RUSSIAN MARITIME REGISTER OF SHIPPING

GUIDELINES

ON CYBER SAFETY

ND No. 2-030101-040-E

St. Petersburg
2021

GUIDELINES ON CYBER SAFETY

Guidelines on Cyber Safety of Russian Maritime Register of Shipping have been approved in accordance with the established approval procedure and come into force on 1 January 2021.

The present edition of the Guidelines is based on IACS Recommendation No. 166 (*Recommendation on Cyber Resilience*).

The Guidelines are published in Russian and English in electronic format.

REVISION HISTORY

(purely editorial amendments are not included in the Revision History)

No amendments

1 GENERAL

1.1 SCOPE OF APPLICATION

1.1.1 Guidelines on Cyber Safety[1] contain the recommendations on design, manufacture, maintenance and testing of the shipboard computer based systems, as well as recommendations applicable to the safety management systems (SMS).

1.1.2 Recommendations of the Guidelines are aimed at implementation of provisions of IMO resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems" subject to which not later than at the first annual verification of a Document of Compliance (DOC) after 1 January 2021 cyber risks related to SMS shall be taken into account in compliance with the provisions of IMO circular MSC-FAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management".

1.1.3 The Guidelines apply to ships contracted for construction on or after 01.01.2021, unless otherwise stated in particular provisions of the Guidelines.

1.1.4 The Guidelines supplement other requirements of Russian Maritime Register of Shipping (RS) applicable in compliance with class notation and purpose of a ship.

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

1.2 DEFINITIONS AND EXPLANATIONS

1.2.1 Definitions and explanations relating to general terminology of the RS rules and guidelines are given in 1.1, Part I "Classification" of the Rules for the Classification and Construction of Sea-Going Ships[1] and 1.1, Part I "General Regulations for Technical Supervision" of the Rules for Technical Supervision during Construction of Ships and Manufacture of Materials and Products for Ships[2].

1.2.2 Basic terms, definitions and abbreviations.

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

Attack surface is the computer based systems which can be accessed externally either through network or locally. The term defines the total number of possible vulnerabilities. The more components of computer based systems, the more potential vulnerabilities and the attack surface are available, respectively.

Bug is unintended functionality in software.

Categories of maintenance are categories assigned to a software maintenance activity based upon the reason for undertaking the maintenance, which may be:

resolving software bugs (Bug fix);

adding additional functionality (Feature release);

maintaining conformity with regulations (Compliance update);

protecting against cyber threats (Security update);

addressing software and/or hardware that is no longer supported (Obsolescence update);

or some combinations of the above.

Company is the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who, on assuming such responsibility, has agreed to take over all the duties and responsibility imposed by the International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code).

Computer based system is combination of interacting programmable devices and/or IT systems organized to achieve one or more specified purposes. Computer based system may be a combination of subsystems connected via network. Shipboard computer based system may be connected directly or via public means of communications (e.g. Internet) to ashore based computer based systems, other ships' computer based system and/or other facilities.

Contingency Plan is the plan which provides essential information and establishes procedures to ensure effective response and recovery in case of a cyber incident affecting computer based system providing essential contribution.

Critical system is a technical system that the sudden operational failure of may result in hazardous situation.

---

[1] Hereinafter referred to as "the RS Rules/C".

[2] Hereinafter referred to as "the RS Rules/TS".

Cyber attack is any type of offensive maneuver that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and shipboard systems and data.

Cyber incident is an occurrence, which actually or potentially results in adverse consequences to a shipboard 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 resilience is 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 ship and/or threat to the environment.

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

Cyber safety is the condition of being protected against vulnerabilities resulting from inadequate operation, integration, maintenance and design of computer based systems, and from intentional and unintentional cyber threats.

Data quality is a characteristic showing the applicability of data generated, processed, transferred and stored in the operation of computer based systems on board. The data quality can be defined as following:

confidentiality – protection against a loss of confidentiality because of an unexpected or unauthorized disclosure of information;

integrity – protection against a loss of integrity because of an unexpected or unauthorized modification of information;

availability – protection against a loss of availability because of an unexpected or unauthorized destruction of the information or disruption of access to, or use of IT system.

Data provider is a person or company that supplies data necessary for the functioning of the shipboard computer based system.

Defense in breadth is a planned, systematic set of activities that seek to identify, manage, and reduce exploitable vulnerabilities in IT and OT systems, networks and equipment at every stage of the system, network, or sub-component life cycle. Onboard ships, this approach will generally focus on network design, system integration, operations and maintenance. The concept of this approach is the system protection against a particular attack where several independent techniques are used.

Defense in depth includes three controls:

physical controls that include all measures on restricting physical access of unauthorized persons to computer based systems;

technical controls that include all hardware and software means of information security intended for control of the network access to the components of computer based systems, firewalls, antivirus software, authentication and authorization systems;

administrative controls that include information security policy and procedures of the company. These documents are aimed at control of security management, distribution and protection of critical information, use of software and hardware in the company, as well as interaction of the crew with computer based systems and other external objects.

Demilitarized zone (DMZ) is a physical or logical sub network that contains and exposes external-facing services, as well as separating them from other components

of a local area network. Integrated restricted server network connecting two or more network zones to control data flow between the network zones. Generally, demilitarized zones are used to avoid direct communication between different network zones.

Essential systems are systems providing the safe operation of the ship.

Failure Mode and Effects Analysis (FMEA) is a technique to identify foreseeable causes of independent failures together with their effects on the hardware, software or process, based on a systematic decomposition into elements. The technique can be used to demonstrating that foreseeable risks have been identified and accounted for.

Firewall is a type of security barrier between various network media consisting of a specialized device or a set of several components and engineering techniques through which the whole traffic from one network medium shall enter the another one and vice versa, thus, only the authorized traffic complying with the local security policy shall be transferred.

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.

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

Integrated system is interconnected system combining a number of interacting shipboard equipment organized to achieve one or more specified purposes.

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

Intrusion Prevention System (IPS) is a device or software application that monitors network or system activities to prevent malicious activities or policy violations.

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

Local control is control from a location in the immediate vicinity of the controlled item.

Malware is generic term for a variety of malicious software, which may adversely impact the performance of computer systems.

Managed Network is network which uses managed switches, that allows connected network devices to communicate with each other, and also gives the network administrator greater control over managing and prioritizing network traffic. Network traffic can be controlled and prioritized through configuration changes.

Network is a group of two or more computer systems linked together.

Network hub is a common connection point for devices in a network.

Network router is a network device which is responsible for routing traffic from one network to another network.

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.

Operational technology (OT) is devices, sensors, software and associated networking that monitor and control shipboard systems.

Patches are software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve computer based systems or applications.

Producer is a firm that manufactures the shipboard equipment and associated software.

Programmable device is a physical component where software is installed.

Protocols are a common set of rules and signals that computers and programmable devices use to communicate.

Quality of service (QoS) is the measurable end-to-end performance properties of a network service:

bandwidth;

delay;

jitter;

packet loss.

QoS technology is traffic prioritization technology, i.e. concession of different priority to different traffic classes in the network service and transfer.

Recovery is a function for support back-up and restoration of the shipboard computer based systems to restore the ship to a safe condition in a timely manner.

Removable media are a collective term for different methods of storing and transferring data between computers without the aid of a network. This includes laptops, USB memory sticks, CDs, DVDs, diskettes, etc.

