducting and approving of systems at FAT and SAT	~~×~~○	~~×~~○
9	Creation and update of system documentation	~~×~~○	-
10	Specific procedure for software modification and installation on board the vessel, including interactions with shipyards and owners	~~×~~○	~~×~~○
11	Specific procedures for verification of software code	~~×~~○	-
12	Procedures for integrating systems with other systems, and testing of the system of systems for the vessel	~~×~~○	~~×~~○
13	Procedures for managing changes to software and configurations before FAT	~~×~~○	-
14	Procedures for managing and documenting changes to software and configurations after FAT	~~×~~○	~~×~~○
15	Checkpoints for the organization's own follow-up of adherence to its quality management system	~~×~~○	~~×~~○

(Note)

~~×~~○: To be included in the quality management system

Amended	Remarks
Chapter 4 CYBER RESILIENCE OF ON-BOARD SYSTEMS AND EQUIPMENT	E27(Rev.1) was incorporated.
4.1 General	
4.1.1 General* This Chapter specifies requirements for cyber resilience of on-board systems and equipment.	E27(Rev.1) 1.1 para.2
4.1.2 Scope **1** This Chapter applies to the following **(1)** and **(2)**: (1) This Chapter applies to the following ships: (a) Passenger ships (including passenger high-speed craft) engaged in international voyages (b) Cargo ships of 500 GT and upwards engaged in international voyages (c) High speed craft of 500 GT and upwards engaged in international voyage (d) Mobile offshore drilling units of 500 GT and upwards (e) Self-propelled mobile offshore units engaged in construction (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc.) (2) This Chapter may be used for the following ships as non-mandatory guidance: (a) Ships of war and troopships (b) Cargo ships less than 500 gross tonnage (c) Vessels not propelled by mechanical means (d) Wooden ships of primitive build (e) Passenger yachts (passengers not more than 12) (f) Pleasure yachts not engaged in trade (g) Fishing vessels (h) Site specific offshore installations (i.e. FPSOs, FSUs, etc)	E27(Rev.1) 1.3
2 This Chapter applies to systems and interfaces for the following **(1)** and **(2)**. (1) Operational Technology (OT) systems onboard ships, i.e. those computer-based systems using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. In particular, the computer-based systems used for the operation of the following ship functions and systems, if present onboard, are to be considered: (a) Propulsion (b) Steering	E26(Rev.1) 1.3.2

Amended	Remarks
(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) (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) (j) Navigational systems required by statutory regulations (k) Internal and external communication systems required by class rules and statutory regulations For navigation and radiocommunication systems, the application of *IEC* 61162-460 or other equivalent standards in lieu of the required security capabilities in **4.4** may be accepted by the Society, on the condition that requirements in this Chapter are complied with. (l) Other systems or interfaces considered necessary by the Society (2) Any Internet Protocol (IP)-based communication interface from computer-based systems in scope of this Chapter to other systems. Examples of such systems are, but not limited to, the following: (a) passenger or visitor servicing and management systems (b) passenger-facing networks (c) administrative networks (d) crew welfare systems (e) any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).	
4.1.3 Limitations This Chapter does not cover environmental performance for the system hardware and the functionality of the software. In addition to this Chapter, the following requirements are to be applied: (1) **18.7.1(1), Part D, if required by 18.7.1, Part D, for the environmental performance of the system hardware** (2) **Chapter 3**, if applicable per **3.1.1**, for safety of equipment for the functionality of the software	E27(Rev.1) 1.2
4.2 Definitions and Abbreviations	
4.2.1 Terminology The terminology used in this Chapter is as specified in the following **(1)** to **(27)**:	E27(Rev.1) 1.4

Amended	Remarks
(1) “Attack surface” is 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. (2) “Authentication” is provision of assurance that a claimed characteristic of an identity is correct. (3) “Compensating countermeasure” is an alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements. (4) “Computer Based System” is a programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. computer-based system on-board include IT and OT systems. A computer-based system may be a combination of subsystems connected via network. On-board computer-based system may be connected directly or via public means of communications (e.g. Internet) to ashore computer-based systems, other vessels’ computer-based system and/or other facilities. (5) “Computer Network” is a connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols. (6) “Control” is a means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature. (7) “Cyber incident” is an event resulting from any offensive cyber manoeuvre, either intentional or unintentional, that targets or affects one or more computer-based system onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based system or transported in the networks connecting such systems. Cyber incidents do not include system failures. (8) “Cyber resilience” is the capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. (9) “Defence in depth” is information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (10) “Essential Systems” are Computer Based System contributing to the provision of services essential for propulsion and steering, and safety of the ship. Essential services comprise “Primary Essential Services” and “Secondary Essential	

Amended	Remarks
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. (11) "Firewall" is a logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules. (12) "Firmware" is 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. (13) "Hardening" is the practice of reducing a system's vulnerability by reducing its attack surface. (14) "Information Technology (IT)" are devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT). (15) "Integrated system" is a system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes. (16) "Network switch (Switch)" is a device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. (17) "Offensive cyber manoeuvre" are actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems. (18) "Operational technology (OT)" are devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. (19) "OT system" are computer based systems, which provide control, alarm, monitoring, safety or internal communication functions. (20) "Patches" are software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications (21) "Protocols" are 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. (22) "Recovery" is 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. (23) "Supplier" is a manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.	

Amended	Remarks
(24) "System" is combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes. (25) "System Categories (I, II, III)" are system categories based on their effects on system functionality, which are defined in **3.3.1**. (26) "System Integrator" is the specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The system integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role is to be taken by the shipyard unless an alternative organization is specifically contracted/assigned this responsibility. (27) "Untrusted network" is any network outside the scope of applicability of this Chapter.	
4.3 Security Philosophy	E27(Rev.1) 2.
4.3.1 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: (1) Network devices (i.e. routers, managed switches) (2) Security devices (i.e. firewall, Intrusion Detection System) (3) Computers (i.e. workstation, servers) (4) Automation devices (i.e. Programmable Logic Controllers) (5) Virtual machine cloud-hosted	E27(Rev.1) 2.1
4.3.2 Cyber Resilience The cyber resilience requirements in **4.4.2** and **4.4.3** will be applicable for all systems in scope of **Chapter 5** as applicable. Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.	E27(Rev.1) 2.2
4.3.3 Essential Systems Availability **1** Security measures for Essential system is not to be adversely affect the systems availability. **2** Implementation of security measures are not to 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.	E27(Rev.1) 2.3

Amended	Remarks
3 The system is to 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.	
4.3.4 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) are to 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 **4.4.1(3)**.	E27(Rev.1) 2.4
4.4 Requirements for Cyber resilience of on-board systems and equipment	
4.4.1 Documentation for Cyber resilience of on-board systems and equipment The following documents are to be submitted to the Society for review and approval in accordance with the requirements in this Chapter (see also **4.6.2**). (1) Computer-based system asset inventory The computer-based system asset inventory is to include the information below. (a) List of hardware components (e.g. host devices, embedded devices and network devices) i) Name ii) Brand/manufacturer iii) Model/type iv) Short description of functionality/purpose v) Physical interfaces (e.g. network and serial) vi) Name/type of system software (e.g. operating system and firmware) vii) Version and patch level of system software viii) Supported communication protocols (b) List of software components (e.g. application software and utility software) i) The hardware component where it is installed ii) Brand/manufacturer iii) Model/type iv) Short description of functionality/purpose	E27(Rev.1) 3.

Amended	Remarks
v) Version of software List of software components (e.g. application software and utility software) (2) Topology diagrams (a) The physical topology diagram is to illustrate the physical architecture of the system. It is to be possible to identify the hardware components in the computer-based system asset inventory. The diagram is to illustrate the following: i) All endpoints and network devices, including identification of redundant units ii) Communication cables (networks, serial links), including communication with I/O units iii) Communication cables to other networks or systems (b) The logical topology diagram is to illustrate the data flow between components in the system. The diagram is to illustrate the following: i) Communication endpoints (e.g. workstations, controllers and servers) ii) Network devices (switches, routers, firewalls) iii) Physical and virtual computers iv) Physical and virtual communication paths v) Communication protocols (c) One combined topology diagram may be acceptable if all requested information can be clearly illustrated. (3) Description of security capabilities (a) This document is to describe how the computer-based system with its hardware and software components meets the required security capabilities in **4.4.1**. (b) Any network interfaces to other computer-based systems in the scope of applicability of this Chapter are to be described. The description is to include destination computer-based system, data flows, and communication protocols. If the System integrator has allocated the destination computer-based system to another security zone, components providing protection of the security zone boundary (see **5.4.3(2)(a)**) are to be described in detail if delivered as part of the computer-based system. (c) Any network interfaces to other systems or networks outside the scope of applicability of this Chapter (untrusted networks) are to be described. The description is to specify compliance with the additional security capabilities in **4.4.3**, and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see **5.4.3(2)(a)**) are to be described in detail if delivered as part of the computer-based system. (d) A separate chapter is to be designated for each requirement. All hardware and software components in the system are to be addressed in the description, as relevant. (e) If any requirement is not fully met, this is to be specified in the description, and compensating countermeasures are to be proposed. The compensating countermeasures should the following: i) protect against the same threats as the original requirement, ii) provide an equal level of protection as the original requirement,	

Amended	Remarks
iii) not be a security control that is required by other requirements in this Chapter, and iv) not introduce a higher security risk. (f) Any supporting documents (e.g. OEM information) necessary to verify compliance with the requirements are to be referenced in the description and submitted. (4) Test procedure of security capabilities (a) This document is to describe how to demonstrate by testing that the system complies with the requirements in **4.4.2** and **4.4.3**, including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure is to include a separate chapter for each applicable requirement and describe the following: i) necessary test setup (i.e. to ensure the test can be repeated with the same expected result), ii) test equipment, iii) initial condition(s), iv) test methodology, detailed test steps, and v) expected results and acceptance criteria. (b) The procedure is to also include means to update test results and record findings during the testing. (5) Security configuration guidelines (a) This document is to 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 **Chapter 5** and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.) (b) The document is to serve as basis for verification of No.**29** in **Table X4.1**. (6) Secure development lifecycle documents This documentation is to be submitted to the Society upon request and is to be describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in **4.5**. Software updates and patching are to be described. The document is to prepare the Society for survey as per **2.2.2-5**. (7) Plans for maintenance and verification of the computer-based system This document is to be submitted to the Society upon request and is to include procedures for security-related maintenance and testing of the system. The document is to include instructions for how the user can verify correct operation of the system's security functions as required by No.**19** in **Table X4.1**. (8) Information supporting the owner’s incident response and recovery plan This document is to be submitted to the Society upon request and is to include procedures or instructions allowing the user to accomplish the following: (a) local independent control (see **5.4.5(2)**),	

Amended	Remarks
(b) network isolation (see **5.4.5(3)**), (c) forensics by use of audit records (see No.**13** in **Table X4.1**), (d) deterministic output (see **5.4.5(4)** and No.**20** in **Table X4.1**), (e) backup (see No.**26** in **Table X4.1**), (f) restore (see No.**27** in **Table X4.1**), and (g) controlled shutdown, reset, roll-back and restart (see **5.4.6(3)**). (9) Management of change plan This document is to be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by **Chapter 3**. (10) Test reports Computer-based systems with Type approval certificate covering the security capabilities of this Chapter may be exempted from survey by the Society. However, test reports signed by the supplier are to 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 (**4.6.3** and **2.2.3**).	
4.4.2 Required Security Capabilities* The security capabilities specified in **Table X4.1** are required for computer-based systems in the scope specified in **4.1.2**. The requirements in **Table X4.1** are based on the selected requirements in *IEC* 62443-3-3. To determine the full content, rationale and relevant guidance for each requirement, the reader should consult the referenced standard. In this table, "*IEC* 62443-3-3/SR x.x" as used (where x is a number) indicates that it is related to the corresponding SR (System requirement) specified in the following *IEC* standards: ・ *IEC* 62443-3-3:2013 (Industrial Communication Networks, Network and System Security, Part 3-3: System security requirements and security levels)	E27(Rev.1) 4.1

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X4.1 Required Security Capabilities	E27(Rev.1) 4.1 Table 1

Table X4.1 Required Security Capabilities

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

Amended					Remarks
		mobile devices	- limit the use of portable and mobile devices only to those permitted by design, and - restrict code and mobile devices. (IEC 62443-3-3/SR 2.3)		
	11	Mobile code	The computer-based system is to control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)		
	12	Session lock	The computer-based system is to be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)		
	13	Auditable events	The computer-based system is to generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)		
	14	Audit storage capacity	The computer-based system is to provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms are to be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)		
	15	Response to audit processing failures	The computer-based system is to provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)		
	16	Timestamps	The computer-based system is to timestamp audit records. (IEC 62443-3-3/SR 2.11)		
	Protect the integrity of the computer-based system against casual or coincidental manipulation				
	17	Communication integrity	The computer-based system is to protect the integrity of transmitted information. (IEC 62443-3-3/SR 3.1)		
	18	Malicious code protection	The computer-based system is to provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It is to have the feature for updating the protection mechanisms. (IEC 62443-3-3/SR 3.2)		
	19	Security functionality verification	The computer-based system is to provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance. (IEC 62443-3-3/SR 3.3)		
	20	Deterministic output	The computer-based system is to provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be the following: - unpowered state,		

Amended					Remarks
			- last-known value, or - fixed value. (IEC 62443-3-3/SR 3.6)		
	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure				
	21	Information confidentiality	The computer-based system is to provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. (IEC 62443-3-3/SR 4.1)		
	22	Use of cryptograph	If cryptography is used, the computer-based system is to use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (IEC 62443-3-3/SR 4.3)		
	Monitor the operation of the computer-based system and respond to incidents				
	23	Audit log accessibility	The computer-based system is to provide the capability for accessing audit logs on read only basis by authorized humans and/or tools. (IEC 62443-3-3/SR 6.1)		
	Ensure that the control system operates reliably under normal production conditions				
	24	Denial of service protection	The computer-based system is to provide the minimum capability to maintain essential functions during DoS events. (IEC 62443-3-3/SR 7.1)		
	25	Resource management	The computer-based system is to provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)		
	26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) are to be supported by the computer-based system without affecting normal operations. (IEC 62443-3-3/SR 7.3)		
	27	System recovery and reconstitution	The computer-based system is to provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)		
	28	Alternative power source	The computer-based system is to provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)		
	29	Network and security configuration settings	The computer-based system traffic is to provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The computer-based system is to provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)		
	30	Least	The installation, the availability and the access rights of the following are to be limited to		

<table>
<tr><th>Amended</th><th>Remarks</th></tr>
<tr><td>
<table>
<tr><td></td><td>Functionality</td><td>the strict needs of the functions provided by the computer-based system:
- operating systems software components, processes and services
- network services, ports, protocols, routes and hosts accesses and any software
(<i>IEC</i> 62443-3-3/SR 7.7)</td></tr>
</table>

<b>4.4.3 Additional Security Capabilities</b>
<b>1</b> The security capabilities specified in <b>Table X4.2</b> are Required for computer-based systems with network communication to untrusted networks (i.e. interface to any networks outside the scope of this chapter). In <b>Table X4.2</b>, “<i>IEC</i> 62443-3-3/SR x.x, RE x.x” as used (where x is a number) indicates the RE (Requirement enhancement) related to the relevant SR (System requirement).
<b>2</b> Computer-based systems with communication traversing the boundaries of security zones are also to meet requirements for network segmentation and zone boundary protection in <b>5.4.3(1)</b> and <b>(2)</b>.
</td><td>

E27(Rev.1) 4.2</td></tr>
</table>

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
Table X4.2 Additional Security Capabilities	E27(Rev.1) 4.2 Table 2

Item No	**Objective**	**Requirements**
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the computer-based system from or via an untrusted network. (*IEC* 62443-3-3/SR 1.1, RE 2)
32	Software process and device identification and authentication	The computer-based system is to identify and authenticate software processes and devices. (*IEC* 62443-3-3/SR 1.2)
33	Unsuccessful login attempts	The computer-based system is to enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (*IEC* 62443-3-3/SR 1.11)
34	System use notification	The computer-based system is to provide the capability to display a system use notification message before authenticating. The system use notification message is to be configurable by authorized personnel. (*IEC* 62443-3-3/SR 1.12)
35	Access via Untrusted Networks	Any access to the computer-based system from or via untrusted networks are to be monitored and controlled. (*IEC* 62443-3-3/SR 1.13)
36	Explicit access request approval	The computer-based system is to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (*IEC* 62443-3-3/SR 1.13, RE1)
37	Remote session termination	The computer-based system is to provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (*IEC* 62443-3-3/SR 2.6)
38	Cryptographic integrity protection	The computer-based system is to employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (*IEC* 62443-3-3/SR 3.1, RE1)
39	Input validation	The computer-based system is to validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the computer-based system. (*IEC* 62443-3-3/SR 3.5)
40	Session integrity	The computer-based system is to protect the integrity of sessions. Invalid session IDs are to be rejected. (*IEC* 62443-3-3/SR 3.8)
41	Invalidation of session IDs after	The system is to invalidate session IDs upon user logout or other session termination (including browser sessions).

	session termination	(*IEC* 62443-3-3/SR 3.8, RE1)

4.5 Secure Development Lifecycle Requirements

E27(Rev.1) 5.