Risk assessment is the process which collects information and assigns values to risks as a base on which to make decision on priorities and developing or comparing courses of action.

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

Security Information Event Monitoring (SIEM) is software application that provides the ability to gather security data from IT and OT system components and present that data as actionable information via a single interface.

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

Simulation test is system testing where the equipment under control is partly or fully replaced with simulation tools, or where parts of the communication network and lines are replaced with simulation tools.

System categories (I, II, III) are categories based on their effects on occurrence of dangerous situations for human safety, safety of the ship and/or threat to the environment:

category I – those systems, failure of which will not lead to dangerous situations for human safety, safety of the ship and/or threat to the environment. Systems providing performance of administrative tasks (recording of fuel oil consumption, maintenance organization, etc.) are related to category I;

category II – those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

The following is related to category II:

alarm and monitoring systems (according to 1.2.1, Part XV "Automation" of the RS Rules/C);

indication systems (according to 1.2.1, Part XV "Automation" of the RS Rules/C);

internal communication systems;

cargo control and ballast management systems;

inert gas system control system;

bunkering control systems;

category III – those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the ship and/or threat to the environment.

The following is related to category III:

main and auxiliary machinery systems (according to 1.2.1, Part VII "Machinery Installations" of the RS Rules/C);

safety systems (according to 1.2.1, Part XV "Automation" of the RS Rules/C);

dynamic positioning systems.

System integrator is a party that integrates computer based systems, subsystems and software provided by suppliers into a system, as well as combines shipboard equipment into an integrated system. The system integrator may be entrusted with installation and integration of the system on board the ship.

Functions of the system integrator shall be performed by the builder/shipyard. The system integrator responsibilities may be entrusted to another organization, provided the relevant contract is available.

In case of system integration with the several parties involved at any stage, the only one party may be a system integrator and coordinate all the works required. In case of multistage integration, different system integrators may bear responsibility for the particular stages, however, only one party shall define the stages and perform overall coordination.

Test case is set of conditions, methods and expected results under which a tester will determine whether a software application is working according to the design specifications or not.

Unmanaged Network is network which uses unmanaged switches, that allows devices connected to a network to communicate with each other. These are plug-and-play switches that do not require or allow any user intervention, setup, or configuration.

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

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

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

DLP (Data loss prevention) is prevention of data loss or theft.

HMI is human machine interface.

IT system is a computer based system of category I that provides control functions for information/administrative tasks.

MAC (Media access control) address is a hardware address that differentiates one device on a network from another.

M2M is machine to machine Interface.

OT system is a computer based category II or III system that provides control, alarm, monitoring, safety or internal communication functions.

RAID is redundant array of independent disks.

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

2 TECHNICAL DOCUMENTATION

2.1 DESIGN DOCUMENTATION

2.1.1 Technical documentation for category I (where the interconnections with category II or III systems are available), II and III systems that shall be developed at the stage of the ship design and construction and submitted to the Register for review is specified in Table 2.1.1.

Table 2.1.1

Item No.	Name	Description	Note
1	Concept of computer based system	The document shall contain the following information: .1 purpose of computer based system with brief description of functions; .2 flowchart (plan) clearly identifying shipboard systems controlled/monitored by the computer based system. The flowchart (plan) shall also contain the following information: communications with external network for monitoring, control and performance of administrative functions; communications with other computer based systems	Shall be submitted to the Register for information
2	Description of data transmission networks	The document shall contain the following information: .1 physical location of the system and subsystem components (e.g., name of a space, deck of location, etc.); .2 category I system communications with category II or III systems; .3 network topology of systems and subsystems (star, ring, etc.); .4 applicable network technologies (e.g, Gigabit Ethernet, Fast Ethernet); .5 applicable network cables (twisted pair, fibre optic, etc.); .6 communications from controllers and field devices (MODBUS, Fieldbus, etc.); .7 network diagrams indicating the devices, nodes, network cable details and general locations of the equipment; .8 list of IT and OT systems indicating their categories; .9 data flows and network devices or resources potentially limiting them; .10 details of external connections for remote access; .11 access points and interfaces, including machine-to-machine (M2M) interfaces; .12 logical diagrams of shipboard networks	Shall be submitted to the Register for information

2.2 SHIPBOARD DOCUMENTATION

2.2.1 Documentation to be available on board the ship is given in Table 2.2.1.

Table 2.2.1

Item No.	Name	Description	Note
1	Description of data transmission networks	The document shall contain the following information: .1 physical location of the system and subsystem components (e.g., name of a space, deck of location, etc.); .2 category I system communications with category II or III systems; .3 network topology of systems and subsystems (star, ring, etc.); .4 applicable network technologies (e.g, Gigabit Ethernet, Fast Ethernet); .5 applicable network cables (twisted pair, fibre optic, etc.); .6 communications from controllers and field devices (MODBUS, Fieldbus, etc.); .7 network diagrams indicating the devices, nodes, network cable details and general locations of the equipment; .8 list of IT and OT systems indicating their categories; .9 data flows and network devices or resources potentially limiting them; .10 details of external connections for remote access; .11 access points and interfaces, including machine-to-machine (M2M) interfaces; .12 logical diagrams of shipboard networks	
2	Inventory of components of category II and III computer based systems	For devices having interface connections with computer based systems (e.g., programmable logical controllers (PLC), remote input/output (I/O), human machine interface (HMI) stations, sensors, variable speed drives,	Shall be applied to ships contracted for construction on or after 01.01.2021 and existing ships after 01.01.2022. For existing ships

Item No.	Name	Description	Note
		circuit breakers, physical servers, computers, workstations, storage units, etc.) and network communication devices, (e.g., switches, routers, firewalls, interface converters, etc.) the following shall be indicated (for each device): .1 name; .2 brand/producer (supplier); .3 model; .4 version of the operating system or embedded firmware and software version; .5 description of settings, where applicable; .6 information on the equipment location (e.g., accommodation space/engine room)	the inventory shall be prepared by the company. For ships contracted for construction on or after 01.01.2021, the inventory shall be prepared by the system integrator prior to delivery of the ship. During the ship operation, immediately after making changes in the computer based system (software update, replacement of equipment, except replacement by the similar equipment without software changes), the responsible personnel on board the ship shall introduce the relevant amendments to the inventory indicating the date and reason of changes, as well as information on the persons making the changes
3	Inventory of category II and III computer based systems (logic level)	The document shall contain the following information: .1 applicable IP address ranges, indicating: list of network devices (indicating IP address) using IP addresses in this range; functional description of IP address range; interconnections with other ranges; .2 for devices with non IP addresses: list of devices, indicating MAC addresses or addresses specific to the industrial protocols on the network; functional description of the network;	Shall be applied to ships contracted for construction on or after 01.01.2021. The inventory shall be prepared by the system integrator prior to delivery of the ship. During the ship operation, immediately after making changes in the computer based system (software update, replacement of equipment, except replacement by the similar equipment without software changes), the responsible