4.5.1 Data to be Submitted

1 A Secure Development Lifecycle (SDLC) broadly addressing security aspects in the following stages is to 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, and

(7) end of life phase.

2 A document is to be produced that records how the security aspects have been addressed in above phases and is to at minimum integrate controlled processes as set out in below **4.5.2** to **4.5.2**. The said document is required to be submitted to class for review and approval. In this section, "*IEC* 62443-4-1" and subsequent statements are relevant to the following statements regarding security management (SM), security update management (SUM) or security guidelines (SG) specified in the IEC standards.

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

4.5.2 Control for Private Key (*IEC* 62443-4-1/SM-8)

The manufacturer is to have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.

4.5.3 Security Update Documentation (*IEC* 62443-4-1/SUM-2）

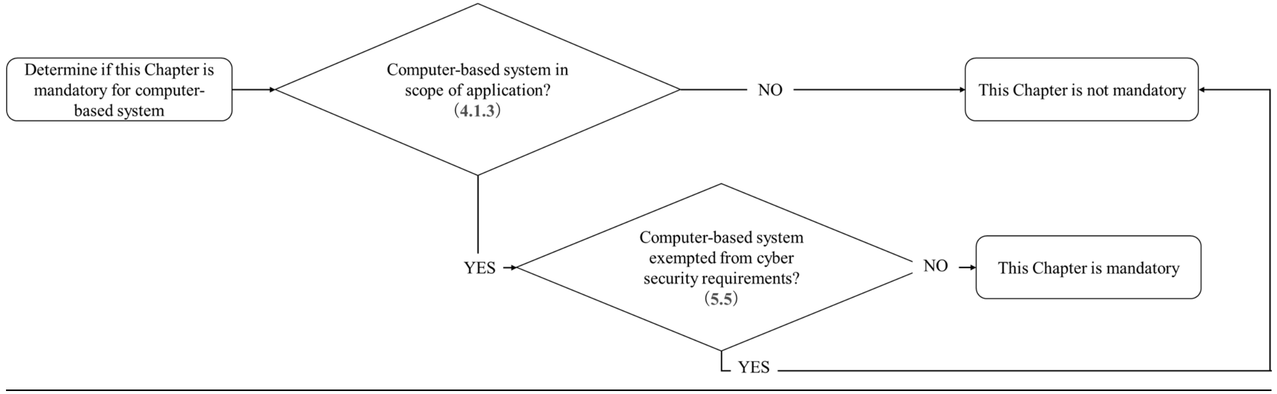
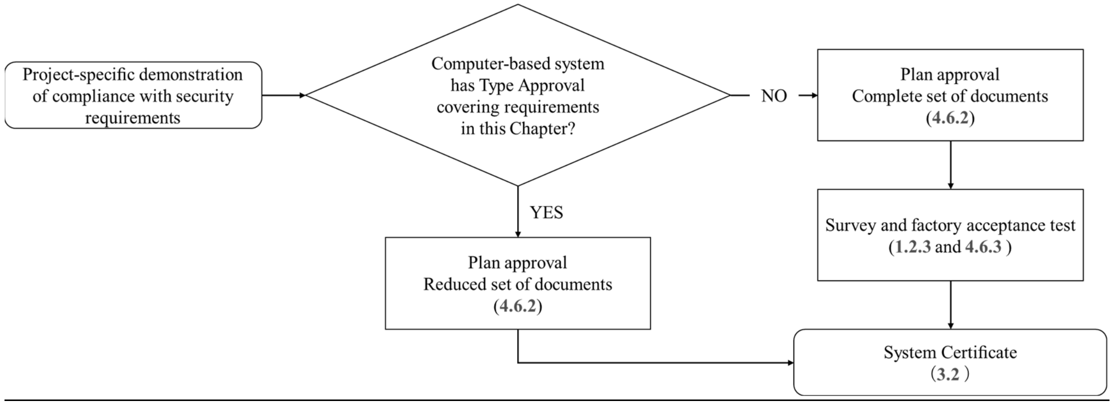
A process is to be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) that includes but is not limited to the following:

(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;

Amended	Remarks
(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. **4.5.4 Dependent Component or Operating System Security Update Documentation (*IEC* 62443-4-1/SUM-2）** A process is to be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to stating whether the product is compatible with the dependent component or operating system security update. **4.5.5 Security Update Delivery (*IEC* 62443-4-1/SUM-4)** A process is to 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. The manufacturer is to have QA process to test the updates before releasing. **4.5.6 Product Defence in Depth (*IEC* 62443-4-1/SG-1)** A process is to exist to create product documentation that describes the security defence in depth strategy for the product to support installation, operation and maintenance that includes the following: (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. **4.5.7 Defence in Depth Measure Expected in the Environment (*IEC* 62443-4-1/SG-2)** A process is to 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. **4.5.8 Security Hardening Guidelines (*IEC* 62443-4-1/SG-3)** A process is to be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines are to 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	

Amended	Remarks
(4) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability for the following: (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.	
4.6 Demonstration of Compliance	E27(Rev.1) 6.
4.6.1 Introduction **1** Suppliers are to in cooperation with the System integrator determine if this Chapter is mandatory for the computer-based system, see **Fig. X4.1**. **2** Compliance with security requirements is to be demonstrated as indicated in **Fig. X4.2**. This classification process is ship-specific and is to result in a System certificate. **3** Type approval based on **Chapter 10, Part 7 of Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use** is voluntary and applies for computer-based systems that are standard and routinely manufactured. See **3.2.1** and **3.2.2**for definition of System certification and Type approval. **4** The process in **Fig. X4.1** and **Fig. X4.2** applies also if other equivalent standards are applied for navigation and radiocommunication equipment (see **4.1.2**). In such case, the process in **Fig. X4.1** illustrates if the equivalent standard is mandatory (in lieu of this Chapter) and the process in **Fig. X4.2** illustrates that the certification process is lessened if the computer-based system has been type approved in accordance with the equivalent standard.	E27(Rev.1) 6.1

Amended	Remarks
Fig. X4.1　Determination of Application  Determine if this Chapter is mandatory for computer-based system Computer-based system in scope of application? (4.1.3) NO This Chapter is not mandatory YES Computer-based system exempted from cyber security requirements? (5.5) NO This Chapter is mandatory YES	E27(Rev.1) Figure 1
Fig. X4.2　Compliance with Security Requirements  Project-specific demonstration of compliance with security requirements Computer-based system has Type Approval covering requirements in this Chapter? NO Plan approval Complete set of documents (4.6.2) Survey and factory acceptance test (1.2.3 and 4.6.3) YES Plan approval Reduced set of documents (4.6.2) System Certificate (3.2)	E27(Rev.1) Figure 2

Amended	Remarks
4.6.2 Plan Approval **1** Plan approval is assessment of documents of a computer-based system intended for a specific vessel. The documents in **2.2.3** are required to be submitted by the supplier. The documents are to enable the Society to verify compliance with requirements in this Chapter. **2** If the computer-based system holds a valid Type approval certificate covering the requirements of this Chapter, subject to approval by the Society, the supplier may submit a reduced set of vessel-specific documents to the Society (see **Table X1.3**). **3** The approved version of the documents are to be included in the delivery of the computer-based system to the system integrator.	E27(Rev.1) 6.2
4.6.3 Survey and Factory Acceptance Test **1** Survey and factory acceptance test is a vessel-specific verification activity required for computer-based systems that do not hold a valid Type approval certificate covering the requirements of this Chapter. **2** The objective of the survey and factory acceptance test is to demonstrate by testing and/or analytic evaluation that the computer-based system complies with applicable requirements in this Chapter. The survey and factory acceptance test is to be carried out at the supplier's premises or at other works having the adequate apparatus for testing and inspection. **3** After completed plan approval and survey/factory acceptance test, the Society will issue a System certificate that is to accompany the computer-based system upon delivery to the system integrator.	E27(Rev.1) 6.3

Amended	Remarks
Chapter 5 CYBER RESILIENCE OF SHIPS **5.1 General**	E27(Rev.1) was incorporated.
5.1.1 Aim* **1** The aim of this Chapter 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 Chapter targets the ship as a collective entity for cyber resilience and is intended as a base for the complementary application of other requirements and industry standards addressing cyber resilience of onboard systems, equipment and components. **3** Minimum requirements for cyber resilience of on-board systems and equipment are given in **Chapter 4**.	E26(Rev.1) 1.2
5.1.2 Scope **1** The requirements in this Chapter are applicable for computer-based systems subject to **4.1.2**. **2** The cyber incidents considered in this Chapter are events resulting from any offensive manoeuvre that targets OT systems onboard ships as defined in **5.2**.	E26(Rev.1) 1.3 Chapter 4 was referred because scope of chapter 5 is the same as chapter 4 which incorporated E27(Rev.1).
5.1.3 System Category System categories are defined in **3.3.1** on the basis of the consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.	E26(Rev.1) 1.3.3
5.1.4 Relative requirements on Computer Based Systems and Cyber Resilience Attention is made to relative requirements on computer-based systems and Cyber Resilience as follows: (1) **Chapter 3** "Computer Based Systems" (2) **Chapter 4** "Cyber Resilience of On-board Systems and Equipment" (3) *IACS* Recommendation 166 Recommendation on Cyber Resilience: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life. *IACS* Recommendation 166 on Cyber Resilience is intended for ships contracted for construction after its publication and may be used as a reference for ships already in service prior to its publication. For ships to which this Chapter applies as mandatory instrument, when both this Chapter and	E26(Rev.1) 1.3.4

Amended	Remarks
Recommendation 166 are used, should any difference in requirements addressing the same topic be found between the two instruments, the requirements in this Chapter is to prevail.	
5.2 Definitions	E26(Rev.1) 2.
5.2.1 Terminology* The terminology used in this Chapter is as specified in the following **(1)** to **(23)**: (1) "Annual Survey" means the survey consist of general examinations of hull, machinery, equipment, fire-fighting equipment, etc. as specified in **Chapter 3, Part B**. (2) "Attack Surface" means 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" means provision of assurance that a claimed characteristic of an entity is correct. (4) "Compensating countermeasure" means an alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements. (5) "Computer-based System" means 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. computer-based systems onboard include IT and OT systems. A computer-based system may be a combination of subsystems connected via network. Onboard computer-based systems may be connected directly or via public means of communications (e.g. Internet) to ashore computer-based systems, other vessels' computer-based systems and/or other facilities. (6) "Cyber incident" means an event resulting from any offensive manoeuvre, either intentional or unintentional, that targets or affects one or more computer-based system onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based system or transported in the networks connecting such systems. Cyber incidents do not include system failures. (7) "Cyber resilience" means 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	

Amended	Remarks
potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. (8) “Essential services” mean 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. (9) “Information Technology (IT)” mean devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT). (10) “Integrated system” means a system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes. (11) “Logical network segment” is the same as “Network segment”, but where two or more logical network segments share the same physical components. (12) “Network” means a connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols. (13) “Network segment” means in the context of this Chapter, a network segment is an OSI layer-2 Ethernet segment (a broadcast domain). (14) “Operational Technology (OT)” means 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. (15) “Physical network segment” is the same as “Network segment”, but where physical components are not shared by other network segments. (16) “Protocol:” means a common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various fieldbuses. (17) “Security zone” means a collection of computer-based systems in the scope of applicability of this Chapter 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. (18) “Shipowner/Company” means 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. (19) “Special Survey” is the survey consist of detailed examinations of hull, machinery, equipment, fire-fighting equipment,	

Amended	Remarks
etc. as specified in **Chapter 5, Part B**. (20) “Supplier” means 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. (21) “Systems Integrator” means 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 is to be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility. (22) “Untrusted network” means any network outside the scope of applicability of this Chapter.	
(23) “Roll-back” is an operation which returns the system to some previous state	(23) is NK original
5.3 Goals and Organization of Requirements	E26(Rev.1) 3.
5.3.1 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 **5.3.2** below.	E26(Rev.1) 3.1
5.3.2 Sub-goals per Functional Element Following sub-goals and relevant functional elements should be concurrent and considered as parts of a single comprehensive risk management framework. **1** Identify Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities. **2** Protect Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations. **3** Detect Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard. **4** Respond	E26(Rev.1) 3.2

Amended	Remarks
Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard. 5 Recover Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident. **5.3.3 Organization of Requirements** The requirements specified in this chapter are structured as follows: (1) The requirements are organized according to a goal-based approach. (2) Functional/technical requirements are given for the achievement of specific sub-goals of each functional element as specified in **5.3.2**. (3) 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. (4) For each requirement, a rationale is given. (5) A summary of actions to be carried out and documentation to be made available is also given for each phase of the ship's life and relevant stakeholders participating to such phase.	E26(Rev.1) 3.3
5.4 Requirements for Cyber Resilience of Ships **5.4.1 General** This section contains the requirements to be satisfied in order to achieve the primary goal defined in **5.3.1**, organized according to the five functional elements identified in **5.3.2**. The requirements are to 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 **5.2** for definitions). Whilst the above requirements may be fulfilled by these stakeholders, for the purposes of this Chapter, responsibility to fulfil them will lie with the stakeholder who has contracted with the Society. (1) Shipowner/Company (2) Systems integrator (3) Supplier (4) Classification Society	E26(Rev.1) 4.
5.4.2 Identify The requirements for the "Identify" functional element are aimed at identifying, on one side, the computer-based	E26(Rev.1) 4.1

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Remarks
systems onboard, their interdependencies and the relevant information flows; and, on the other side, the key resources involved in their management, operation and governance, their roles and responsibilities.	
(1) Vessel asset inventory (a) Requirement An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the computer-based systems in the scope of applicability of this Chapter and of the networks connecting such systems to each other and to other computer-based systems onboard or ashore are to be provided and kept up to date during the entire life of the ship. (b) Rationale The inventory of computer-based systems onboard and relevant software used in OT systems, is essential for an effective management of cyber resilience of the ship, the main reason being that every computer-based system becomes a potential point of vulnerability. Cybercriminals can exploit unaccounted and out-of- date hardware and software to hack systems. Moreover, managing computer-based system assets enables Companies understand the criticality of each system to ship safety objectives. (c) Requirement details The vessel asset inventory is to include at least the computer-based systems indicated in **5.1.2-1.**, if present onboard. The inventory is to 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 are to be recorded in the inventory. If confidential information is included in the inventory (e.g. IP addresses, protocols, port numbers), special measures are to be adopted to limit the access to such information only to authorized people. i) Hardware 1) For all hardware devices in the scope of applicability of this Chapter, the vessel asset inventory is to include at least the information in **4.4.1(1)**. 2) In addition, the vessel asset inventory may specify system category and security zone associated with the computer-based system. ii) Software 1) For all software in the scope of applicability of this Chapter (e.g., application program, operating system, firmware), the vessel asset inventory is to include at least the information in **4.4.1(1)**. 2) The software of the computer-based systems in the scope of applicability of this Chapter are to 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 **2.2.3-5(7)**) (d) Demonstration of compliance	E26(Rev.1) 4.1.1

Amended	Remarks
i) Design phase 1) The systems integrator is to submit vessel asset inventory to the Society (see **2.2.3-4**). 2) The vessel asset inventory is to incorporate the asset inventories of all individual computer-based systems falling under the scope of this Chapter. Any equipment in the scope of this Chapter delivered by the systems integrator is also to be included in the vessel asset inventory. ii) Construction phase The systems integrator is to keep the vessel asset inventory updated. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society: 1) vessel asset inventory is updated and completed at delivery, 2) computer-based systems in the scope of applicability of this Chapter are correctly represented by the vessel asset inventory, and 3) software of the computer-based systems in the scope of applicability of this Chapter has been kept updated, e.g. by vulnerability scanning or by checking the software versions of computer-based systems while switched on. iv) Operation phase 1) For general requirements to surveys in the operation phase (see **2.2.3-5**). 2) The shipowner is to in the Ship cyber security and resilience program describe the process of management of change (MoC) for the computer-based systems in the scope of applicability of this Chapter, addressing at least the following requirements in this Chapter: - management of change (**2.2.3-5**), and - hardware and software modifications (**5.4.2(1)(c)**). 3) The shipowner is to 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 (**5.4.2(1)(b)** and **(c)**), and - security patching (**5.4.3(6)(c)iii)2)**). 4) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - the approved management of change process has been adhered to, - known vulnerabilities and functional dependencies have been considered for the software in the computer-based systems, and	

Amended	Remarks
- the Vessel asset inventory has been kept updated. 5) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey. 6) Special Survey The shipowner is to demonstrate to the Society the activities in **5.4.2(1)(d)iii)** as per the Ship cyber resilience test procedure.	
5.4.3 Protect* The requirements for the Protect functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential incident.	E26(Rev.1) 4.2
(1) Security zones and network segmentation (a) Requirement i) All computer-based systems in the scope of applicability of this Chapter are to be grouped into security zones with well-defined security policies and security capabilities. Security zones are to 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.) ii) Only explicitly allowed traffic are to traverse a security zone boundary. (b) Rationale i) 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. ii) The main benefits of security zones and network segmentation are to reduce the extent of the attack surface, prevent attackers from achieving lateral movement through systems, and improve network performance. The concept of allocating the computer-based systems into security zones allows grouping the computer-based systems in accordance with their risk profile. (c) Requirement details i) A security zone may contain multiple computer-based systems and networks, all of which are to comply with applicable security requirements given in this Chapter and **Chapter 4**. ii) The network(s) of a security zone are to be logically or physically segmented from other zones or networks (see also **5.4.3(6)(c)**). iii) Computer-based systems providing required safety functions are to be grouped into separate security zones	E26(Rev.1) 4.2.1

Amended	Remarks
and are to be physically segmented from other security zones. iv) Navigational and communication systems are not to be in same security zone as machinery or cargo systems. If navigation and/or radiocommunication systems are approved in accordance with other equivalent standard(s) (see **4.1.2-2(1)(k)**), these systems should be in a dedicated security zone. v) Wireless devices are to be in dedicated security zones (see also **5.4.3(5)**). vi) Systems, networks or computer-based systems outside the scope of applicability of this Chapter are considered untrusted networks and are to 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. vii) It is to be possible to isolate a security zone without affecting the primary functionality of the computer-based systems in the zone (see also **5.4.5(3)**). (d) Demonstration of compliance i) Design phase 1) The systems integrator is to submit Zones and conduit diagram and the Cyber security design description (see **2.2.3-3(4)** and **(5)**). 2) The Zones and conduit diagram is to illustrate the computer-based systems in the scope of applicability of this Chapter, how they are grouped into security zones, and include the following information: - clear indication of the security zones, - simplified illustration of each computer-based system in scope of applicability of this Chapter, and indication of the security zone in which the computer-based system is allocated, and indication of physical location of the computer-based system/equipment, - reference to the approved version of the computer-based system topology diagrams provided by the suppliers (**4.4.1(2)**), - illustration of network communication between systems in a security zone - illustration of any network communication between systems in different security zones (conduits), and - illustration of any communication between systems in a security zone and untrusted networks (conduits). 3) The systems integrator is to include the following information in the cyber security design description: - a short description of the computer-based systems allocated to the security zone. It is to be possible to identify each computer-based system in the Zones and conduit diagram, - network communication between computer-based systems in the same security zone. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication, - network communication between computer-based systems in different security zones. The description	

Amended	Remarks
is to include purpose and characteristics (i.e. protocols and data flows) of the communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules), and - any communication between computer-based systems in security zones and untrusted networks. The description is to include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description is to also include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules). ii) Construction phase The systems integrator is to keep the Zones and conduit diagram updated. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society: 1) The security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design. 2) Security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to 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 (**5.4.3(2)(a)**), - explicitly allowed traffic (**5.4.3(1)(a)**), - protection against denial of service (DoS) events (**5.4.3(2)(a)**), and - inspection of security audit records (**5.4.4(1)(c)**). 2) First Annual Survey The shipowner is to demonstrate to the Society that the Zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.	

Amended	Remarks
3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey. 4) Special Survey The shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(2) Network protection safeguards (a) Requirement i) Security zones are to be protected by firewalls or equivalent means as specified in **5.1.1**. ii) The networks are to also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources. iii) The computer-based systems in scope of this Chapter are to be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited. (b) Rationale i) 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. ii) 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. iii) While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour. (c) Requirement details The design of network are to include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate is to at least consider the capacity of network, data speed requirement for intended application and data format. (d) Demonstration of compliance i) Design phase No requirements. ii) Construction phase	E26(Rev.1) 4.2.2

Amended	Remarks
No requirements. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society. The tests specified in **2)** and **3)** may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. 1) Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable. 2) Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests are to cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network) 3) Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the computer-based systems have been removed or prohibited in accordance with hardening guidelines provided by the suppliers (see **4.5.8** and **2.2.2-5(7)**). iv) Operation phase 1) For general requirements to surveys in the operation phase (see **2.2.3-5**). 2) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(3) Antivirus, antimalware, antispam and other protections from malicious code (a) Requirement Computer-based systems in the scope of applicability of this Chapter are to be protected against malicious code such as viruses, worms, trojan horses, spyware, etc. (b) Rationale i) A virus or any unwanted program that enters a user’s system without his/her knowledge can self-replicate and spread, perform unwanted and malicious actions that end up affecting the system’s performance, user’s data/files, and/or circumvent data security measures. ii) Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off the malicious intruding viruses performing a prophylactic function. It detects potential virus and then works to remove it, mostly before the virus gets to harm the system. iii) Common means for malicious code to enter computer-based systems are electronic mail, electronic mail attachments, websites, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops. (c) Requirement details	E26(Rev.1) 4.2.3

Amended	Remarks
i) Malware protection is to be implemented on computer-based systems in the scope of applicability of this Chapter. On computer-based systems having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software is to be installed, maintained and regularly updated, unless the installation of such software impairs the ability of computer-based system to provide the functionality and level of service required (e.g. for Category II and Category III computer-based systems performing real-time tasks). ii) On computer-based systems where anti-virus and anti-malware software cannot be installed, malware protection is to be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations. (d) Demonstration of compliance i) Design phase The systems integrator is to include the following information in the Cyber security design description: 1) For each computer-based system, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software. 2) For computer-based systems with anti-malware software, information about how to keep the software updated. 3) Any operational conditions or necessary physical safeguards to be implemented in the shipowner's management system. ii) Construction phase The systems integrator is to ensure that malware protection is kept updated during the construction phase. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. 1) Approved anti-malware software or other compensating countermeasures is effective (e.g. test with a trustworthy anti-malware test file). iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to 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 (**5.4.3(3)(c)**) - Operational procedures, physical safeguards (**5.4.3(3)(c)**) - Use of mobile, portable, removable media (**5.4.3(4)(c)iv**） and **5.4.3(7)(c)**)	

Amended	Remarks
- Access control (**5.4.3(4)**) 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - any anti-malware software has been maintained and updated, - procedures for use of portable, mobile or removable devices have been followed, - policies and procedures for access control have been followed, and - physical safeguards are maintained. 3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey. 4) Special Survey The shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(4) Access control (a) Requirement Computer-based systems and networks in the scope of applicability of this Chapter are to provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures are to be such as not to hamper the ability of authorized personnel to access computer-based system for their level of access according to the least privilege principle. (b) Rationale i) Attackers may attempt to access the ship's systems and data from either onboard the ship, within the company, or remotely through connectivity with the internet. Physical and logical access controls to cyber assets, networks etc. should then be implemented to ensure safety of the ship and its cargo. ii) Physical threats and relevant countermeasures are also considered in the ISPS Code. Similarly, the ISM Code contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of ISPS and ISM Codes may imply inclusion in the Ship Security Plan (SSP) and Safety Management System (SMS) of instructions and procedures for access control to safety critical assets. (c) Requirement details Access to computer-based systems and networks in the scope of applicability of this Chapter and all information	E26(Rev.1) 4.2.4

Amended	Remarks
stored on such systems are to only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality. i) Physical access control Computer-based systems of Category II and Category III are to generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access or are to be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles are to be however easy to access to the crew and various stakeholders who need to access to computer-based systems for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship. ii) Physical access control for visitors Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives are to be restricted regarding access to computer-based systems onboard whilst on board, e.g. by allowing access under supervision. iii) Physical access control of network access points Access points to onboard networks connecting Category II and/or Category III computer-based systems are to be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance. Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, are to be used in case of occasional connection requested by a visitor (e.g. for printing documents). iv) Removable media controls A policy for the use of removable media devices are to 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 **5.4.3(7)**). v) Management of credentials 1) Computer-based systems and relevant information are to be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel are to be left active only for a limited period according to the role and responsibility of the account holder and are to be removed when no longer needed. 2) Onboard computer-based systems are to be provided with appropriate access control that fits to the policy of their Security Zone but does not adversely affect their primary purpose. computer-based systems which require strong access control may need to be secured using a strong encryption key or multi-factor authentication.	

Amended	Remarks
3) Administrator privileges are to be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the computer-based system, who as part of their role in the company or onboard need to log on to systems using these privileges. vi) Least privilege principle 1) Any human user allowed to access computer-based system and networks in the scope of applicability of this Chapter are to have only the bare minimum privileges necessary to perform its function. 2) The default configuration for all new account privileges are to be set as low as possible. Wherever possible, raised privileges are to 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 are to be avoided, e.g. by regular auditing of user accounts. (d) Demonstration of compliance i) Design phase The systems integrator is to include the information related to location and physical access controls for the computer-based systems in the Cyber security design description. 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 are to be specified. ii) Construction phase The systems integrator is to prevent unauthorised access to the computer-based systems during the construction phase. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society: 1) Components of the computer-based systems are located in areas or enclosures where physical access can be controlled to authorised personnel. 2) User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of computer-based systems as per **2.2.3-4(2)**) iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to 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 (**5.4.3(4)(c)i)**),	

Amended	Remarks
- physical access control for visitors (**5.4.3(4)(c)ii)**), - physical access control of network access points (**5.4.3(4)(c)iii)**), - management of credentials (**5.4.3(4)(c)v)**), and - least privilege policy (**5.4.3(4)(c)vi)**). 2) The shipowner is to 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 (**5.4.2(1)(c)**), - information allowed to authorized personnel (**5.4.3(4)(c)**), and - information transmitted on the wireless network (**5.4.3(5)(c)**). 3) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - Personnel are authorized to access the computer-based systems in accordance with their responsibilities. - Only authorised devices are connected to the computer-based systems. - Visitors are given access to the computer-based systems according to relevant policies and procedures. - Physical access controls are maintained and applied. - Credentials, keys, secrets, certificates, relevant computer-based system documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures. 4) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey.	
(5) Wireless communication (a) Requirement Wireless communication networks in the scope of this Chapter are to be designed, implemented and maintained to ensure the following: i) cyber incidents will not propagate to other control systems. ii) only authorised human users will gain access to the wireless network. iii) only authorised processes and devices will be allowed to communicate on the wireless network. iv) information in transit on the wireless network cannot be manipulated or disclosed. (b) Rationale i) Wireless networks give rise to additional or different cybersecurity risks than wired networks. This is mainly	E26(Rev.1) 4.2.5

Amended	Remarks
due to less physical protection of the devices and the use of the radio frequency communication. ii) Inadequate physical access control may lead to unauthorised personnel gaining access to the physical devices, which in turn could lead to circumventing logical access restrictions or deployment of rogue devices on the network. iii) Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn could cater for attacks such as Piggybacking or Evil twin attacks (see https://us-cert.cisa.gov/ncas/tips/ST05-003). (c) Requirement details i) Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices are to be applied to ensure integrity and confidentiality of the information transmitted on the wireless network. ii) Devices on the wireless network are to only communicate on the wireless network (i.e. they are not to be “dual-homed”) iii) Wireless networks are to be designed as separate segments in accordance with **5.4.3(1)** and protected as per **5.4.3(2)**. iv) Wireless access points and other devices in the network are to be installed and configured such that access to the network can be controlled. v) The network device or system utilizing wireless communication is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication. (d) Demonstration of compliance i) Design phase The systems integrator is to include the description of wireless networks in the scope of applicability of this Chapter and how these are implemented as separate security zones in the Cyber security design description. The description is to include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules) ii) Construction phase The systems integrator is to prevent unauthorised access to the wireless networks during the construction phase. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. 1) Only authorised devices can access the wireless network.	

Amended	Remarks
2) Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).	
iv) Operation phase	
1) For general requirements to surveys in the operation phase (see **2.2.3-5**).	
2) Special Survey Subject to modifications of the wireless networks in the scope of applicability of this Chapter, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(6) Remote access control and communication with untrusted networks	E26(Rev.1) 4.2.6
(a) Requirement Computer-based systems in scope of this Chapter are to be protected against unauthorized access and other cyber threats from untrusted networks.	
(b) Rationale Onboard computer-based systems have become increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions. The use of digital systems to monitor and control onboard computer-based systems makes them vulnerable to cyber incidents. Attackers may attempt to access onboard computer-based systems through connectivity with the internet and may be able to make changes that affect a computer-based system’s operation or even achieve full control of the computer-based system or attempt to download information from the ship’s computer-based system. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects cyber resilience, special care should be put to relevant hardware and software installations on board to help maintain a sufficient level of cyber resilience when such systems can be remotely accessed, also keeping in mind that not all cyber incidents are a result of a deliberate attack.	
(c) Requirement details	
i) User’s manual is to be delivered for control of remote access to onboard IT and OT systems. Clear guidelines are to identify roles and permissions with functions.	
ii) For computer-based systems in the scope of applicability of this Chapter, no IP address is to be exposed to untrusted networks.	
iii) Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality are to be ensured for information that is subject to read authorization.	
1) Design Computer-based systems in the scope of applicability of this Chapter are to :	

Amended	Remarks
- have the capability to terminate a connection from the onboard connection endpoint. Any remote access are not to be possible until explicitly accepted by a responsible role on board. - be capable of managing interruptions during remote sessions so as not to compromise the safe functionality of OT systems or the integrity and availability of data used by OT systems. - provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident. 2) Additional requirements for remote maintenance When remote access is used for maintenance, the following requirements are to be complied with in addition to those in **1)**: - Documentation is to be provided to show how they connect and integrate with the shore side. - Security patches and software updates are to 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 are to be obtained, prior to undertaking remote update. - Suppliers are to provide plans for- and make security updates available to the shipowner (see **4.5.3**, **4.5.4** and **4.5.5**). - At any time, during remote maintenance activities, authorized personnel is to have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of the computer-based system and systems involved. - Multi-factor authentication is required for any access by human users to computer-based system's in scope from an untrusted network. - After a configurable number of failed remote access attempts, the next attempt is to be blocked for a predetermined length of time. - If the connection to the remote maintenance location is disrupted for some reason, access to the system is to be terminated by an automatic logout function. (d) Demonstration of compliance i) Design phase The systems integrator is to include the following information in the Cyber security design description: 1) Identification of each computer-based system 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. 2) For each computer-based system, a description of compliance with requirements in **5.4.3(6)c)**, as applicable	

Amended	Remarks
ii) Construction phase The systems integrator is to ensure that any communication with untrusted networks is only temporarily enabled and used in accordance with the requirements of this Chapter. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate the following to the Society: 1) Communication with untrusted networks is secured in accordance with **4.4.3** and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool). 2) Remote access requires multifactor authentication of the remote user. 3) A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established. 4) Remote connections must be explicitly accepted by responsible personnel on board. 5) Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity. 6) Remote sessions are logged (see No.**13** in **Table X4.1**). 7) Instructions or procedures are provided by the respective product suppliers (see **4.4.1(3)**). iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to 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 (**5.4.3(6)(c)**), - roles and permissions (**5.4.3(6)(c)**), - patches and updates (**5.4.3(6)(c)iii)2)**), - confirmation prior to undertaking remote software update (**5.4.3(6)(c)iii)2)**), and - interrupt, abort, roll back (**5.4.3(6)(c)iii)2)**). 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals, and - installation of security patches and other software updates have been carried out in accordance with	

Amended	Remarks

Management of change procedures and in cooperation with the supplier.