Item No.	Name	Description	Note
		.3 network connection points, indicating: list of access ports; addressing, if there is a special protocol; list of connected devices; .4 logical servers and computers, indicating, where applicable: IP addressing (network, subnetwork mask, gateways); operating system version; underlying physical server; applications and their versions; .5 connectors and communicating field devices (remote I/O, smart sensors, etc.) indicating: IP addressing (network, subnetwork mask, gateways), associated MAC address and network or address specific to the industrial protocols on the network, where necessary	personnel on board the ship shall introduce the relevant amendments to the inventory, indicating the date and reason of changes, as well as information on the persons making the changes
4	Inventory of software of category II and III computer based systems	The document shall contain the following information: .1 software name; .2 software publisher; .3 software installation date and version number; .4 software maintenance type (local/remote); .5 accounts type (generic/dedicated); .6 access control with read, write or execution rights; .7 license number, where applicable; .8 type and date of the software maintenance performed; .9 information on the company indicating the person performing software maintenance	Shall be applied to ships contracted for construction on or after 01.01.2021. The inventory shall be prepared by the system integrator prior to delivery of the ship. During the ship operation, immediately after making changes in the computer based system (software update, replacement of equipment, except replacement by the similar equipment without software changes), the responsible personnel on board the ship shall introduce the relevant amendments to the inventory, indicating the date and reason of changes,

Item No.	Name	Description	Note
			as well as information on the persons making the changes
5	Risk assessment	In compliance with Section 3	
6	Instructions on Cyber Safety on Board the Ship	The document shall contain the following information: description of actions to prevent cyber incidents; Contingency Plan; software maintenance procedures	Shall be applied to ships contracted for construction on or after 01.01.2021 and existing ships after 01.01.2022. The document shall be developed by a company based on the results of risk assessment and recommendations of the equipment producers
7	List of service providers	The document shall contain the following information: list of equipment indicating the name of software maintained by the service provider; name of organization licensed for maintenance of particular equipment	The requirements to service providers are specified in 4.3.2.3. Shall be applied to existing ships and ships contracted for construction on or after 01.01.2021. The document shall be developed and updated, where necessary, by the company during the ship life cycle
8	Description of security perimeter	The document shall contain the following information: list of spaces, indicating the list of equipment (communication equipment, computers, controllers) located inside each space; description of measures on access restriction	Shall be applied to ships contracted for construction on or after 01.01.2021 and existing ships after 01.01.2022. For existing ships the description shall be prepared by the company. For ships contracted for construction on or after 01.01.2021, the description shall be

Item No.	Name	Description	Note
			prepared by the system integrator prior to delivery of the ship. The description shall be updated, where necessary, by the company during the ship life cycle

3 RISK ASSESSMENT

3.1 GENERAL REQUIREMENTS TO RISK ASSESSMENT

3.1.1 Risk assessment of cyber attacks and cyber incidents shall be performed for category I (where communications with category II and III systems is available), II and III computer based systems.

3.1.2 For ships contracted for construction on or after 01.01.2021, risk assessment shall be performed by the system integrator, for existing ships risk assessment shall be performed by the company. Risk reassessment shall be performed in case of changes (system configuration change, replacement of components by new ones differing from those used earlier, supplement of new functions, etc.) to the category I (where communications with category II and III systems are available), II and III computer based systems.

3.1.3 For ships contracted for construction on or after 01.01.2021, risk assessment for the prototype ship may be performed in case there are no significant differences between the computer based systems of the ships of a series. The following differences are considered significant:

by number of interconnected computer based systems;

by functions performed by the computer based systems;

by composition of the network communication devices;

by maintenance type (local, remote) of computer based systems;

by available connections of the shipboard computer based systems with external systems outside the ship.

3.1.4 During risk assessment for existing ships, general risk assessment may be performed for the ships of one project in case there are no differences between the computer based systems of various ships specified in 3.1.3.

3.1.5 During risk assessment, type of the ship, available communications between different systems and between the ship and the shore or between the ship and another object shall be considered.

3.1.6 Risk analysis shall identify immediate effect on the equipment, safety of the ship, human safety and threat to the environment. Risk analysis shall consider the effect on the integrated or interfaced systems.

3.1.7 In case of remote access to the shipboard systems, risk assessment shall take into account threats associated with remote access.

3.1.8 Risk assessment results shall be documented. The document shall contain qualitative and/or quantitative risk assessment, risk acceptance criteria, as well as information on the severity level of the risk occurrence consequences.

3.1.9 Based on risk assessment performed, taking into consideration the producers' recommendations, the Instructions on Cyber Safety on Board the Ship shall be developed.

3.2 TYPICAL RISKS

3.2.1 During the assessment, the risks related to the peculiar features and operating conditions of different ship types shall be taken into consideration. At least the following risks shall be considered:

.1 gaining unauthorized access;

.2 operation failure of category II and III systems due to physical damage of the system components, software damage, violation of data integrity, loss of power, etc.;

.3 unintended actions of the personnel operating the system;

.4 infection of software and hardware of category I (where communications between category II and III systems are available), II and III systems.

3.3 RISK ASSESSMENT STANDARDS

3.3.1 Risk assessment related to operation of the shipboard computer based systems shall be performed using standardized procedures.

3.3.2 During risk assessment, the national and/or international standards on risk management and risk assessment, e.g. ISO/IEC 27005 and ISO/IEC 31010 or other equivalent standards shall be used.

4 TECHNICAL REQUIREMENTS

The technical requirements specified in this Section are aimed at provision of compliance with the target and functional requirements on cyber safety on board the ships.

In the context of design and construction, the Guidelines are aimed at provision of cyber resilience of the ship that shall be maintained during the ship life cycle. For achievement of this goal, the following target and functional requirements shall be met.

Identification (I) means the availability of complete information on all devices, systems, networks and data flows between the systems and system components on board the ship for taking safety measures against cyber incidents, identification of cyber attacks and cyber incidents, taking countermeasures in the event of cyber incidents and recovery of systems exposed to cyber incidents.

Functional requirements:

I1: information that flows among the shipboard OT systems and between shipboard OT systems and other systems shall be identified;

I2: interdependencies across critical systems and risks that can affect safety of the ship, human safety and environment when such systems are compromised shall be identified.

Protection (P) means the use of safety systems and devices to provide different safety of OT systems and the relevant information.

Functional requirements:

P1: IT and OT systems shall be designed to support secure configuration, secure integration and secure software maintenance;

P2: interoperability of OT systems shall be limited to identified critical functions only;

P3: IT and OT systems' network infrastructure shall be segmented by division into network zones;

P4: both physical and logical access to OT systems shall be restricted;

P5: the possibility of disruption to OT system which affect the availability of safety critical functions shall be minimized.

Detection (D) means provision of timely and effective identification of cyber incidents.

Functional requirements:

D1: means for monitoring of normal operations of OT systems shall be provided, based on continuous and/or on-demand self-diagnostics and connection quality and/or network performance monitoring tools. These tools shall be available at least on networks connecting OT systems and on networks connecting IT systems with OT systems.

Response (R) means isolation of the expansion and duration of possible disruption to OT systems and the relevant information.

R1: impact of cyber incidents shall be contained to the network zone of origin.

R2: extension of possible disruption to OT system which affects the availability of safety critical functions shall be minimized.

Recovery (RC) means restoration of OT systems in a timely manner to maintain the ship in a safe condition.

Functional requirements:

RC1: Equipment shall be designed to support back-up and restoration of OT systems to restore the ship to a safe condition in a timely manner.

The technical solutions differing from those specified in this Section may be used, in case they provide full compliance with the above target and functional requirements.

The summary indicating the particular paragraphs of the Guidelines providing compliance with the functional requirements is given in Table 4.