3) Subsequent Annual Survey

The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey.

4) Special Survey

The shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.

(7) Use of mobile and portable devices — E26(Rev.1) 4.2.7

(a) Requirement

The use of mobile and portable devices in computer-based systems in the scope of applicability of this Chapter are to be limited to only necessary activities and be controlled in accordance with No.**10** in **Table X4.1**. For any computer-based system that cannot fully meet these requirements, the interface ports are to be physically blocked.

(b) Rationale

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

(c) Requirement details

Mobile and portable devices are to only be used by authorised personnel. Only authorised devices may be connected to the computer-based systems. All use of such devices are to 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 computer-based system.

(d) Demonstration of compliance

i) Design phase

The systems integrator is to include the information related to any computer-based systems in the scope of applicability that do not meet the requirements in No.**10** in **Table X4.1**, i.e., that are to have protection of interface ports by physical means such as port blockers in the Cyber security design description.

ii) Construction phase

The systems integrator is to ensure that use of physical interface ports in the computer-based systems is controlled in accordance with No.**10** in **Table X4.1**, and that any use of such devices follows procedures to prevent malware from being introduced in the computer-based system.

iii) Commissioning phase

Amended	Remarks
The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures are to be demonstrated as relevant: 1) use of mobile and portable devices is restricted to authorised users, 2) interface ports can only be used by specific device types, 3) files cannot be transferred to the system from such devices, 4) files on such devices will not be automatically executed (by disabling autorun), 5) network access is limited to specific MAC or IP addresses, 6) unused interface ports are disabled, and 7) unused interface ports are physically blocked. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to 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 (**5.4.3(4)(c)iv)**), - physical block of interface ports (**5.4.3(7)(a)**), - use by authorized personnel (**5.4.3(7)(c)**), - connect only authorized devices (**5.4.3(7)(c)**), and - consider risk of introducing malware (**5.4.3(7)(c)**). 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures. - Only authorised devices are connected to the computer-based systems. - Means to restrict use of physical interface ports are implemented as per approved design documentation. 3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey. 4) Special Survey The shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test	

Amended	Remarks
procedure.	
5.4.4 Detect The requirements for the Detect functional element are aimed at the development and implementation of appropriate means supporting the ability to reveal and recognize anomalous activity on computer-based systems and networks onboard and identify cyber incidents.	E26(Rev.1) 4.3
(1) Network operation monitoring (a) Requirement Networks in scope of this Chapter are to be continuously monitored, and alarms are to be generated if malfunctions or reduced/degraded capacity occurs. (b) Rationale Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction could result in incidents where the vessel is 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. (c) Requirement details i) Measures to monitor networks in the scope of applicability of this Chapter are to have the following capabilities: 1) monitoring and protection against excessive traffic, 2) monitoring of network connections, 3) monitoring and recording of device management activities, 4) protection against connection of unauthorized devices, and 5) generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier (see **3.7.2-1**). ii) Intrusion detection systems (IDS) may be implemented, subject to the following: 1) The IDS is to be qualified by the supplier of the respective computer-based system 2) The IDS is to be passive and not activate protection functions that may affect the performance of the computer-based system 3) Relevant personnel should be trained and qualified for using the IDS (d) Demonstration of compliance i) Design phase No requirements.	E26(Rev.1) 4.3.1

Amended	Remarks
ii) Construction phase No requirements. iii) Commissioning phase 1) The systems integrator is to specify in the Ship cyber resilience test procedure and demonstrate to the Society the network monitoring and protection mechanisms in the computer-based systems. The following tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. - 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 **5.4.5(4)(d)iii)**. - Demonstrate that the computer-based system will respond in a safe manner to network storm scenarios, considering both unicast and broadcast messages (see also **5.4.3(2)(d)iii)**) - 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 computer-based systems. 2) Any Intrusion detection systems in the computer-based systems in scope of applicability to be implemented are to be subject to verification by the Society. Relevant documentation are to be submitted for approval, and survey/tests are to be carried out on board. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to in the Ship cyber security and resilience program describe the management activities to detect anomalies in the computer-based systems and networks, addressing at least the following requirements in this Chapter. The following activities may be addressed together with incident response in **5.4.5(1)**. - reveal and recognize anomalous activity (**5.4.4**), - inspection of security audit records (**5.4.4(1)(c)**), and - instructions or procedures to detect incidents (**5.4.5(1)(a)**). 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - The computer-based systems are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the computer-based systems. 3) Subsequent Annual Surveys	

Amended	Remarks
The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey. 4) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(2) Verification and diagnostic functions of computer-based system and networks (a) Requirement Computer-based systems and networks in the scope of applicability of this Chapter are to be capable to check performance and functionality of security functions required by this Chapter. Diagnostic functions are to provide adequate information on computer-based systems integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship. (b) Rationale The ability to verify intended operation of the security functions is important to support management of cyber resilience in the lifetime of the ship. Tools for diagnostic functions may comprise automatic or manual functions such as self-diagnostics capabilities of each device, or tools for network monitoring (such as ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap, etc.). It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the computer-based system. (c) Requirement details Computer-based systems and networks' diagnostics functionality are to be available to verify the intended operation of all required security functions during test and maintenance phases of the ship. (d) Demonstration of compliance i) Design phase No requirements. ii) Construction phase No requirements. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society the effectiveness of the procedures for verification of security functions provided by the suppliers. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**).	E26(Rev.1) 4.3.2

Amended	Remarks
1) The shipowner is to in the Ship cyber security and resilience program describe the management activities to verify correct operation of the security functions in the computer-based systems and networks, addressing at least the following requirements in this Chapter: - test and maintenance periods (**5.4.4(2)(c)**) and - periodic maintenance (**2.2.3-5(9)**). 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - The security functions in the computer-based systems are periodically tested or verified. 3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey.	
5.4.5 Respond The requirements for the Respond functional element are aimed at the development and implementation of appropriate means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of computer-based systems and networks onboard.	E26(Rev.1) 4.4
(1) Incident response plan (a) Requirement An incident response plan is to be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan is to contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against computer-based systems in the scope of applicability of this Chapter. (b) Rationale An incident response plan is an instrument aimed to help responsible persons respond to cyber incidents. As such, the Incident response plan is as effective as it is simple and carefully designed. When developing the Incident response plan, it is important to understand the significance of any cyber incident and prioritize response actions accordingly. Means for maintaining as much as possible the functionality and a level of service for a safe operation of the ship, e.g. transfer active execution to a standby redundant unit, should also be indicated. Designated personnel ashore should be integrated with the ship in the event of a cyber incident. (c) Requirement details i) The various stakeholders involved in the design and construction phases of the ship are to provide information to the shipowner for the preparation of the Incident Response Plan to be placed onboard at the first Annual	E26(Rev.1) 4.4.1

Amended	Remarks
Survey. ii) The Incident Response Plan is to be kept up-to-date (e.g. upon maintenance) during the operational life of the ship. The Incident response plan is to be provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin. iii) The incident response plan is to, as a minimum, include the following information. The Incident response plan is to be kept in hard copy in the event of complete loss of electronic devices enabling access to it. 1) Breakpoints for the isolation of compromised systems 2) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events 3) A description of expected major consequences related to cyber incidents 4) Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any 5) Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable (d) Demonstration of compliance i) Design phase The systems integrator is to include the references to information provided by the suppliers (see **4.4.1(8)**) that may be applied by the shipowner to establish plans for incident response in the Cyber security design description. ii) Construction phase No requirements. iii) Commissioning phase No requirements. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to in the Ship cyber security and resilience program describe incident response plans. The plans are to cover the computer-based systems in scope of applicability of this Chapter and are to 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 **5.4.5(1)** - Procedures or instructions for local/manual control in accordance with requirements in **5.4.5(2)** - Procedures or instructions for isolation of security zones in accordance with requirements in **5.4.5(3)**	

Amended	Remarks
- Description of expected behaviour of the computer-based systems in the event of cyber incidents in accordance with requirements in **5.4.5(4)** 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - The incident response plans are available for the responsible personnel onboard. - Procedures or instructions for local/manual controls are available for responsible personnel onboard. - Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard. - Any cyber incidents have been responded to in accordance with the incident response plans. 3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey.	
(2) Local, independent and/or manual operation (a) Requirement Any computer-based system needed for local backup control as required by Regulation 31, Chapter II-1, *SOLAS* are to be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation. (b) Rationale Independent local controls of machinery and equipment needed to maintain safe operation is a fundamental principle for manned vessels. The objective of this requirement has traditionally been to ensure that personnel can cope with failures and other incidents by performing manual operations in close vicinity of the machinery. Since incidents caused by malicious cyber events should also be considered, this principle of independent local control is no less important. (c) Requirement details i) The computer-based system for local control and monitoring are to be self-contained and not depend on communication with other computer-based system for its intended operation. ii) If communication to the remote control system or other computer-based system's is arranged by networks, segmentation and protection safeguards as described in **5.4.3(1)** and **5.4.3(2)** are to be implemented. This implies that the local control and monitoring system are to be considered a separate security zone. Notwithstanding the above, special considerations can be given to computer-based systems with different concepts on case by case basis.	E26(Rev.1) 4.4.2

Amended	Remarks
iii) The computer-based system for local control and monitoring are to otherwise comply with requirements in this Chapter.	
(d) Demonstration of compliance	
i) Design phase The systems integrator is to include the description of how the local controls specified in Regulation 31, Chapter II-1, *SOLAS* are protected from cyber incidents in any connected remote or automatic control systems in the Cyber security design description.	
ii) Construction phase No requirements.	
iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the 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. The tests are to be carried out by disconnecting all networks from the local control system to other systems/devices. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**.	
iv) Operation phase	
1) For general requirements to surveys in the operation phase, (see **2.2.3-5**).	
2) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(3) Network isolation	E26(Rev.1) 4.4.3
(a) Requirement It is to be possible to terminate network-based communication to or from a security zone.	
(b) Rationale In the event that a security breach has occurred and is detected, it is likely that the incident response plan includes actions to prevent further propagation and effects of the incident. Such actions could be to isolate network segments and control systems supporting essential functions.	
(c) Requirement details	
i) Where the Incident Response Plan indicates network isolation as an action to be done, it is to be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There are to be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner.	

Amended	Remarks
ii) Individual system’s data dependencies that may affect function and correct operation, including safety, are to be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.	
(d) Demonstration of compliance	
i) Design phase The systems integrator is to include the information related to Specification of how to isolate each security zone from other zones or networks in the Cyber security design description. The effects of such isolation is also to be described, demonstrating that the computer-based systems in a security zone do not rely on data transmitted by IP-networks from other zones or networks.	
ii) Construction phase No requirements.	
iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see**2.2.3-4(2)**) and demonstrate to the Society by disconnecting all networks traversing security zone boundaries, that the computer-based systems in the security zone will maintain adequate operational functionality without network communication with other security zones or networks. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**.	
iv) Operation phase	
1) For general requirements to surveys in the operation phase (see **2.2.3-5**).	
2) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(4) Fallback to a minimal risk condition	E26(Rev.1) 4.4.4
(a) Requirement In the event of a cyber incident impairing the ability of a computer-based system or network in the scope of applicability of this Chapter to provide its intended service, the affected system or network is to fall back to a minimal risk condition, i.e. bring itself in a stable, stopped condition to reduce the risk of possible safety issues.	
(b) Rationale	
i) The ability of a computer-based system and integrated systems to fallback to one or more minimal risk conditions to be reached in case of unexpected or unmanageable failures or events is a safety measure aimed to keep the system in a consistent, known and safe state.	
ii) 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	

Amended	Remarks

phase of the ship (e.g. port depart/arrival vs. open sea passage) and the events occurred.

(c) Requirement details

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

1) bringing the system to a complete stop or other safe state,
2) disengaging the system,
3) transferring control to another system or human operator, and
4) other compensating actions.

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

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

(d) Demonstration of compliance

i) Design phase

The systems integrator is to include the information related to specification of safe state for the control functions in the computer-based systems in the scope of applicability of this Chapter in the Cyber security design description.

ii) Construction phase

No requirements.

iii) Commissioning phase

The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society that computer-based systems in the scope of applicability of this Chapter respond to cyber incidents in a safe manner (as per **5.4.5(4)(d)i)**), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests are to at least include denial of service (DoS) attacks and may be done together with related test in **5.4.4(1)(d)iii)**. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**.

iv) Operation phase

1) For general requirements to surveys in the operation phase (see **2.2.3-5**).

2) Special Survey

Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.