Table 4

Description of functional requirement	Section/para of the Guidelines
I1	4.1.1.1
I2	Section 3, 4.1.1.1
P1	4.1.1
P2	4.1.5.4
P3	4.1.5.6, 4.1.5.9, 4.1.5.10
P4	4.1.5.5, 4.1.6, 4.1.7
P5	4.1.5.3, 4.1.5.4
D1	4.1.3
R1	item 6 of Table 2.2.1
R2	item 6 of Table 2.2.1
RC1	4.1.4, 4.3.1.6

4.1 DESIGN REQUIREMENTS

4.1.1 General requirements.

4.1.1.1 System integrator shall develop the documentation specified in Table 2.1.1.

4.1.1.2 At design stage, the producer of the computer based system shall perform the Failure Mode and Effect Analysis (FMEA) of the computer based system. Based on the analysis performed, technical safety measures shall be specified.

4.1.1.3 Protection shall be provided against unauthorized access to the system components, data exchange functions and functions affecting safety of the ship, human safety and threat to the environment.

4.1.1.4 When selecting the equipment, the operating conditions, possibility of mechanical damage or unauthorized access to installation points of the computer based system components shall be considered. The computer based system components shall be located in the points complying with the technical parameters (ingress protection (IP) rating of the equipment, working temperature range, etc.) of the equipment taking into consideration instructions of the equipment producer and the requirements of the Guidelines.

4.1.1.5 The computer based system shall be designed in such a way that the confidentiality, integrity, and availability of the data necessary for safety of the ship shall be provided.

4.1.2 Cyber incident prevention.

4.1.2.1 Based on the Failure Mode and Effects Analysis (FMEA) performed, the following network protection safeguards may be provided:

.1 management of public key infrastructure *(*PKI) and network user account, including M2M networks;

.2 authentication or restricted privileges for remote access;

.3 physical access control to network access points;

.4 granting access for user or system to information and resources at least required for success task performance (Least Privilege Policy);

.5 data encryption for remote access;

.6 data integrity check;

.7 separation of IT and OT systems. Where necessary to communicate IT and OT systems, the requirements of 4.1.5.7 and 4.1.5.9 shall be met;

.8 QoS technology.

4.1.2.2 Where practicable, and subject to the producers' requirements, anti-virus software shall be installed on the computers or other programmable devices having a standard operating system. The anti-virus software shall not affect the performance of category II and III systems. For programmable logic controllers or other devices without standard operating system, security measures shall be applied in accordance with the producers' recommendations.

4.1.2.3 In case of demilitarized zone (*DMZ*), anti-virus software may be installed on the application server only, provided that the software components of the computer based systems are maintained through the application server. Where the software components

of the computer based systems maintained through the dedicated patch management server, anti-virus software may be installed on this server only.

4.1.2.4 Anti-virus software shall be updated automatically. Where automatic update is not possible, manual update is allowed at least one a week subject to Internet access.

4.1.3 Cyber incident detection.

4.1.3.1 Based on the Failure Mode and Effects Analysis (FMEA) performed, and according to recommendations of the producers, cyber incident detection safeguards shall be provided to limit the cyber incident impact to the network zone of origin. The following detection safeguards may be used:

Intrusion Detection System (IDS) and Intrusion Protection System (IPS);

connection quality monitoring tools;

network performance monitoring system;

malicious code detection tools;

Security Information Event Monitoring (SIEM).

4.1.3.2 The shipboard computer based systems shall apply monitoring, logging and alarm systems that shall provide at least:

.1 control and alarm of the following cyber attacks:

network attacks (network traffic analysis);

IP-spoofing (use of foreign IP-source address);

Man-in-the-Middle attacks (cyber attacks where an attacker is able to read and modify the data the communicants are exchanging);

application attacks;

web intelligence;

port forwarding;

gaining unauthorized network access;

attacks using Trojan or computer worm malware;

.2 control and alarm of the following failures:

absence of network connection of equipment within a specified time interval,

failure of components of the computer based systems;

.3 monitoring and logging of events related to the following:

authentication of users,

creating, changing, deleting and locking of user accounts,

event logging (downloading and deleting of records, capacity alarm),

system setting;

software update,

backing up and recovery of database,

start or rebooting of system and services, as well as system log,

violation of firewalling or network routing procedures,

connection of unknown device not related to the network,

equipment connection to/disconnection from the network.

4.1.3.3 The network monitoring systems shall provide adequate information describing the cyber incident for the use of the intended user. When the ship has provision for remote connectivity, it shall be possible to identify a cyber incident originating external to ship.

4.1.4 Recovery.

4.1.4.1 Recovery measures shall be developed by the producer and/or system integrator. Critical systems shall have the capability to support back-up and restore in a timely, complete and safe manner.

4.1.4.2 The following measures to restore the computer based systems that have been impaired due to a cyber incident shall be provided:

.1 redundancy or backup measure of data and components of the computer based systems;

.2 controlled shutdown, reset or restart of affected systems or system components.

4.1.5 Network.

4.1.5.1 During design of the data transmission network, the standard interfaces shall be used, and volume of transmitted data and the required rate of data exchange among the system components shall be also considered to provide the required performance of the computer based systems. Capacity margin of the data transmission networks of at least 40 % shall be provided to effect the required performance of the computer based systems in case of their changing (addition of new functions, new system components, etc.) during the ship operation.

4.1.5.2 Redundancy of data channels for category II and III systems shall be provided in compliance with the requirements specified in Section 7, Part XV "Automation" of the RS Rules/C or based on the Failure Mode and Effects Analysis (FMEA) performed.

4.1.5.3 Fault in one part of the ship network due to failure of the network devices or cyber incident shall not affect the remaining systems connected to unaffected network.

4.1.5.4 To provide fault tolerance, during design of the computer based systems, the following requirements shall be met:

.1 for category II and III systems, connections between the systems and system components shall be resilient to faults with self-correcting properties (data retransmission/request, automatic switching to redundant channel, etc.) that guarantee to provide data to be transmitted without failures;

.2 for essential systems, the possibility of local control of systems and equipment shall be provided in case of a failure of the computer based system;

.3 the attack surface of category II and III systems shall be reduced by separating them (physically or logically) from non-critical data and processes;

.4 measures shall be taken to prevent ripple effects that can contaminate the remaining systems and subsystems as a result of a single cyber incident;

.5 for category II and III computer based systems, in the event of failure of any network equipment or impairment due to a cyber incident, the shipboard equipment controlled by the said computer based systems shall go to a defined safe state maintaining safe operation of the ship.

4.1.5.5 The network access control system which ensures the capability to identify and authenticate valid sessions and reject any usage of invalid session identifiers shall be provided.

4.1.5.6 Segregation of networks shall be made carried out as per the computer based system philosophy and upon results of the Failure Mode and Effects Analysis (FMEA).

The segregation can be done by using either physically different networks or by using different logical networks. The perimeter of each network zone shall be well defined and documented.

4.1.5.7 When access between different network zones is allowed, it shall be controlled at the perimeter by using the appropriate boundary protection devices (e.g., proxy servers, routers, firewalls, unidirectional gateways, guards and encrypted tunnels). The demilitarized zone (DMZ) shall be provided between the shipboard network and external network (shore-based network, network of other ship or object). Firewalls shall be provided between the networks of category I and II systems and between the networks of category I and III systems.

4.1.5.8 Networks that are provided with remote access shall be controlled to prevent any security risks from connected devices by use of firewalls, routers and switches complying with the requirements of IEC 61162-460. External access of such connections shall be secured to prevent unauthorized access.

4.1.5.9 Segregation of networks shall be performed meeting the following requirements:

.1 no permanent gateway between public networks (networks used by the passengers, networks not related to those of IT and OT systems used by the crew) and other area networks shall be installed;

.2 non-secured wireless access shall not be connected to the network perimeter for OT systems;

.3 access (physical or logical) to ports for removable devices shall be restricted. If sensitive data are contained inside the network, it is recommended to provide physical locks of ports to prevent unauthorized access to these ports;

.4 no data communication between different network zones is permitted, except through appropriate boundary protection devices according to 4.1.5.7.

4.1.5.10 Within the zone (set of the computer based system components complying with the general safety requirements), segmentation of the network (segmentation of the network for the network traffic optimization and/or improvement of the network safety in general) shall be implemented as per identified risk level. Critical systems (including communications cables) shall be grouped and separated into zones with common security levels in order to manage security risks and to achieve a desired target security level for each zone.

During segmenting, the following requirements shall be met:

.1 for networks of category II system, physical or logical segmentation (virtual local area network (VLAN)) shall be provided;

.2 for networks of category III system, physical segmentation shall be provided and independent switches shall be used;

.3 segmentation shall be such as to prevent loss of critical systems upon a single failure (e.g. equipment fault, cable breaking, software bug) for category III systems;

.4 interconnection between networks that include systems of lower category and those of higher category shall result in all interconnected systems being treated as the highest category included, e.g., if a network that includes systems of category I is connected to a network that includes category III systems, both networks shall be regarded as category III;

.5 two network devices between the segments of critical systems shall be provided. Where loss of connection between the segments may result in emergency, both network devices shall operate in real time. They shall be arranged such that in case of any device failure or cyber incident, the second device shall be capable to provide functioning of the entire system.

4.1.5.11 Where wireless communication channels are used, the following requirements shall be met:

.1 capability to uniquely identify and authenticate all users (humans, software or devices) engaged in wireless communications shall be provided;

.2 capability to authorize (granting authorization for certain action performance), monitor and enforce usage restrictions for wireless connectivity to the control system shall be provided;

.3 encryption mechanisms to prevent loss of integrity and confidentiality of information during communication shall be used.

4.1.5.12 Radio frequencies and power levels of the shipboard wireless data transmission network shall comply with the requirements of the International Telecommunication Union (ITU) and the requirements of Administration.

When using wireless data transmission network, the requirements of a port and local regulations that prohibit use of wireless data transmission due to frequency and power limitations shall be considered.

4.1.6 Computer based system access control.

4.1.6.1 Components of the computer based systems shall be installed at a location providing effective and efficient operation of ship by the crew and various stakeholders who need to access to computer based systems for update, maintenance, repair, replacement, etc.

A document shall be developed describing security perimeter where the following information shall be indicated:

inventory of spaces (name of a space, deck of location, etc.), indicating the equipment (communication equipment, computers, controllers) located inside each space;

description of measures on access restriction.

For existing ships the description shall be prepared by the company. For ships contracted for construction on or after 01.01.2021, the description shall be prepared by the system integrator prior to delivery of the ship.

4.1.6.2 To prevent unauthorized access, category II and III computer based systems shall be located in spaces that can be locked or restricted spaces (e.g., wheelhouse, electric rooms, machinery spaces). If this is not possible, then the equipment shall be located in lockable cabinets or consoles.

4.1.6.3 Measures to restrict physical access to the components of category II and III computer based systems located in the security perimeter, e.g. lock, surveillance camera, etc.

4.1.6.4 The connection to the network shall be both physically and logically blocked, except when connecting an external device for maintenance of the system or equipment.

4.1.7 Remote access.

4.1.7.1 The requirements apply to the shipboard IT and OT systems which can be accessed from a remote location (not on board the ship).

4.1.7.2 Data transmission to category II and III shipboard computer based systems which is critical for the safety of navigation, power and cargo management, etc., shall be protected against unauthorized access and measures necessary to mitigate the risks arising due to remote access shall be taken. The capability to terminate a connection from the onboard terminal and revert to the known and uncorrupted state shall be provided. The network equipment supporting the above mentioned functions may be used for termination.

In case of cyber incident, the system shall provide the possibility of local control.

4.1.7.3 Systems and equipment shall have capabilities necessary to prevent interruptions to remote access sessions interfering with the integrity and availability of OT systems and the data used by OT systems.

4.1.7.4 The ships provided with facility for remote access for maintenance, shall implement the following safeguards:

.1 hardware or software mechanisms shall be provided to manage the acceptance of remote maintenance;

.2 it shall be possible at all times to cancel remote maintenance from the ship;

.3 initiation of maintenance session shall be authenticated by the responsible personnel on board the ship. Passwords shall not be transmitted in unencrypted form. Tunneling traffic through an encrypting virtual private network (VPN) shall be adopted;

.4 activation of the maximum-trial period in the event of failed access attempts shall be provided;

.5 activation a lock-out period in the event of inactivity shall be provided;

.6 the system shall have the feature to block the access for remote maintenance feature during normal system operation. Express approval shall be limited and shall be accorded only for a precisely defined period of time;

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

4.1.8 Manual operation.

4.1.8.1 Manual backup of the system shall be provided. If systems are integrated or connected in other ways that could permit several systems to be affected simultaneously, then the implications of manual backup in these circumstances needs to be considered:

.1 identification of affected systems for planning manual response;

.2 identification of potentials for cascading failure of the systems.

4.1.8.2 The following requirements shall be met during design and manufacture of the local computer based machinery systems:

.1 local control systems shall include necessary human-machine interface (HMI) for effective local operation;

.2 local control systems shall be of a robust design suitable for the environmental exposure and the intended operation;

.3 local control systems shall be self-contained and not depend on other systems or external communications links;

.4 failure in remote control systems shall not prevent local operation;

.5 unused communications ports shall be disabled or access shall be restricted to prevent unauthorized connection to ports;

.6 facilities for selecting "local" at or near the controlled items shall be provided. When manual control is selected, any signals from the remote control system shall be ignored.

4.2 REQUIREMENTS TO EQUIPMENT

4.2.1 Equipment to be used in category II and III systems shall provide mitigation of the risk related to cyber attacks.

4.2.2 The network communication equipment for the shipboard computer based monitoring, control, logging and alarm systems, shall have verified compliance with the industry standards applicable to network communications equipment (e.g., IEC 62443 or equivalent standards) and shall be tested in compliance with the requirements of Section 12, Part IV "Technical Supervision during Manufacture of Products" of the RS Rules/TS.

4.2.3 The network communication equipment for the shipboard navigational systems and radio communication systems shall comply with the requirements of IEC 61162-460.

4.2.4 The network communication equipment for category II and III systems shall be able to detect the following states by performing self-diagnostics:

.1 link up of each port on the network device;

.2 link down of each port on the network device;

.3 power ON or hardware reset;

.4 network storm detection;

.5 fan failure (for devices using fan for cooling);

.6 abnormal temperature (only if the network device has an abnormal-temperature detection function).

Information on the status of the network communication equipment shall be accessible to the responsible personnel in the permanently attended places.

4.2.5 The network communication equipment for category II and III systems shall provide alarm functions to detect the following abnormal conditions:

.1 when a link is disconnected or the power is turned off for a network device;

.2 loss of a network device.