5.4.6 Recover

E26(Rev.1) 4.5

The requirements for the Recover functional element are aimed at the development and implementation of appropriate

Amended	Remarks
means supporting the ability to restore computer-based systems and networks onboard affected by cyber incidents. (1) Recovery plan (a) Requirement A recovery plan is to be made by the shipowner to support restoring computer-based systems under the scope of applicability of this Chapter to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom are to be part of the recovery plan. (b) Rationale i) 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. ii) Where appropriate, external cyber incident response support should be obtained to assist in preservation of evidence whilst restoring operational capability. (c) Requirement details i) The various stakeholders involved in the design and construction phases of the ship are to provide information to the shipowner for the preparation of the recovery plan to be placed onboard at the first Annual Survey. The recovery plan is to be kept up-to-date (e.g. upon maintenance) during the operational life of the ship. ii) Recovery plans are to 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 are to be available. iii) When developing recovery plans, the various systems and subsystems involved are to be specified. The following recovery objectives are also to be specified: l) System recovery: methods and procedures to recover communication capabilities are to be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities. 2) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation are to be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated. iv) Once the recovery objectives are defined, a list of potential cyber incidents is to be created, and the recovery procedure developed and described. Recovery plans are to include, or refer to the following information; l) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.	 E26(Rev.1) 4.5.1

Amended	Remarks
2) Processes and procedures for the backup and secure storage of information. 3) Complete and up-to-date logical network diagram. 4) The list of personnel responsible for restoring the failed system. 5) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc. 6) Current configuration information for all components. v) The operation and navigation of the ship are to be prioritized in the plan in order to help ensure the safety of onboard personnel. vi) Recovery plans in hard copy onboard and ashore are to be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents. (d) Demonstration of compliance i) Design phase The systems integrator is to include the references to information provided by the suppliers (**4.4.1(8)**) that may be applied by the shipowner to establish plans to recover from cyber incidents in the Cyber security design description. ii) Construction phase No requirements. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in **5.4.6(2)** and **(3)** The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. iv) Operation phase For general requirements to surveys in the operation phase (see **2.2.3-5**). 1) The shipowner is to in the Ship cyber security and resilience program describe incident recovery plans. The plans are to cover the computer-based systems in scope of applicability of this Chapter and are to 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 **5.4.6(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 computer-based systems in accordance with requirements in **5.4.6(2)**. - Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the	

Amended	Remarks
computer-based systems in accordance with requirements in **5.4.6(2)** and **5.4.6(3)**. 2) First Annual Survey The shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that: - Instructions and/or procedures for incident recovery are available for the responsible personnel onboard. - Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard. - Backup of the computer-based systems have been taken in accordance with the policies and procedures. - Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard. 3) Subsequent Annual Surveys The shipowner is to upon request by the Society demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first Annual Survey.	
(2) Backup and restore capability (a) Requirement Computer-based systems and networks in the scope of applicability of this Chapter are to have the capability to support back-up and restore in a timely, complete and safe manner. Backups are to be regularly maintained and tested. (b) Rationale In general, the purpose of a backup and restore strategy should protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following: i) planning and testing responses to different kinds of failures, ii) configuring the database environment for backup and recovery, iii) setting up a backup schedule, iv) monitoring the backup and recovery environment, v) creating a database copy for long-term storage, vi) moving data from one database or one host to another, etc. (c) Requirement details i) Restore capability 1) Computer-based systems in the scope of applicability of this Chapter are to have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident.	E26(Rev.1) 4.5.2

Amended	Remarks
2) Data are to be restorable from a secure copy or image.	
3) Information and backup facilities are to be sufficient to recover from a cyber incident.	
ii) Backup	
1) Computer-based systems and networks in the scope of applicability of this Chapter are to provide backup for data. The use of offline backups is to also be considered to improve tolerance against ransomware and worms affecting online backup appliances.	
2) Backup plans are to be developed, including scope, mode and frequency, storage medium and retention period.	
(d) Demonstration of compliance	
i) Design phase No requirements.	
ii) Construction phase No requirements.	
iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society the procedures and instructions for backup and restore provided by the suppliers for computer-based systems in the scope of applicability of this Chapter. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**.	
iv) Operation phase	
1) For general requirements to surveys in the operation phase (see **2.2.3-5**).	
2) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
(3) Controlled shutdown, reset, roll-back and restart	E26(Rev.1) 4.5.3
(a) Requirement	
i) Computer-based system and networks in the scope of applicability of this Chapter are to 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.	
ii) Suitable documentation on how to execute the above-mentioned operations are to be available to onboard personnel.	
(b) Rationale	
i) Controlled shutdown consists in turning a computer-based system or network off by software function allowing other connected systems to commit/rollback pending transactions, terminating processes, closing	

Amended	Remarks
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. ii) 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. iii) 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. iv) 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. v) Restarting a system and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source appears to be an effective approach to recover from unexpected faults or cyber incidents. Restart operations should be however controlled in particular for integrated systems, where unexpected restart of a single component can result in inconsistent system state or unpredictable behaviour. (c) Requirement details i) Computer-based system and networks in the scope of applicability of this Chapter are to be capable of the following: 1) 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. 2) resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state. 3) rolling back to a previous configuration and/or state, to restore system integrity and consistency. 4) 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 is to be compatible with the system's intended service and is not to bring other connected systems, or the integrated system it is part of, to an inconsistent or unsafe state. ii) Documentation are to be available to onboard personnel on how to execute the above- mentioned operations in case of a system affected by a cyber incident.	

Amended	Remarks
(d) Demonstration of compliance i) Design phase The systems integrator is to include the references to product manuals or procedures describing how to safely shut down, reset, restore and restart the computer-based systems in the scope of applicability of this Chapter in the Cyber security design description. ii) Construction phase No requirements. iii) Commissioning phase The systems integrator is to submit Ship cyber resilience test procedure (see **2.2.3-4(2)**) and demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the computer-based systems in the scope of applicability of this Chapter. These manuals/procedures are to be provided to the shipowner. The above tests may be omitted if performed during the certification of computer-based systems as per **2.2.3-4(2)**. iv) Operation phase 1) For general requirements to surveys in the operation phase (see **2.2.3-5**). 2) Special Survey Subject to modifications of the computer-based systems, the shipowner is to demonstrate to the Society the activities in **iii)** as per the Ship cyber resilience test procedure.	
5.5 Risk Assessment for Exclusion of Computer-based System from the Application of Requirements	E26(Rev.1) 6.
5.5.1 Requirement A risk assessment is to be carried out in case any of the computer-based systems falling under the scope of applicability of this Chapter is excluded from the application of relevant requirements. The risk assessment is to provide evidence of the acceptable risk level associated to the excluded computer-based systems.	E26(Rev.1) 6.1
5.5.2 Rationale **1** Exclusion of a computer-based system falling under the scope of applicability of this Chapter from the application of relevant requirements needs to be duly justified and documented. Such exclusion can be accepted by the Society only if evidence is given that the risk level associated to the operation of the computer-based system is under an acceptable threshold by means of specific risk assessment. **2** The risk assessment is to be based on available knowledge bases and experience on similar designs, if any, considering	E26(Rev.1) 6.2

Amended	Remarks
the computer-based system category, connectivity and the functional requirements and specifications of the ship and of the computer-based system. Cyber threat information from internal and external sources may be used to gain a better understanding of the likelihood and impact of cybersecurity events.	
5.5.3 Requirement Details **1** Risk assessment is to 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 is to update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in computer-based system onboard in a process of continuous improvement. **3** Should new risks be identified, the shipowner is to update existing, or implement new risk mitigation measures. Should the changes in the cyber scenario be such as to elevate the risk level associated to the computer-based system under examination above the acceptable risk threshold, the shipowner is to inform the Society and submit the updated risk assessment for evaluation. **4** The envisaged operational environments for the computer-based system under examination are to be analyzed in the risk assessment to discern the likelihood of cyber incidents and the impact they could have on the human safety, the safety of the vessel or the marine environment, taking into account the category of the computer-based system. The attack surface is to be analyzed, taking into account the connectivity of the computer-based system, possible interfaces for portable devices, logical access restrictions, etc. **5** Emerging risks related to the specific configuration of the computer-based system under examination is to be also identified. In the risk assessment, the following elements are to 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, and (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).	E26(Rev.1) 6.3
5.5.4 Acceptance Criteria **1** Exclusion of a computer-based system falling under the scope of applicability of this Chapter from the application of relevant requirements can be accepted by the Society only if assurance is given that the operation of the computer-based system has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a computer-based system which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence	E26(Rev.1) 6.4

and is found satisfactory by the Society. The Society may also require submittal of additional documents to consider the said exclusion.

2 The following criteria are to be met to exclude a system from the scope of applicability of this Chapter:

(1) The computer-based system is to be isolated (i.e, have no IP-network connections to other systems or networks).

(2) The computer-based system is to have no accessible physical interface ports. Unused interfaces are to be logically disabled. It is not to be possible to connect unauthorised devices to the computer-based system.

(3) The computer-based system is to be located in areas to which physical access is controlled.

(4) The computer-based system is not to be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Chapter.

3 The following additional criteria are to be considered for the evaluation of risk level acceptability:

(1) The computer-based system should not serve ship functions of category III.

(2) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the computer-based system have been duly considered in the risk assessment.

(3) The attack surface for the computer-based system is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points.

EFFECTIVE DATE AND APPLICATION

1. The effective date of the amendments is 1 July 2024.

2. Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date.

* “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29.

IACS PR No.29 (Rev.0, July 2009)

1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding.

2. The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder.

For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided:

(1) such alterations do not affect matters related to classification, or

(2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval.

The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed.

3. If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.**

Amended	Remarks
and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.	

Amended	Original	Remarks
RULES FOR BALLAST WATER MANAGEMENT INSTALLATIONS	**RULES FOR BALLAST WATER MANAGEMENT INSTALLATIONS**	
Part 4 REQUIREMNETS FOR BALLAST WATER MANAGEMENT SYSTEM INSALLATION	**Part 4 REQUIREMNETS FOR BALLAST WATER MANAGEMENT SYSTEM INSALLATION**	
Chapter 2 ARRAGEMENT, PIPING, ELECTRICAL INSTALLATIONS, ETC.	**Chapter 2 ARRAGEMENT, PIPING, ELECTRICAL INSTALLATIONS, ETC.**	
2.2 Installation	**2.2 Installation**	
2.2.1 General Requirements	**2.2.1 General Requirements**	
9 In general, *BWMS* monitoring functions of *BWMS* belong to system category I when applying **Part X of the Rules for the Survey and Construction of Steel Ships**. However, in cases where by-pass valves are integrated into valve remote control systems, such by-pass valves belong to the system category II for ballast transfer remote control systems.	**9** In general, *BWMS* monitoring functions of *BWMS* belong to system category I when applying **Annex D18.1.1, the Guidance for the Survey and Construction of Steel Ships**. However, in cases where by-pass valves are integrated into valve remote control systems, such by-pass valves belong to the system category II for ballast transfer remote control systems.	Reference was changed. Annex 18.1.1, Part D transfer to part X in previous amendment (Computer based systems, December 2023).
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * "contract for construction" is defined in the		

Amended	Original	Remarks
latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: **This Procedural Requirement applies from 1 July 2009.**		

Amended	Original	Remarks
RULES FOR HIGH SPEED CRAFT	**RULES FOR HIGH SPEED CRAFT**	
Part 1 GENERAL RULES	**Part 1 GENERAL RULES**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.2 Class Notations	**1.2 Class Notations**	
1.2.4 Hull Construction and Equipment, etc. **9** For crafts complying with the provisions of **Chapter 4 and 5, Part X of the Rules for the Survey and Construction of Steel Ships**, the notation of "*Cyber Resilience*" (abbreviated to *CybR*) is affixed to the Classification Characters.	**1.2.4 Hull Construction and Equipment, etc.** (Newly added)	Addition of Notation.
10 Otherwise specified in the above, for craft where deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	**9** Otherwise specified in the above, for craft where deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	
1.2.5 Compliance with the Special Requirements for International Voyages For craft complying with the special requirements for those engaged in international voyage in accordance with the provisions of **Part 15**, the notation of "*High Speed Craft complied with International Code of Safety for High Speed Craft*" (abbreviated to *HSC*) is affixed to the Classification Characters.	**1.2.5 Compliance with the Special Requirements for International Voyages** For craft complying with the special requirements for those engaged in international voyage in accordance with the provisions of **Part 14**, the notation of "*High Speed Craft complied with International Code of Safety for High Speed Craft*" (abbreviated to *HSC*) is affixed to the Classification Characters.	

Amended	Original	Remarks
Part 2 CLASS SURVEYS	**Part 2 CLASS SURVEYS**	
Chapter 2 CLASSIFICATION SURVEYS	**Chapter 2 CLASSIFICATION SURVEYS**	
2.1 Classification Survey during Construction	**2.1 Classification Survey during Construction**	
2.1.1 General In the Classification Survey during construction, the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, computer-based systems, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in this Rule.	**2.1.1 General** In the Classification Survey during construction, the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in this Rule.	Addition of rules which refer to new rules of Part X. (the same as follow)
2.1.2 Submission of Plans and Documents for Approval* **1** When it is intended to build a craft to the classification with the Society, the following plans and documents are to be submitted for the approval by the Society before the work is commenced. Plans and documents may be subjected to examination by the Society prior to the submission of the application for the classification of the craft in accordance with the provision specified otherwise by the Society: ((1) is omitted) (2) Machinery ((a) to (m) are omitted) (n) Computer-based systems Plans and data specified in **2.1.1(2), Part X of the Rules for the Survey and Construction of Steel Ships.** ((3) and (4) are omitted)	**2.1.2 Submission of Plans and Documents for Approval*** **1** When it is intended to build a craft to the classification with the Society, the following plans and documents are to be submitted for the approval by the Society before the work is commenced. Plans and documents may be subjected to examination by the Society prior to the submission of the application for the classification of the craft in accordance with the provision specified otherwise by the Society: ((1) is omitted) (2) Machinery ((a) to (m) are omitted) (Newly added) ((3) and (4) are omitted)	

Amended	Original	Remarks
2.1.3 Submission of Other Plans and Documents **1** When it is intended to build a craft to the classification with the Society, the following plans and documents are to be submitted in addition to those required in **2.1.2**: ((1) to (6) are omitted) (7) The following plans and documents related to machinery: ((a) to (i) are omitted) (n) Computer-based systems Plans and data specified in **2.1.1(2), Part X of the Rules for the Survey and Construction of Steel Ships.** ((8) to (10) are omitted)	**2.1.3 Submission of Other Plans and Documents** **1** When it is intended to build a craft to the classification with the Society, the following plans and documents are to be submitted in addition to those required in **2.1.2**: ((1) to (6) are omitted) (7) The following plans and documents related to machinery: ((a) to (i) are omitted) (Newly added) ((8) to (10) are omitted)	
2.1.4 Presence of Surveyor* **2** The presence of the Surveyor is required at the following stages of the work in relation to machinery. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where the Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. ((1) is omitted) (2) Main parts of machinery (a) When the tests specified in **Part D**, **Part H** and **Part X of the Rules for the Survey and Construction of Steel Ships** depending upon the kind of machinery are carried out. ((b) to (e) are omitted) ((3) to (6) are omitted)	**2.1.4 Presence of Surveyor*** **2** The presence of the Surveyor is required at the following stages of the work in relation to machinery. To implement surveys of items specified otherwise by the Society, in lieu of traditional ordinary surveys where the Surveyor is in attendance, the Society may approve other survey methods which it considers to be appropriate in the following cases. ((1) is omitted) (2) Main parts of machinery (a) When the tests specified in **Part D** and **Part H of the Rules for the Survey and Construction of Steel Ships** depending upon the kind of machinery are carried out. ((b) to (e) are omitted) ((3) to (6) are omitted)	
2.1.6 Documents to be Maintained On Board* **1** At the completion of a classification survey, the	**2.1.6 Documents to be Maintained On Board*** **1** At the completion of a classification survey, the	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
Surveyor confirms that the following drawings, plans, manuals, lists, etc., as applicable, of finished version are on board.	Surveyor confirms that the following drawings, plans, manuals, lists, etc., as applicable, of finished version are on board.	
(1) Documents approved by the Society or their copies	(1) Documents approved by the Society or their copies	Addition of drawings kept onboard because E26(Rev.1) was incorporated.
（(a) to (d) are omitted）	（(a) to (d) are omitted）	
(e) Zones and conduit diagram **(2.2.3-3(4), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(f) Cyber security design description **(2.2.3-3(5), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(g) Vessel asset inventory **(2.2.3-3(6), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(h) Risk assessment for the exclusion of computer-based systems **(2.2.3-3(7), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(i) Description of compensating countermeasures **(2.2.3-3(8), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(j) Ship cyber resilience test procedure **(2.2.3-4(2), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
（(2) and (3) are omitted）	（(2) and (3) are omitted）	

Amended	Original	Remarks
Chapter 3 PERIODICAL SURVEYS AND PLANNED MACHINERY SURVEYS	**Chapter 3 PERIODICAL SURVEYS AND PLANNED MACHINERY SURVEYS**	
3.3 Annual Surveys for Hull	**3.3 Annual Surveys for Hull**	
3.3.1 Requirements for Annual Surveys **1** At each Annual Survey, the general condition of the hull and equipment is to be examined and tested as far as practicable and placed in good order with special attention being paid to the following: （(1) to (16) are omitted）	**3.3.1 Requirements for Annual Surveys** **1** At each Annual Survey, the general condition of the hull and equipment is to be examined and tested as far as practicable and placed in good order with special attention being paid to the following: （(1) to (16) are omitted）	
(17) For craft of not less than 500 *gross tonnage* engaged on international voyages, general conditions of portable atmosphere testing instruments for enclosed spaces specified in **1.2.1, Part 15** are to be examined. (This includes the confirmation of calibration records.)	(17) For craft of not less than 500 *gross tonnage* engaged on international voyages, general conditions of portable atmosphere testing instruments for enclosed spaces specified in **1.2.1, Part 14** are to be examined. (This includes the confirmation of calibration records.)	Editorial correction.
3.11 Surveys for Crafts Using Low-flashpoint Fuels	**3.11 Annual Surveys for Crafts Using Low-flashpoint Fuels**	
3.11.1 Annual Surveys At Annual Surveys for crafts using low-flashpoint fuels, the examinations specified in **3.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.3** and **3.6**.	**3.11.1 Requirements** At Annual Surveys for crafts using low-flashpoint fuels, the examinations specified in **3.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.3** and **3.6**.	

Amended	Original	Remarks
	3.12 Intermediate Surveys for Crafts Using Low-flashpoint Fuels	
3.11.2 Intermediate Surveys At Intermediate Surveys for crafts using low-flashpoint fuels, the examinations specified in **4.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.4** and **3.7**.	**3.12.1 Requirements** At Intermediate Surveys for crafts using low-flashpoint fuels, the examinations specified in **4.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.4** and **3.7**.	
	3.13 Special Surveys for Crafts Using Low-flashpoint Fuels	
3.11.3 Special Surveys At Special Surveys for crafts using low-flashpoint fuels, the examinations specified in **5.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.5** and **3.8**.	**3.13.1 Requirements** At Special Surveys for crafts using low-flashpoint fuels, the examinations specified in **5.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.5** and **3.8**.	
3.12 Surveys of Water jet Propulsion Systems, etc.	**3.14 Surveys of Water jet Propulsion Systems, etc.**	
3.12.1 Annual Surveys For ships fitted with water jet propulsion systems, the annual surveys are to be carried out in accordance with the surveys specified in **3.3.4**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	**3.14.1 Annual Surveys** For ships fitted with water jet propulsion systems, the annual surveys are to be carried out in accordance with the surveys specified in **3.3.4**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	
3.12.2 Intermediate Surveys For ships fitted with water jet propulsion systems, the intermediate surveys are to be carried out in accordance with the surveys specified in **4.3.4**, **Part B of the Rules for the**	**3.14.2 Intermediate Surveys** For ships fitted with water jet propulsion systems, the intermediate surveys are to be carried out in accordance with the surveys specified in **4.3.4**, **Part B of the Rules for the**	

Amended	Original	Remarks
Survey and Construction of Steel Ships.	**Survey and Construction of Steel Ships**.	
3.12.3 Special Surveys For ships fitted with water jet propulsion systems, the special surveys are to be carried out in accordance with the surveys specified in **5.3.4**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	**3.14.3 Special Surveys** For ships fitted with water jet propulsion systems, the special surveys are to be carried out in accordance with the surveys specified in **5.3.4**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	
3.12.4 Docking Surveys For ships fitted with water jet propulsion systems, the docking surveys are to be carried out in accordance with the surveys specified in **6.1.1-2**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	**3.14.4 Docking Surveys** For ships fitted with water jet propulsion systems, the docking surveys are to be carried out in accordance with the surveys specified in **6.1.1-2**, **Part B of the Rules for the Survey and Construction of Steel Ships**.	
3.13 Surveys of Crafts Affixed with the Notation "*CybR*"	**(Newly added)**	Addition of requirement of survey because E26(Rev.1) was incorporated.
3.13.1 Annual Surveys At Annual Surveys for crafts affixed with the notation "*CybR*", the examinations specified in **3.9**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.3** and **3.6**.	**(Newly added)**	
3.13.2 Intermediate Surveys At Intermediate Surveys for crafts affixed with the notation "*CybR*", the examinations specified in **4.9**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.4** and **3.7**.	**(Newly added)**	
3.13.3 Special Surveys At Special Surveys for crafts affixed with the notation	**(Newly added)**	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
“*CybR*”, the examinations specified in **5.9, Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out, in addition to the examinations specified in **3.5** and **3.8**.		

Amended	Original	Remarks
Part 9 MACHINERY INSTALLATIONS	**Part 9 MACHINERY INSTALLATIONS**	
Chapter 12 AUTOMATIC AND REMOTE CONTROL	**Chapter 12 AUTOMATIC AND REMOTE CONTROL**	
12.1 General	**12.1 General**	
12.1.1 Scope*	**12.1.1 Scope***	
1 The requirements in this Chapter apply to the systems of automatic or remote control which are used to control the following machinery and equipment.	**1** The requirements in this Chapter apply to the systems of automatic or remote control which are used to control the following machinery and equipment.	
(1) Main propulsion machinery (in this Chapter, propulsion generating set in electric propulsion ships are excluded),	(1) Main propulsion machinery (in this Chapter, propulsion generating set in electric propulsion ships are excluded),	
(2) Controllable pitch propeller	(2) Controllable pitch propeller	
(3) Steam generating set	(3) Steam generating set	
(4) Electric generating set (in this Chapter, propulsion generating set in electric propulsion ships are included)	(4) Electric generating set (in this Chapter, propulsion generating set in electric propulsion ships are included)	
(5) Auxiliary machinery associated with machinery and equipment listed in **(1)** to **(4)**	(5) Auxiliary machinery associated with machinery and equipment listed in **(1)** to **(4)**	
(6) Fuel oil systems	(6) Fuel oil systems	
(7) Bilge systems	(7) Bilge systems	
(8) Deck machinery	(8) Deck machinery	
2 Where considered necessary by the Society, the requirements in this Chapter are correspondingly applied to the systems of automatic or remote control which are used for controlling machinery and equipment not listed in **-1(1)** to **(8)**.	**2** Where considered necessary by the Society, the requirements in this Chapter are correspondingly applied to the systems of automatic or remote control which are used for controlling machinery and equipment not listed in **-1(1)** to **(8)**.	
3 Computer based systems are to be in accordance with **Part X of the Rules for the Survey and Construction of Steel Ships** in addition to those specified in **-1** and **-2** above	**3** Computer based systems, including the hardware and software which constitute such systems, are to be in accordance with **Annex 18.1.1, Part D of the Rules for the**	

Amended	Original	Remarks
and throughout the rest of this chapter.	**Survey and Construction of Steel Ships** in addition to those specified in **-1** and **-2** above and throughout the rest of this chapter for design, construction, commissioning, maintenance, etc.	

Amended	Original	Remarks
Part 14 COMPUTER-BASED SYSTEMS	**(Newly added)**	
Chapter 1 GENERAL	**(Newly added)**	
1.1 General	**(Newly added)**	Addition of rules which refer to new rules of Part X.
1.1.1 Application Computer-based systems are to be according to relevant requirements in **Chapter 3** and subsequent chapters, **Part X of the Rules for the Survey and Construction of Steel Ships**.	**(Newly added)**	
Part 15 SPECIAL REQUIREMENTS FOR CRAFT ENGAGED IN INTERNATIONAL VOYAGE	**Part 14 SPECIAL REQUIREMENTS FOR CRAFT ENGAGED IN INTERNATIONAL VOYAGE**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.1 General	**1.1 General**	
1.1.1 Application* In addition to the requirements specified in **Part 1** to **Part 14 of the Rules**, crafts engaged on international voyages are to be complied with the requirements *of IMO Resolution MSC*.97(73) *THE INTERNATIONAL CODE OF SAFETY FOR HIGH SPEED CRAFT*, as may be amended,	**1.1.1 Application*** In addition to the requirements specified in **Part 1** to **Part 13 of the Rules**, crafts engaged on international voyages are to be complied with the requirements *of IMO Resolution MSC*.97(73) *THE INTERNATIONAL CODE OF SAFETY FOR HIGH SPEED CRAFT*, as may be amended,	

Amended	Original	Remarks
in its entirety or other technical requirements which the Society considers to be equivalent to the said international code. EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is	in its entirety or other technical requirements which the Society considers to be equivalent to the said international code.	

Amended	Original	Remarks
the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: **This Procedural Requirement applies from 1 July 2009.**		

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF PASSENGER SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF PASSENGER SHIPS**	
Part 1 GENERAL	**Part 1 GENERAL**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.2 Class Notations	**1.2 Class Notations**	
1.2.4 Hull Construction and Equipment, etc.*	**1.2.4 Hull Construction and Equipment, etc.***	
9 For ships complying with the provisions of **Chapter 4** and **5, Part X of the Rules for the Survey and Construction of Steel Ships**, the notation of "*Cyber Resilience*" (abbreviated to *CybR*) is affixed to the Classification Characters.	(Newly added)	Addition of Notation.
10 Otherwise specified in the above, for ships where deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	**9** Otherwise specified in the above, for ships where deemed necessary by the Society, an appropriate notation may be affixed to the Classification Characters.	

Amended	Original	Remarks
Part 2 CLASS SURVEY	**Part 2 CLASS SURVEY**	
Chapter 2 CLASSIFICATION SURVEYS	**Chapter 2 CLASSIFICATION SURVEYS**	
2.1 Classification Survey during Construction	**2.1 Classification Survey during Construction**	
2.1.1 General* In the Classification Survey during Construction, the hull and its equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, computer-based systems, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in the Rules.	**2.1.1 General*** In the Classification Survey during Construction, the hull and its equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, stability and load lines are to be examined in detail in order to ascertain that they meet the relevant requirements in the Rules.	Addition of rules which refer to new rules of Part X. (the same as follow)
2.1.7 Documents to be Maintained On Board* **1** At the completion of a classification survey, the Surveyor confirms that the following drawings, plans, manuals, lists, etc., as applicable, of finished version are on board. (1) Documents approved by the Society or their copies （(a) to (h) are omitted）	**2.1.7 Documents to be Maintained On Board*** **1** At the completion of a classification survey, the Surveyor confirms that the following drawings, plans, manuals, lists, etc., as applicable, of finished version are on board. (1) Documents approved by the Society or their copies （(a) to (h) are omitted）	
(i) Zones and conduit diagram **(2.2.3-3(4), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	Addition of drawings kept onboard because E26(Rev.1) was incorporated.
(j) Cyber security design description **(2.2.3-3(5), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	
(k) Vessel asset inventory **(2.2.3-3(6), Part X of the Rules for the Survey and Construction of Steel Ships)**	(Newly added)	

Amended	Original	Remarks
(l) Risk assessment for the exclusion of computer-based systems (**2.2.3-3(7), Part X of the Rules for the Survey and Construction of Steel Ships**)	(Newly added)	
(m) Description of compensating countermeasures (**2.2.3-3(8), Part X of the Rules for the Survey and Construction of Steel Ships**)	(Newly added)	
(n) Ship cyber resilience test procedure (**2.2.3-4(2), Part X of the Rules for the Survey and Construction of Steel Ships**)	(Newly added)	
（(2) and (3) are omitted）	（(2) and (3) are omitted）	
2.2 Classification Survey of Ships Not Built under Survey	**2.2 Classification Survey of Ships Not Built under Survey**	
2.2.1 General	**2.2.1 General**	
1 The Classification Survey of Ships not built under Survey is to be carried out in accordance with the requirement in **2.2.1**, **Part B of the Rules for the Survey and Construction of Steel Ships** corresponding to the ship's age for the hull and its equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, computer-based systems, stability and load lines.	**1** The Classification Survey of Ships not built under Survey is to be carried out in accordance with the requirement in **2.2.1**, **Part B of the Rules for the Survey and Construction of Steel Ships** corresponding to the ship's age for the hull and its equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, stability and load lines.	

Amended	Original	Remarks
Chapter 3 INTERMEDIATE SURVEYS	**Chapter 3 INTERMEDIATE SURVEYS**	
3.1 General	**3.1 General**	
3.1.1 Application	**3.1.1 Application**	
1 At Intermediate Surveys, the surveys required for general cargo ships specified in **Chapter 4**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	**1** At Intermediate Surveys, the surveys required for general cargo ships specified in **Chapter 4**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	
2 For ships using low-flashpoint fuels, the examinations specified in **4.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	**2** For ships using low-flashpoint fuels, the examinations specified in **4.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	
3 For ships affixed with the notation "*CybR*", the examinations specified in **4.9**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	(Newly added)	Addition of requirement of survey because E26(Rev.1) was incorporated.
4 In addition to those specified in **-1**, **-2** and **-3** above, the surveys specified in **3.2** and **3.3** are to be carried out.	**3** In addition to those specified in **-1** and, **-2** above, the surveys specified in **3.2** and **3.3** are to be carried out.	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
Chapter 4 SPECIAL SURVEYS	**Chapter 4 SPECIAL SURVEYS**	
4.1 General	**4.1 General**	
4.1.1 Application	**4.1.1 Application**	
1 At Special Surveys, the surveys required for general cargo ships specified in **Chapter 5, Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	**1** At Special Surveys, the surveys required for general cargo ships specified in **Chapter 5, Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	
2 For ships using low-flashpoint fuels, the examinations specified in **5.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	**2** For ships using low-flashpoint fuels, examinations specified in **5.6**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	
3 For ships affixed with the notation "*CybR*", the examinations specified in **5.9**, **Part B of the Rules for the Survey and Construction of Steel Ships** are to be carried out.	(Newly added)	Addition of requirement of survey because E26(Rev.1) was incorporated.
4 In addition to those specified in **-1**, **-2** and **-3** above, the surveys specified in **4.2** and **4.3** are to be carried out.	**3** In addition to those specified in **-1** and, **-2** above, the surveys specified in **4.2** and **4.3** are to be carried out.	

Amended	Original	Remarks
Part 11 COMPUTER-BASED SYSTEMS	**(Newly added)**	
Chapter 1 GENERAL	**(Newly added)**	
1.1 General	**(Newly added)**	
1.1.1 Scope Computer-based systems are to be according to relevant requirements in **Chapter 3** and subsequent chapters, **Part X of the Rules for the Survey and Construction of Steel Ships**.	**(Newly added)**	Addition of rules which refer to new rules of Part X.
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) 1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. 2. The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on		

Amended	Original	Remarks
which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: **This Procedural Requirement applies from 1 July 2009.**		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS	**RULES FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS**	
Part 2 CLASS SURVEYS	**Part 2 CLASS SURVEYS**	
Chapter 2 CLASSIFICATION SURVEYS	**Chapter 2 CLASSIFICATION SURVEYS**	
2.1 Classification Survey during Construction	**2.1 Classification Survey during Construction**	
2.1.2 Submission of Plans and Documents for Approval*	**2.1.2 Submission of Plans and Documents for Approval***	
1 When it is intended to build a ship for classification by the Society, the following plans and documents are to be submitted for the approval by the Society before the work is commenced. The plans and documents may be submitted for examination by the Society prior to making an application for the classification of the ship as stipulated otherwise by the Society.	**1** When it is intended to build a ship for classification by the Society, the following plans and documents are to be submitted for the approval by the Society before the work is commenced. The plans and documents may be submitted for examination by the Society prior to making an application for the classification of the ship as stipulated otherwise by the Society.	
((1) is omitted)	((1) is omitted)	
(2) Machinery	(2) Machinery	
((a) to (m) are omitted)	((a) to (m) are omitted)	
(Deleted)	(n) Computer-based systems: Plans and data specified in **2.1.1(1), Part X of the Rules for the Survey and Construction of Steel Ships**	Requirements of Computer-based systems are deleted from RULES FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS. (the same as follow)
((3) to (5) are omitted)	((3) to (5) are omitted)	