Alarm shall be provided in the permanently attended places. Forming of group malfunction alarm with interpretation of the alarm actuating in the points of the network equipment location is permitted.

4.2.6 The possibility of physical or logical locking of unused ports of the network devices shall be provided.

4.2.7 The network communication equipment shall be provided with the following configuration parameters:

.1 password encryption;

.2 password protected console ports;

.3 configurable session timeouts;

.4 flow control enabled;

.5 unused ports closed.

4.2.8 The electronic devices used to store data for category II and III systems shall be appropriate for intended use and suitable for the marine environment. Data stored on such devices shall be appropriately replicated to minimize data loss in case of device single failure.

4.3 REQUIREMENTS TO SOFTWARE

4.3.1 Software development.

4.3.1.1 The requirements of this Chapter apply to software of category II and III computer based systems.

4.3.1.2 Software shall be developed in compliance with the standards and procedures for software development adopted by the company.

4.3.1.3 Software shall be developed on the basis of specifications containing information on the purpose of development, tasks and functions to be performed by a software module.

4.3.1.4 During development, the software developer shall:

.1 document the development results;

.2 provide control and management of software changes (software versioning);

.3 document results of software testing to verify achievement of objectives, fulfillment of tasks and functions according to specifications for the software module.

4.3.1.5 For category I, II and III systems, security measures, such as authentication and authorization, shall be in place to prevent unauthorized or unintentional software modification (including software configuration) or software (local or remote) uninstallation.

4.3.1.6 The backup and recovery of software and data shall be considered during software design and development. The producer shall develop software and data recovery procedures.

4.3.2 Software maintenance.

4.3.2.1 Software maintenance includes checking, re-configuring or upgrading the software of the computer based system in order to prevent or correct faults, maintain regulatory compliance, and/or improve performance.

4.3.2.2 Software maintenance of category II and III computer based systems shall mandatorily include the following stages:

.1 organization of (local or remote) access for software maintenance in compliance with the equipment maintenance and repair procedures developed by the company;

.2 previous versions of software shall be stored for the system having the ability to revert simply to earlier revisions in the case of corruption;

.3 software maintenance;

.4 tests of the computer based system subject to maintenance;

.5 recording of maintenance information (updating the components' inventory of category II and III computer based systems and software inventory of category II and III computer based systems).

4.3.2.3 Software maintenance of category II and III computer based systems shall be performed by the RS-recognized company (code 22014002) being producer of the equipment, which software is subject to updating, or being authorized by the producer of this equipment.

4.3.2.4 Removable media intended to be used in software maintenance shall be subject to a malware check immediately prior to connection to the equipment.

4.3.2.5 Update of anti-virus software is not maintenance.

5 REQUIREMENTS TO SMS

5.1 CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS (SMS)

5.1.1 The provisions of this Section are recommendatory, nevertheless, they seek to support implementation of the IMO instruments in the context of maritime cyber security, which require cyber risks to be addressed after 1 January, 2021 in safety management system (SMS) that shall be developed, implemented and maintained by every company in compliance with the requirements of the International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code).

5.1.2 Despite the fact that the ISM Code does not directly regulate cyber risk management, cyber security may apply to the ISM Code requirements, since they fully comply with the ISM Code objectives, namely provision of safety at sea, prevention of accidents or loss of life and damage to environment, in particular, to marine environment, and property. Therefore, the International Maritime Organization (IMO) by resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems" encourages Maritime Administrations to ensure that cyber risks are appropriately addressed in SMS and that during the SMS audit of the companies and ships after 1 January, 2021, together with assessment of efficiency of the ISM Code elements' compliance, measures on cyber risk assessment and management, as well as efficiency of measures on prevention of detected cyber incidents are properly assessed.

5.1.3 It shall be noted that no two organizations in the shipping industry are the same, and approaches to cyber risk management will always be individual for each particular company and its ships. These approaches may depend on many factors, but herewith they shall be based on the appropriate international regulations, Flag State requirements, and take into account the applicable codes, guidelines and standards recommended by IMO, Maritime Administrations, classification societies, as stated in para 1.2.3.2 of the ISM Code.

5.1.4 This Section does not contain direct instructions for the companies on cyber security management and the way of their integration to SMS. This shall be done by the company. Such integration shall comply with IMO resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems", IMO circular MSC-FAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management" and will allow the companies to avoid additional administrative and financial loads. Each company may introduce specific requirements for cyber risk management to the existing SMS.

5.1.5 In this context the following may be considered an evidence of the fact that cyber safety management issues are referred to in SMS and are in the controlled conditions:

.1 risks related to cyber attacks or cyber incidents have been assessed by the company to provide continuous operation of its shore-based divisions in compliance with risk assessment procedures established in SMS;

.2 cyber risk management starts at the top management level. A culture of cyber risk awareness has been embedded into all levels of an organization to ensure flexible cyber attack

and cyber incident resilience regime. Top management understands the importance of cyber risk assessment and management;

.3 company has developed approach to prevent cyber attacks and cyber incidents, such as shutdown, breach, introduction of malware, lockout of computer systems, etc. based on risk assessment. These principles may be submitted in the form of functional components that shall apply in practice, permanently and simultaneously within the introduced management system, namely:

personnel solutions on cyber safety management have been defined. Functions and responsibilities of the personnel related to use and maintenance have been assigned, the access system and regulations for use have been established;

data and resources, which operational fault leads to risks related to shipboard operations have been identified;

protection measures have been developed, including emergency response to a failure of the computer based systems to provide continuous maritime operations;

measures have been developed and implemented on timely detection of the computer based systems failures;

measures have been developed and implemented on recovery of the shipboard operations by alternative methods in case of the computer based system failures;

measures have been defined on backup and recovery of the computer based systems in case of their malfunction.

5.1.6 Integration of cyber safety management in the company's SMS may be realized via the following SMS components:

.1 objectives:

company shall establish that the objectives of integration of the cyber safety management system comply with the ISM Code objectives, namely, provision of safety at sea, prevention of accidents or loss of life and damage to environment, in particular, to marine environment, and property;

.2 policy:

top management of the company shall assess and, in case of relevancy of the cyber attack and cyber incident matters within the ship operation, recognize the need for changing the company's SMS to implement cyber safety processes. Safety management policy may be revised with regard to the cyber attack and cyber incident matters and the necessity of response. Cyber safety, together with other matters of safety management, shall be regulated by the top management and mandatory for the shipboard and shore-based personnel;

.3 company's responsibility:

top management is ultimately responsible for cyber safety. Assignment of a person responsible for cyber safety management, cyber attack and cyber incident protection in the company, as well as for support to the Master when executing the IT and OT-related tasks and responsibilities;

.4 compliance with the requirements:

as regards cyber safety, the company shall meet the mandatory international and national requirements, assess and consider the applicable codes, recommendations and guidelines of IMO, Maritime Administrations, classification societies and organizations of maritime

industry. In its turn, this shall assist in forming the basis for risk assessment and changing of the company's SMS;

.5 risk assessment:

based on the risk assessment procedures specified in SMS, the main risks related to cyber attacks and cyber incidents, as well the methods of protection against adverse effects shall be determined. Where no equivalent system is available, for systematic evaluation the approach specified in Section 3 may be applied.

The results of risk assessment and protection measures against cyber attacks and cyber incidents shall be considered in the company's SMS. They may include the procedures, instructions, guidelines, etc. All accepted changes to SMS shall be harmonized with the company's procedures and brought to notice of the appropriate shore-based and shipboard personnel.

.6 Master:

SMS shall establish the requirements to the Master's qualification in IT and OT matters enabling the Master to discharge the duties associated with the position;

.7 support by the company's shore-based division:

a shore-based division shall be specified to support the Master and the ship, where necessary to provide:

response to cyber attack;

response to the cyber incident consequences;

recovery of the computer based systems' operability;

.8 resources and personnel; qualification; access to the computer based systems;

when employed, new shipboard personnel and the employees of the shore-based divisions shall get acquainted with the company's regulations related to cyber safety. The responsibilities shall be allocated and the instructions shall be developed for all persons responsible for cyber safety, as well as for the personnel using the shipboard computer based systems in any manner.

The company shall develop and implement measures restricting both physical and logical access to information resources and computer based systems, and measures on use of removable media and connection of other computer based systems.

Where necessary, measures shall be provided for familiarization, training and improvement of skills of the shipboard and shore-based personnel on a regular basis. SMS may contain training and advanced training program, as well as qualification requirements for a certain position;

.9 emergency preparedness:

for ships and shore-based divisions of the company, the contingency plans shall be provided in SMS for response to cyber attacks and cyber incidents. Also, drills and training shall be provided for emergency response to cyber attacks and cyber incidents;

.10 maintenance and repair:

safety measures shall be added to the maintenance and repair system of ship machinery, which shall be taken during maintenance and repair of the computer based systems. These measures shall be specified based on risk assessment.

SMS shall contain the criteria on selection of service providers;

.11 reports:

for improving the system, information on cyber attacks and cyber incidents shall be sent to the responsible divisions of the company for assessment, review and development of corrective actions in compliance with the procedures established by SMS;

.12 check, analysis and assessment performed by the company; documentation:

generally, SMS establishes the applicable requirements to maintenance and availability of documentation. When preparing documentation on cyber security, it may be required to provide restrictions of public access to the information available only for the limited group of persons onboard the ship and/or ashore, e.g. granting administrator privileges, password control, backup and recovery, etc.

5.1.7 The cyber safety management system integrated in the company's SMS, its functioning and efficiency shall be periodically verified and assessed by the company in compliance with the requirements established by the ISM Code.

5.1.8 Cyber safety management is a continually changing process that may undergo changes depending on external situation, thus, single establishment of cyber safety procedures and implementation of protection means cannot be considered sufficient. The company shall consider the permanent changes and deficiencies detected in its own system and provide update of the risk assessment and SMS, initiating therefore continuous improvement.

6 TESTS AND CHECKS

Checks and tests shall be carried out during review of technical documentation, manufacture of equipment and ship construction.

During the ship construction, on board tests shall be carried out on completion of installation and connection of all cables and equipment of the computer based systems.

The scope of tests and checks of the computer based systems shall include at least the following:

review of technical documentation for the computer based systems;

survey of cables and equipment used in the computer based systems;

tests of the computer based systems on board;

tests after software maintenance;

check of remote access;

check of manual control.

6.1 REVIEW OF TECHNICAL DOCUMENTATION

6.1.1 Review of technical documentation shall be carried out in compliance with Part II "Technical Documentation" of the RS Rules/TS.

6.1.2 The following documentation specified in Table 2.1.1 shall be submitted to the Register for review.

6.1.3 Based on the review of technical documentation, the final letter of conclusion shall be prepared, indicating all reviewed documents and remarks, if any.

6.2 SURVEY OF CABLES AND EQUIPMENT

6.2.1 The cables used in the computer based systems shall be tested in compliance with Section 10, Part IV "Technical Supervision during Manufacture of Products" of the RS Rules/TS.

6.2.2 Check of compliance of the network communication equipment used in the shipboard computer based monitoring, control, logging and alarm systems with the industry standards (e.g., IEC 62443 or equivalent) shall be confirmed by the certificate of compliance issued by a competent body.

6.2.3 In addition to specified in 6.2.2, the network equipment shall be tested in compliance with Section 12, Part IV "Technical Supervision during Manufacture of Products" of the RS Rules/TS, and also tested for compliance with the requirements of the Guidelines according to the test program and procedure developed by the producer.

6.2.4 Test program and procedure for the electronic devices used for data storage of category II and III computer based systems shall be developed by the producer, taking into consideration the type of data storage devices and submitted to the Register for agreement.

6.2.5 The network communication equipment used in the shipboard navigational systems and radio communication systems shall be tested in compliance with IEC 61162-460.

6.2.6 Based on satisfactory test results, the appropriate form of certificate shall be issued in compliance with Part I "General Regulations for Technical Supervision" of the RS Rules/TS.

6.3 TESTS OF COMPUTER BASED SYSTEMS ON BOARD THE SHIP

6.3.1 General requirements.

6.3.1.1 General requirements for survey of equipment and systems on board the ship are specified in Part I "General Regulations for Technical Supervision" of the RS Rules/TS and Section 1 of the Guidelines on Technical Supervision of Ships under Construction.

6.3.1.2 Preliminary list of the items of technical supervision shall be developed by the system integrator.

6.3.1.3 List of items of technical supervision containing detailed scope and procedure of the technical supervision, types of checks, tests and control shall be developed by the shipyard in compliance with 13.3, Part I "General Regulations for Technical Supervision" of the RS Rules/TS based on the preliminary list specified in 6.3.1.2, reviewed and agreed upon with the RS Branch Office for technical supervision under construction.

6.3.1.4 Programs of mooring and sea trials shall be reviewed by the Register in compliance with Part II "Technical Documentation" of the RS Rules/TS and Section 18 of the Guidelines on Technical Supervision of Ships under Construction.

6.3.1.5 On completion of mooring and sea trials the test reports of the computer based systems shall be prepared and submitted to the Register.

6.3.1.6 Software (e.g., WireShark, TCPdump, NMAP, XSpider, RedCheck, Efros Config Inspector, etc.) and hardware for testing of safeguards, means for detection of cyber incidents and cyber attacks, monitoring, alarm and logging systems shall be provided.

6.3.2 Tests of data communication network.

6.3.2.1 Tests of the data communication network shall be carried out during mooring trials in compliance with the procedure and program developed by the system integrator. The following tests to verify the network functionality and performance, at least:

.1 network maximum loading;

.2 network storm test;

.3 redundancy tests where systems are designed with redundant network and network devices.

6.3.2.2 Compliance of actual location of the network devices and those specified in the description of data communication networks shall be verified.

6.3.3 Tests of monitoring, alarm and logging systems.

6.3.3.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator. Test program and procedure shall contain the list of items to be tested, list of software and hardware required for tests, description of test procedures or substantiation of the relevant tests' necessity.

6.3.3.2 The objective of the tests is to ensure reliability and quality of the data transfer networks, and the provision of suitable alarm, monitoring and logging of cyber incident detection. During the tests, control, alarm and logging of events, cyber incidents and failure indication specified in 4.1.3.2, 4.2.4 and 4.2.5 shall be verified.

6.3.3.3 For wireless data communication equipment, test during mooring and sea trials shall be conducted to demonstrate that radio-frequency transmission does not cause failure of any shipboard equipment and does not its self-fail as a result of electromagnetic interference during operating conditions.