Amended	Original	Remarks
2.1.3 Submission of Other Plans and Documents **1** When it is intended to build a ship to the classification with the Society the following plans and documents are to be submitted, in addition to those required in **2.1.2**: ((1) to (6) are omitted) (7) The following plans and documents related to machinery: ((a) to (f) are omitted) (Deleted)	**2.1.3 Submission of Other Plans and Documents** **1** When it is intended to build a ship to the classification with the Society the following plans and documents are to be submitted, in addition to those required in **2.1.2**: ((1) to (6) are omitted) (7) The following plans and documents related to machinery: ((a) to (f) are omitted) (g) Computer-based systems: Plans and data specified in **2.1.1(1), Part X of the Rules for the Survey and Construction of Steel Ships**	
2.1.4 Presence of Surveyor* **2** The presence of the Surveyor is required at the following stages of the work in relation to machinery: ((1) is omitted) (2) Main parts of machinery (a) When the tests stipulated in either **Part 7** or **Part 8** (according to the kind of machinery) are carried out. ((b) to (e) are omitted) ((3) to (6) are omitted)	**2.1.4 Presence of Surveyor*** **2** The presence of the Surveyor is required at the following stages of the work in relation to machinery: ((1) is omitted) (2) Main parts of machinery (a) When the tests stipulated in either **Part 7** or **Part 8** (according to the kind of machinery) and **Part X of the Rules for the Survey and Construction of Steel Ships** are carried out. ((b) to (e) are omitted) ((3) to (6) are omitted)	

Amended	Remarks

Chapter 3 ANNUAL SURVEYS

Table 2.3.1 Examination of Plans and Documents

Items	Examination
1 Loading Manual	・ For ships required to have the manual on board in accordance with the requirements of **10.2.4, Part 4**, confirmation that the manual is kept on board is to be made.
2 Stability Information Booklet	・ Confirmation as to whether the booklet is kept on board is to be made.
3 Fire Control Plan	・ Confirmation that the fire control plan is provided on board is to be made.
~~4 Procedures for software and hardware change management and relevant change records~~	~~(1) Confirmation that the procedures for software and hardware change management are kept on board in accordance with **3.6.12-1, Part X of the Rules for the Survey and Construction of Steel Ships.**~~ ~~(2) Confirmation that the change records are updated in accordance with **3.6.11** **and** **3.6.12-1, Part X of the Rules for the Survey and Construction of Steel Ships.**~~

Amended	Original	Remarks
Part 7 MACHINERY INSTALLATIONS	**Part 7 MACHINERY INSTALLATIONS**	
Chapter 14 AUTOMATIC AND REMOTE CONTROL	**Chapter 14 AUTOMATIC AND REMOTE CONTROL**	
14.1 General	**14.1 General**	
14.1.1 Scope*	**14.1.1 Scope***	
1 The requirements in this Chapter apply to automatic or remote control systems which are used to control the following machinery and equipment:	**1** The requirements in this Chapter apply to automatic or remote control systems which are used to control the following machinery and equipment:	
(1) Main propulsion machinery (in this Chapter, propulsion generating sets in electric propulsion ships are excluded)	(1) Main propulsion machinery (in this Chapter, propulsion generating sets in electric propulsion ships are excluded)	
(2) Controllable pitch propeller	(2) Controllable pitch propeller	
(3) Steam generating sets	(3) Steam generating sets	
(4) Electric generating sets (in this Chapter, propulsion generating sets in electric propulsion ships are included)	(4) Electric generating sets (in this Chapter, propulsion generating sets in electric propulsion ships are included)	
(5) Auxiliary machinery associated with the machinery and equipment listed in **(1)** to **(4)**	(5) Auxiliary machinery associated with the machinery and equipment listed in **(1)** to **(4)**	
(6) Fuel oil systems	(6) Fuel oil systems	
(7) Bilge systems	(7) Bilge systems	
(8) Deck machinery	(8) Deck machinery	
2 In case where considered necessary by the Society, the requirements in this Chapter are correspondingly applied to those automatic or remote control systems which are used for controlling machinery and equipment not listed in **-1(1)** to **(8)**.	**2** In case where considered necessary by the Society, the requirements in this Chapter are correspondingly applied to those automatic or remote control systems which are used for controlling machinery and equipment not listed in **-1(1)** to **(8)**.	
(Deleted)	**3** Computer based systems, including the hardware and software which constitute such systems, are to be in	

Amended	Original	Remarks
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series	accordance with **Chapter1, 2 and 3, Part X of the Rules for the Survey and Construction of Steel Ships** in addition to those specified in **-1** and **-2** above and throughout the rest of this chapter for design, construction, commissioning, maintenance, etc.	

Amended	Original	Remarks
was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: **This Procedural Requirement applies from 1 July 2009.**		

Amended	Original	Remarks
RULES FOR THE SURVEY AND CONSTRUCTION OF SHIPS OF FIBREGLASS REINFORCED PLASTICS	**RULES FOR THE SURVEY AND CONSTRUCTION OF SHIPS OF FIBREGLASS REINFORCED PLASTICS**	
Chapter 2 CLASS SURVEYS	**Chapter 2 CLASS SURVEYS**	
2.2 Classification Survey during Construction	**2.2 Classification Survey during Construction**	
2.2.1 General **1** In the classification survey during construction, "the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, computer-based systems, stability and load lines" are to be examined in detail in order to ascertain that they meet the requirements in the relevant Chapters.	**2.2.1 General** **1** In the classification survey during construction, "the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installation, stability and load lines" are to be examined in detail in order to ascertain that they meet the requirements in the relevant Chapters.	Addition of rules which refer to new rules of Part X. (the same as follow)
2.3 Classification Survey Not Built under Survey	**2.3 Classification Survey Not Built under Survey**	
2.3.1 General **1** In the classification survey of *FRP* ships not built under the Society's survey, the actual scantlings of main parts of the ship are to be measured in addition to such examinations of the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, computer-based systems, stability and load lines as required for the special survey corresponding to the ship's age.	**2.3.1 General** **1** In the classification survey of *FRP* ships not built under the Society's survey, the actual scantlings of main parts of the ship are to be measured in addition to such examinations of the hull and equipment, machinery, fire protection and detection, means of escape, fire extinction, electrical installations, stability and load lines as required for the special survey corresponding to the ship's age.	

Amended	Original	Remarks
Chapter 19 MACHINERY **19.1 General** **19.1.1 Application** Prime movers, power transmission system, shaftings, pressure vessels, auxiliaries, piping systems, electrical installations, computer-based systems, etc. are, as a rule, to be in accordance with the requirements in the relevant chapters in the **Rules for the Survey and Construction of Steel Ships**, except those specified in this chapter. EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Rules, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single	**Chapter 19 MACHINERY** **19.1 General** **19.1.1 Application** Prime movers, power transmission system, shaftings, pressure vessels, auxiliaries, piping systems and electrical installations are, as a rule, to be in accordance with the requirements in the relevant chapters in the **Rules for the Survey and Construction of Steel Ships**, except those specified in this chapter.	

Amended	Original	Remarks
contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
GUIDANCE FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS	**GUIDANCE FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS**	
Part BCLASS SURVEYS	**Part BCLASS SURVEYS**	
B3 ANNUAL SURVEYS	**B3 ANNUAL SURVEYS**	
B3.9 Special Requirements for Ships Affixed with the Notation “*CybR*”	**(Newly added)**	
B3.9.3 Surveys The wording “upon request by the Society” in item 2(1) of **Table B3.12, Part B of the Rules** includes the case where the shipowners (or ship management companies) were changed.	**(Newly added)**	E26(Rev.1) 5.3.1
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the		

Amended	Original	Remarks
contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Remarks
GUIDANCE FOR THE SURVEY AND CONSTRUCTION OF STEEL SHIPS **Part X COMPUTER-BASED SYSTEMS** **X4 Cyber resilience of on-board systems and equipment** **X4.1 General**	
X4.1.1 General **1** Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.	E27(Rev.1) 1.1
2 Attention is made to the requirements on Computer-Based Systems and Cyber Resilience as follows: (1) Requirements on computer-based systems specified in **Chapter 3, Part X of the Rules** (2) Requirements on cyber resilience of ships specified in **Chapter 5, Part X of the Rules** (3) *IACS* Recommendation 166 on Cyber Resilience: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life.	E27(Rev.1) 1.3.1
X4.4 Requirements for Cyber resilience of on-board systems and equipment	
X4.4.2 Required Security Capabilities **1** In applying No.10 in **Table X4.1, Part X of the Rules**, port limits/blockers (and silicone) could be accepted for a specific system. **2** In applying No.17 in **Table X4.1, Part X of the Rules**, cryptographic mechanisms are to be employed for wireless	Requirement which was extracted E27(Rev. 1) 4.1 Note.

Amended	Remarks
networks. **3** In applying No.21 in **Table X4.1, Part X of the Rules**, for wireless network, cryptographic mechanisms are to be employed to protect confidentiality of all information in transit. **4** In applying No.24 in **Table X4.1, Part X of the Rules**, it is acceptable that the computer-based system may operate in a degraded mode upon DoS events, but it is not to 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.	

Amended	Remarks

X5 CYBER RESILIENCE OF SHIPS

X5.1 General

X5.1.1 Aim

E26(Rev.1) 1.

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. Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving. It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient. IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

2 The content of **Chapter 5, Part X of the Rules** is to be in accordance with **Table X5.1.1-1**.

E26(Rev.1) 1.1 Table 1

Table X5.1.1-1 The content of **Chapter 5, Part X of the Rules**

Introductory Part	5.1 Introduction
	5.2 Definitions
	5.3 Goals and Organization of Requirements
Main Part	5.4 Requirements 5.4.1 General 5.4.2 Identify 5.4.3 Protect 5.4.4 Detect 5.4.5 Respond 5.4.6 Recover
Supplementary Part	5.5 Risk assessment for exclusion of computer-based system from the application of requirements

Amended	Remarks
X5.2 Definitions	
X5.2.1 Terminology In “Network segment” referred to in **5.2.1(13), Part X of the Rules**, 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).	Requirement which was extracted E26(Rev. 1) 2. Note.
X5.4 Requirements for Cyber Resilience of Ships	
X5.4.3 Protect In **5.4.3(4)(c)v), Part X of the Rules**, computer-based systems are required to identify and authenticate human users as per Item No.1 in **Table X4.1, Part X of the Rules**,. In other words, it is not necessary to “uniquely” identify and authenticate each human user.	Requirement which was extracted E26(rev.1) 4.2.4.3.5 Note.
EFFECTIVE DATE AND APPLICATION 1. The effective date of the amendments is 1 July 2024. 2. Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) 1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. 2. The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed.	

Amended	Remarks
3. If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.	

Amended	Original	Remarks
GUIDANCE FOR AUTOMATIC AND REMOTE CONTROL SYSTEMS	**GUIDANCE FOR AUTOMATIC AND REMOTE CONTROL SYSTEMS**	
Chapter 2 SURVEYS OF AUTOMATIC AND REMOTE CONTROL SYSTEMS	**Chapter 2 SURVEYS OF AUTOMATIC AND REMOTE CONTROL SYSTEMS**	
2.2 Registration Surveys	**2.2 Registration Surveys**	
2.2.1 Drawings and Data	**2.2.1 Drawings and Data**	
1 (Omitted)	**1** (Omitted)	Reference was deleted. Annex 18.1.1, Part D transfer to part X in previous amendment (Computer based systems, December 2023).
(Deleted)	**2** In applying **2.2.1(1)(a)** and **(2)(a) of the Rules**, in cases where the automatic and remote control system includes computer based systems subject to **18.1.1-3, Part D of the Rules for the Survey and Construction of Steel Ships**, the drawings and data stipulated in **1.2, Annex 18.1.1, Part D of the Rules for the Survey and Construction of Steel Ships** are to be submitted. However, for computer based systems which have been already approved by the Society in accordance with **Chapter 8, Part 7 of the Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use**, only drawings and data on parts that differ from ship to ship need to be submitted; this, however, excludes those specified in **1.2(2)(a)** of the said Annex.	
2 (Omitted)	**3** (Omitted)	
EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the		

Amended	Original	Remarks
date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) **1.** The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
GUIDANCE FOR HIGH SPEED CRAFT	**GUIDANCE FOR HIGH SPEED CRAFT**	
Part 2 CLASS SURVEYS	**Part 2 CLASS SURVEYS**	
Chapter 1 GENERAL	**Chapter 1 GENERAL**	
1.1 Surveys	**1.1 Surveys**	
1.1.3 Occasional Surveys For the occasional surveys specified in **1.1.3(5), Part 2 of the Rules,** the following is to be complied with: ((1) is omitted)	**1.1.3 Occasional Surveys** For the occasional surveys specified in **1.1.3(5), Part 2 of the Rules,** the following is to be complied with: ((1) is omitted)	
(2) Portable Atmosphere Testing Instruments for Enclosed Spaces For craft of not less than 500 *gross tonnage* engaged on international voyages which had been at the beginning stage of construction before 1 July 2016, it is to be verified that portable atmosphere testing instruments complying with **1.2.1, Part 15 of the Rules** are provided on board by the first survey on or after 1 July 2016.	(2) Portable Atmosphere Testing Instruments for Enclosed Spaces For craft of not less than 500 *gross tonnage* engaged on international voyages which had been at the beginning stage of construction before 1 July 2016, it is to be verified that portable atmosphere testing instruments complying with **1.2.1, Part 14 of the Rules** are provided on board by the first survey on or after 1 July 2016.	Editorial correction.
((3) is omitted)	((3) is omitted)	

Amended-Original Requirements Comparison Table (Cyber Resilience)

Amended	Original	Remarks
Part 15 SPECIAL REQUIREMENTS FOR CRAFT ENGAGED IN INTERNATIONAL VOYAGE **Chapter 1 GENERAL** **1.2 Others** **1.2.1 Portable Atmosphere Testing Instruments for Enclosed Spaces** The wording "suitable means are to be provided for the calibration of all such instruments" in **1.2.1, Part 15 of the Rules** refers to portable atmosphere testing instruments being calibrated on board or ashore in accordance with the manufacturer's instructions together with corresponding calibration records being kept. In this regard, the calibration of portable atmosphere testing instruments does not include any pre-operational accuracy tests as recommended by the manufacturer. EFFECTIVE DATE AND APPLICATION **1.** The effective date of the amendments is 1 July 2024. **2.** Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the date of contract for construction is before the effective date. * "contract for construction" is defined in the latest version of IACS Procedural Requirement (PR) No.29.	**Part 14 SPECIAL REQUIREMENTS FOR CRAFT ENGAGED IN INTERNATIONAL VOYAGE** **Chapter 1 GENERAL** **1.2 Others** **1.2.1 Portable Atmosphere Testing Instruments for Enclosed Spaces** The wording "suitable means are to be provided for the calibration of all such instruments" in **1.2.1, Part 14 of the Rules** refers to portable atmosphere testing instruments being calibrated on board or ashore in accordance with the manufacturer's instructions together with corresponding calibration records being kept. In this regard, the calibration of portable atmosphere testing instruments does not include any pre-operational accuracy tests as recommended by the manufacturer.	Editorial correction.