6.3.4 Tests of network protection safeguards.

6.3.4.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator. Test program and procedure shall contain the list of items to be tested, list of software and hardware required for tests, description of test procedures or substantiation of the relevant tests' necessity.

6.3.4.2 The objective of the tests is to ensure efficiency of network protection safeguards used in the computer based systems. Tests of the network protection safeguards specified in 4.1.2 shall be carried out.

6.3.5 Tests of cyber attack and cyber incident detection safeguards.

6.3.5.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator. Test program and procedure shall contain the list of items to be tested, list of software and hardware required for tests, description of test procedures or substantiation of the relevant tests' necessity.

6.3.5.2 The objective of the tests is to ensure efficiency of cyber attack and cyber incident detection safeguards used in the computer based systems. Tests of the detection safeguards specified in 4.1.3.1 shall be carried out.

6.3.6 Tests of recovery measures to restore computer based systems.

6.3.6.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator. Test program and procedure shall contain the list of items to be tested, list of software and hardware required for tests, description of test procedures or substantiation of the relevant tests' necessity.

6.3.6.2 The objective of the tests is to ensure efficiency of recovery measures to restore the computer based systems. Tests of recovery measures specified in 4.1.4.1 shall be carried out.

6.3.7 Tests of access control to computer based systems.

6.3.7.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator.

6.3.7.2 The objective of the tests is to ensure the security perimeter availability by access control to the computer based systems specified in 4.1.6.3 and 4.1.6.4.

6.4 TESTS AFTER SOFTWARE MAINTENANCE

6.4.1.1 Subsequent to execution of software maintenance, the following tests shall be carried out:

.1 regression tests;

.2 new functionalities and/or improvements tests;

.3 load tests.

6.4.1.2 Reports on the test results shall be submitted to the Register.

6.4.1.3 The objective of software tests after maintenance is to verify that the equipment subject to software maintenance, integrated in the relevant system or sub-system, behaves according to the specification and the applicable requirements.

6.4.1.4 During the software maintenance planning, the producer or service provider shall issue a test plan specifying the tests to be executed. Test cases covering both normal operation and failure conditions shall be specified in the test plan.

6.4.1.5 Regression tests are aimed at verifying that no functionality which is expected to be still present after the maintenance has been impaired.

6.4.1.6 The purpose of testing new functionalities and/or improvements is to verify that the software maintenance had the intended effect.

6.4.1.7 The load test shall be conducted to verify the compliance of software and hardware performance with the specification requirements.

6.4.1.8 The tests shall cover each equipment subject to maintenance and shall be subdivided into the following activities:

.1 development of the test plan determining the scope and risks related to software maintenance, as well as identifying the objectives and procedures of testing, expected time and resources required for the testing process. It shall provide clear information on how the tests are carried out and how to verify the success or failure of each test;

.2 selection of test cases based on requirements, specifications, risk analysis and interfaces of the equipment subject to software maintenance;

.3 documenting of the results of the executed tests, including the versions of software to be maintained;

.4 test of procedures that can roll back to the previous software version and configuration after a software update has been attempted to the shipboard equipment without success;

.5 review of the executed tests in order to confirm that software updates may be installed and that no failure has been detected during the test activities. In case of failure, corrective actions shall be planned, and an updated test plan shall be issued;

.6 process shall consider the implications and any risks related to that could result from the rollback and identify appropriate testing performed post roll back in order to provide satisfactory working condition of the system in compliance with the applicable requirements.

6.4.1.9 Rollback procedures shall be submitted upon the Register request.

6.4.1.10 Documents (e.g., service provider report) verifying the performance and containing the test results shall be submitted upon the Register request.

6.5 TEST OF REMOTE ACCESS

6.5.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator.

6.5.2 The objective of the tests is to verify compliance with the requirements in 4.1.7.

6.6 TEST OF MANUAL OPERATION

6.6.1 Tests shall be carried out in compliance with the procedure and program developed by the system integrator.

6.6.2 The objective of the tests is to verify compliance with the requirements in 4.1.8.

APPENDIX

DATA QUALITY

1 Data security.

1.1 The general objective of data security is to ensure confidentiality, integrity and accessibility of data. Depending upon the intended use of the data, these may take a different order of priority. For example, OT systems transmitting safety critical data will prioritize availability and then integrity.

1.2 The scope of application of data assurance covers data which life cycle is entirely within the shipboard computer based system, as well as data exchanged with shore systems connected to the ship networks. While the consequences of unauthorized modification, data corruption or data loss may differ between IT systems data (typically, operational data with a business impact) and OT systems data (may include set points for control and safety with a safety of environmental impact), where data transfers and updates are implemented using a network, these data security objectives share common features and shall be considered for the system as a whole.

2 Data categorization.

2.1 Data categorization document identifying the risks for various categories of data shall be developed by the system integrator. Data shall be categorized according to the possible consequences of a breach of data assurance affecting confidentiality, integrity and availability.

2.2 The potential impact of loss of data assurance shall be categorized as follows:

.1 LOW: the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on safety of the ship, human safety and/or threat to the environment;

.2 MODERATE: the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on safety of the ship, human safety and/or threat to the environment;

.3 HIGH: the loss of confidentiality, integrity, or availability could be expected to have severe or catastrophic adverse effect on safety of the ship, human safety and/or threat to the environment.

2.3 Table 2.3 shows how to assign systems with categories based on their effects on data confidentiality, integrity and availability.

Table 2.3

Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems which failure will not lead to dangerous situations for safety of the ship, human safety and/or threat to the environment	Monitoring functions for informational/ administrative tasks	Low	Moderate	Low
II	Those systems which failure could eventually lead to dangerous situations for safety of the ship, human safety and/or threat to the environment	Alarm, monitoring and control functions which are necessary to maintain the ship in its normal operational and habitable conditions	Moderate	High	Moderate
III	Those systems which failure could immediately lead to dangerous situations for safety of the ship, human safety and/or threat to the environment	Control functions for maintaining the ships propulsion and steering safety functions	Moderate	High	High

2.4 The categorization given in Table 2.3 shall be used as a guidance on a case by case basis.

Notes: 1. Escalation: systems involving essential services sharing data necessary for their functions might need to have the potential impact escalated to a higher level.

2. Confidentiality level: it is understood the confidentiality level of information might have an immediate business risk.

2.5 Data properties shall establish what aspects of the data (e.g., timeliness, accuracy) need to be guaranteed in order that the system operates in a safe manner.

3 Secured and encrypted data.

3.1 An analysis shall be carried by the system integrator to assess the value of data security and its potential impact on system performance.

3.2 The system shall be provided with suitable access control measures and other technological and/or procedural measures over the computer based systems or means of communication directly interacting with the system.

3.3 Networks protocols shall ensure the integrity of control, alarm and monitoring, communication and safety related data, and provide timely recovery of corrupted or invalid data.

4 Data storage.

4.1 Document specifying the critical data which is required to be stored towards operation of systems identified through risk analysis shall be developed.

4.2 Devices used to store data for category II or III systems shall be appropriate for intended use and suitable for the marine environment. Data stored on such devices shall be appropriately replicated to minimize data loss in case of device single failure.

Russian Maritime Register of Shipping

Guidelines on Cyber Safety

FAI "Russian Maritime Register of Shipping"
8, Dvortsovaya Naberezhnaya,191186, St. Petersburg
https://rs-class.org/en/