Amended	Original	Remarks
IACS PR No.29 (Rev.0, July 2009) **1.** The date of "contract for construction" of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of "contract for construction" of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a "series of vessels" if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of "contract for construction" for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a "new contract" to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of "contract for construction" of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Original	Remarks
GUIDANCE FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS	**GUIDANCE FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS**	
Part 2 CLASS SURVEYS	**Part 2 CLASS SURVEYS**	
Chapter 9 PLANNED MACHINERY SURVEYS	**Chapter 9 PLANNED MACHINERY SURVEYS**	
9.1 Planned Machinery Surveys	**9.1 Planned Machinery Surveys**	
9.1.4 Condition Based Maintenance Scheme (CBM) **5** Approval of CBM Conditions for approval of CBM are as follows: ((1) is omitted) (2) Condition monitoring system The condition monitoring system is to satisfy the following requirements specified in **(a)** to **(h)**. In cases where this system is modified, that modification is to be approved by the Society. ((a) is omitted)	**9.1.4 Condition Based Maintenance Scheme (CBM)** **5** Approval of CBM Conditions for approval of CBM are as follows: ((1) is omitted) (2) Condition monitoring system The condition monitoring system is to satisfy the following requirements specified in **(a)** to **(h)**. In cases where this system is modified, that modification is to be approved by the Society. ((a) is omitted)	
(Deleted)	(b) The hardware and software of the computer is to comply with **9.1.3-4(5)(a)** to **(e)** and **Annex D18.1.1 "COMPUTER BASED SYSTEMS", Part D of the Guidance for the Survey and Construction of Steel Ships.**	Requirements of Computer-based systems are deleted from RULES FOR THE SURVEY AND CONSTRUCTION OF INLAND WATERWAY SHIPS. (the same as follow)
(b) The software is to have condition monitoring function specified in **Annex 9.1.3, Part B of the Rules for the Survey and Construction of Steel Ships** and be suited to diagnosing any	(c) In addition to **(b)**, the software is to have condition monitoring function specified in **Annex 9.1.3, Part B of the Rules for the Survey and Construction of Steel Ships** and be suited	

Amended	Original	Remarks
deterioration of machinery, equipment or associated components on the basis of the data from the sensors or centralized machinery monitoring and control systems specified in **(a)**. The software is to be suitable for diagnosing the condition of equipment or its components on the basis of independent or coalesced data, or their trends. (c) The condition monitoring system is to produce condition monitoring records. (d) In cases where condition monitoring and diagnosis are conducted on board ships, the condition monitoring system is to be such that no specialized knowledge of data analysis is required to use the system. (e) In cases where remote condition monitoring and diagnosis are conducted (i.e. the data sent from the ship is analyzed remotely), the condition monitoring systems are to include a communication function to transfer the data collected by the sensors or centralized machinery monitoring and control systems specified in **(a)**. Particular attention is to be paid to the cyber safety and security of said communication function. The system equipped on board is to be arranged to store the condition monitoring data in the event of loss of the communication function and transfer the data after the communication function is restored. (f) In cases where limiting parameters are modified, such modifications are to be identified. (g) The condition monitoring system is to include a method for backing up data at regular intervals.	to diagnosing any deterioration of machinery, equipment or associated components on the basis of the data from the sensors or centralized machinery monitoring and control systems specified in **(a)**. The software is to be suitable for diagnosing the condition of equipment or its components on the basis of independent or coalesced data, or their trends. (d) The condition monitoring system is to produce condition monitoring records. (e) In cases where condition monitoring and diagnosis are conducted on board ships, the condition monitoring system is to be such that no specialized knowledge of data analysis is required to use the system. (f) In cases where remote condition monitoring and diagnosis are conducted (i.e. the data sent from the ship is analyzed remotely), the condition monitoring systems are to include a communication function to transfer the data collected by the sensors or centralized machinery monitoring and control systems specified in **(a)**. Particular attention is to be paid to the cyber safety and security of said communication function. The system equipped on board is to be arranged to store the condition monitoring data in the event of loss of the communication function and transfer the data after the communication function is restored. (g) In cases where limiting parameters are modified, such modifications are to be identified. (h) The condition monitoring system is to include a method for backing up data at regular intervals.	

Amended	Original	Remarks
((3) to (7) are omitted)	((3) to (7) are omitted)	
Part 7 MACHINERY INSTALLATIONS	**Part 7 MACHINERY INSTALLATIONS**	
Chapter 14 AUTOMATIC AND REMOTE CONTROL	**Chapter 14 AUTOMATIC AND REMOTE CONTROL**	
14.1 General	**14.1 General**	
14.1.1 (omitted)	**14.1.1 (omitted)**	
(Deleted)	**14.1.2 Terminology** The computer based system referred to in **14.1.2(11), Part 7 of the Rules** includes a system which contains programmable controllers such as sequencers.	
EFFECTIVE DATE AND APPLICATION 1. The effective date of the amendments is 1 July 2024. 2. Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the date of contract for construction is before the effective date. * “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29. IACS PR No.29 (Rev.0, July 2009) 1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all		

Amended	Original	Remarks
the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding. **2.** The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder. For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided: (1) such alterations do not affect matters related to classification, or (2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval. The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed. **3.** If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply. **4.** If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder. Note: This Procedural Requirement applies from 1 July 2009.		

Amended	Remarks
GUIDANCE FOR THE APPROVAL AND TYPE APPROVAL OF MATERIALS AND EQUIPMENT FOR MARINE USE **Part 7 CONTROL AND INSTRUMENTATION EQUIPMENT AND ELECTRICAL INSTALLATIONS**	
Chapter 10 APPROVAL OF USE OF SYSTEMS AND EQUIPMENT WITH IMPROVED CYBER RESILIENCE	Newly regulated, in accordance with requirement of type approval specified in E27(Rev.1) 6.
10.1 General **10.1.1 Scope** **1** The requirements in this chapter applies to computer-based systems to which **Chapter 4, Part X of the Rules for the Survey and Construction of Steel Ships** applies and for which a voluntary offer has been made in accordance with **4.6.1, Part X of the Rules**. **2** Computer-based systems subjected to **Chapter 4, Part X of the Rules for the Survey and Construction of Steel Ships** are to be subjected to the factory acceptance test specified in **10.3**. However, for computer-based systems which have already received approval of use from the Society, plans and documents which obtained at the time of the type approval may be acceptable. **10.1.2 Definitions** The definitions of terms which appear in this chapter are as specified in **Chapter 4, Part X of the Rules for the Survey and Construction of Steel Ships** unless otherwise specified.	
10.2 Application	E27(Rev.1) 6.2
10.2.1 Application Forms	

Amended	Remarks
The manufacturer who makes an application for approval of use of the computer based system is to submit the appropriate application form (**Form 7-10**) filled in with necessary data and information to the Society. **10.2.2 Documents to be Submitted** **1** Three copies each of the following documents are to be submitted to the Society with the application form specified in **10.2.1**. (1) Drawings and data for approval: The following drawings and data: (a) Computer-based system asset inventory (**4.4.1(1), Part X of the Rules for the Survey and Construction of Steel Ships**) (b) Topology diagrams (**4.4.1(2), Part X of the Rules for the Survey and Construction of Steel Ships**) (c) Description of security Capabilities (**4.4.1(3), Part X of the Rules for the Survey and Construction of Steel Ships**) (d) Test procedure for security Capabilities (**4.4.1(4), Part X of the Rules for the Survey and Construction of Steel Ships**) (e) Secure development lifecycle (**4.4.1(6), Part X of the Rules for the Survey and Construction of Steel Ships**) (f) Other drawings and data deemed necessary by the Society (2) Drawings and data for reference: The following drawings and data: (a) Security configuration Guidelines (**4.4.1(5), Part X of the Rules for the Survey and Construction of Steel Ships**) (b) Plans for maintenance and Verification (**4.4.1(7), Part X of the Rules for the Survey and Construction of Steel Ships**) (c) Information supporting incident response and recovery plans (**4.4.1(8), Part X of the Rules for the Survey and Construction of Steel Ships**) (d) Management of change plan (**4.4.1(9), Part X of the Rules for the Survey and Construction of Steel Ships**) (e) Other drawings and data deemed necessary by the Society **2** Notwithstanding the requirements in **-1**, where the documents are duplicated by the ones at the previous approval for other computer based systems, part or all of the documents may be omitted. However, test programs and procedures specified in **-1(1)(a)** and **(b)** are not be exempted from submission.	
10.3 Factory Acceptance Test The objective of factory acceptance test is to demonstrate by testing and/or analytic evaluation that the computer-based	E27(Rev.1) 6.3

Amended	Remarks
system complies with applicable requirements in **Chapter 4, Part X of the Rules for the Survey and Construction of Steel Ships**. The survey and factory acceptance test is to be carried out at the supplier's premises or at other works having the adequate apparatus for testing and inspection. After completed plan approval and survey/ factory acceptance test, the Society will issue a System certificate that is to accompany the computer-based system upon delivery to the system integrator.	
10.3.1 General Survey Items The supplier is to demonstrate that design, construction, and internal testing has been completed. It is to also be demonstrated that the system to be delivered is correctly represented by the approved documentation. This is to be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (**10.2.2-1(1)(a)**) and the topology diagrams (**10.2.2-1(1)(b)**).	E27(Rev.1) 6.3.1
10.3.2 Test of Security Capabilities The supplier is to test the required security capabilities on the system to be delivered. The tests are to be carried out in accordance with the approved test procedure in **10.2.2-1(1)(c)** and be witnessed/accepted by the class surveyor. The tests are to provide the surveyor with reasonable assurance that all requirements are met. This implies that testing of identical components is normally not required.	E27(Rev.1) 6.3.2
10.3.3 Correct Configuration of Security Capabilities The supplier is to test/demonstrate for the class surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in **10.2.2-1(2)(a)**. This demonstration may be carried out in conjunction with testing of the security capabilities. The security settings are to be documented in a report, e.g. a ship-specific instance of the configuration guidelines.	E27(Rev.1) 6.3.3
10.3.4 Secure Development Lifecycle The supplier is to, in accordance with documentation in **10.2.2-1(1)(e)**, demonstrate compliance with requirements for secure development lifecycle in **4.5, Pare X of the Rules for the Survey and Construction of Steel Ships**.	E27(Rev.1) 6.3.4
(1) Controls for private keys (*IEC* 62443-4-1/SM-8) This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity. The supplier is to present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access. The policies and procedures are to address roles, responsibilities and work processes. The technical controls are to include e.g. physical access restrictions and cryptographic hardware (e.g. Hardware security module) for storage of the private key.	E27(Rev.1) 6.3.4.1
(2) Security update documentation (*IEC* 62443-4-1/SUM-2)	E27(Rev.1) 6.3.4.2

Amended	Remarks
The supplier is to 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 are to include the items listed in **4.5.3, Pare X of the Rules for the Survey and Construction of Steel Ships**.	
(3) Dependent component security update documentation (*IEC* 62443-4-1/SUM-3) The supplier is to present management system documentation, as required by **4.5.4, Pare X of the Rules for the Survey and Construction of Steel Ships**, 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 is to address how to manage risks related to not applying the updated acquired software.	E27(Rev.1) 6.3.4.3
(4) Security update delivery (*IEC* 62443-4-1/SUM-4) The supplier is to present management system documentation, as required by **4.5.5, Pare X of the Rules for the Survey and Construction of Steel Ships**, 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.	E27(Rev.1) 6.3.4.4
(5) Product defence in depth (*IEC* 62443-4-1/SG-1) The supplier is to present management system documentation, as required by **4.5.6, Pare X of the Rules for the Survey and Construction of Steel Ships**, 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 computer-based system during installation, maintenance and operation. Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.	E27(Rev.1) 6.3.4.5
(6) Defence in depth measures expected in the environment (*IEC* 62443-4-1/SG-2) The supplier is to present management system documentation, as required by **4.5.7, Pare X of the Rules for the Survey and Construction of Steel Ships**, 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.	E27(Rev.1) 6.3.4.6
(7) Security hardening guidelines (*IEC* 62443-4-1/SG-3) The supplier is to present management system documentation, as required by **4.5.8, Pare X of the Rules for the Survey and Construction of Steel Ships**, substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system. The guidelines are to specify how to reduce vulnerabilities in the system by removal/prohibiting /disabling of unnecessary software, accounts, services, etc.	E27(Rev.1) 6.3.4.7

10.4 Approval

10.4.1 Certificate

When the results of the examinations of submitted drawings and data and the tests specified in **10.2** and **10.3** are confirmed appropriate, the Society approves the computer based system (hereinafter referred to as "approved computer based system") and issues the relevant approval certificate.

10.4.2 Validity of Approval

The certificate specified in **10.4.1** is to be valid until a date not exceeding 5 *years* from its date of issue. However, when the approval is renewed in accordance with **10.4.3**, the new certificate is to be valid until a date not exceeding 5 *years* from the date of expiry of the existing certificate.

10.4.3 Renewal of Approval

1 In the case of application for renewal of approval, the manufacturer is to submit to the Society the appropriate application form (**Form 7-10**) accompanied with a copy of the certificate previously issued. The changes in particulars of the approved computer based system, quality system of manufacturer, etc., if any, are to be described in the application.

2 When the particulars of the approved computer based system, quality system of manufacturer, etc. remain unchanged, the Society approves the renewal of approval and issues a new certificate. The manufacturer who received the new certificate is to return the existing certificate to the Society as soon as possible.

10.5 Changes in Particulars of Approved Computer Based System, Quality System of Manufacturer, etc.

10.5.1 Changes in Particulars of Approved Computer Based System, Quality System of Manufacturer, etc.

1 In cases where the particulars of the approved computer based system, quality system of manufacturer, etc. are intended to be changed, the manufacturer is to submit to the Society the appropriate application form for changes (**Form 7-10**) accompanied with the following documents.

(1) explanatory notes for changes (three copies),

(2) necessary drawings and data (three copies each), and

(3) a copy of the certificate previously issued.

2 Upon examination of the documents, etc. according to **-1**, a confirmation test for changes is to be carried out when considered necessary by the Society. The details of the confirmation test are to be determined by the Society in consideration of the nature and extent of changes.

3 When confirmation tests are carried out, the manufacturer is to produce a report of the test and is to submit three copies to the Society upon receiving confirmation from the Society's surveyor.

4 When the results of the examination for documents and the confirmation test specified in **-1** to **-3** are confirmed to be satisfactory, the Society reissues the certificate with contents duly revised. The manufacturer who received the new certificate is to return the existing certificate to the Society as soon as possible.

5 In the case specified in **-4**, the validity of the certificate is not changed in principle.

10.6 Revocation of Approval

10.6.1 Revocation of Approval

1 In cases where any of the following **(1)** to **(5)** is applicable, the Society may revoke approval based on the requirements in this chapter. In such cases, the Society is to notify the manufacturer of the revocation.

(1) Where the result of the confirmation tests were found unsatisfactory.
(2) Where the valid term of the certificate has expired.
(3) Where the confirmation test was not carried out without any unavoidable reason.
(4) Where withdrawal of the approval has been offered by the manufacturer.
(5) Where the Society judged the approved computer based system to be unsuitable in the light of the service records of the shipboard automation equipment.

2 The manufacturer who received a notice of revocation of approval is to return the certificate of the relevant computer based system to the Society immediately.

10.7 Markings

10.7.1 Markings

Manufacturers of the approved computer based systems are, in principle, to mark their products before shipment for identification of approved equipment; in addition, at least the following items to be marked at a suitable place:

(1) Manufacturer name or equivalent
(2) Type No. or symbol
(3) Serial No. and date of manufacture

Amended	Remarks

(4) Particulars or ratings

(5) Approval number

EFFECTIVE DATE AND APPLICATION

1. The effective date of the amendments is 1 July 2024.

2. Notwithstanding the amendments to the Guidance, the current requirements apply to ships for which the date of contract for construction is before the effective date.

* “contract for construction” is defined in the latest version of IACS Procedural Requirement (PR) No.29.

IACS PR No.29 (Rev.0, July 2009)

1. The date of “contract for construction” of a vessel is the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. This date and the construction numbers (i.e. hull numbers) of all the vessels included in the contract are to be declared to the classification society by the party applying for the assignment of class to a newbuilding.

2. The date of “contract for construction” of a series of vessels, including specified optional vessels for which the option is ultimately exercised, is the date on which the contract to build the series is signed between the prospective owner and the shipbuilder.

For the purpose of this Procedural Requirement, vessels built under a single contract for construction are considered a “series of vessels” if they are built to the same approved plans for classification purposes. However, vessels within a series may have design alterations from the original design provided:

(1) such alterations do not affect matters related to classification, or

(2) If the alterations are subject to classification requirements, these alterations are to comply with the classification requirements in effect on the date on which the alterations are contracted between the prospective owner and the shipbuilder or, in the absence of the alteration contract, comply with the classification requirements in effect on the date on which the alterations are submitted to the Society for approval.

The optional vessels will be considered part of the same series of vessels if the option is exercised not later than 1 year after the contract to build the series was signed.

3. If a contract for construction is later amended to include additional vessels or additional options, the date of “contract for construction” for such vessels is the date on which the amendment to the contract, is signed between the prospective owner and the shipbuilder. The amendment to the contract is to be considered as a “new contract” to which **1.** and **2.** above apply.

4. If a contract for construction is amended to change the ship type, the date of “contract for construction” of this modified vessel, or vessels, is the date on which revised contract or new contract is signed between the Owner, or Owners, and the shipbuilder.

Note:
This Procedural Requirement applies from 1 July 2009.