No. 166 Recommendation on Cyber Resilience

(Apr 2020)
(Corr.1 July 2020)
(Corr.2 Apr 2022)

Contents

No. 166 (cont)

1. Introduction

1.1 Purpose of the recommendation

1.1.1 The purpose of this recommendation is to provide technical information to stakeholders which would lead to delivery of cyber resilient ships, whose resilience can be maintained throughout their service life.

1.1.2 Resilience, in this context, is meant as a characteristic that provides crew and ships the capabilities to effectively cope with cyber incidents occurring on computer-based systems onboard which contribute to operate and maintain the ship in a safe condition. The most effective method of dealing with an incident is to prevent it ever happening, so in this context "prevention" is even more important than "cure".

1.1.3 It is intended that recommendations herein provide guidance for mitigating the risk related to events affecting onboard computer-based systems, recognizing that, if no measures are implemented, such events could potentially affect the human safety, safety of vessel and/ or the threat to the marine environment.

1.1.4 The recommendation intends to ensure that design, integration and/or maintenance of computer-based systems support secure operation and provide means to protect against unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based systems or transported in the networks connecting such systems.

1.1.5 This recommendation seeks to support IMO Resolution MSC.428(98) (June 2017): 'Maritime Cyber Risk Management in Safety Management Systems', which requires cyber risks to be addressed in safety management systems by 1 January 2021, based on MSC-FAL.1/Circ.3 (June 2017): 'Guidelines on Maritime Cyber Risk Management[1]'.

1.1.6 This recommendation seeks to support IACS UR E26: "Cyber resilience of ships". Should any difference be found between this document and UR E26 when addressing the same topic, for ships in which the UR is applied the requirements in IACS UR E26 shall prevail.

1.2 Overview of the Recommendation structure

1.2.1 This Recommendation is organized in eight Sections, three Appendices and one Annex:

Section 1, Introduction, contains the introductory part and an explanation on how to use this Recommendation.

Section 2, Scope, defines the applicability of this Recommendation.

Section 3, Reference Standards, provides a list of existing international standards and guidance, which are referenced in this recommendation.

Section 4, Terms and definitions, contains definition of terms for the purpose of this recommendation.

Sections 5 and 6 respectively set out Goals and functional requirements. Goals are high-level objectives to be met; the criteria to be satisfied in order to conform to the Goals are provided by functional requirements.

Section 7, Technical Considerations, describes detailed technical topics and processes that

No. 166 (cont)

should be considered.

Section 8, Verification & testing, describes verification and testing methods to demonstrate the conformance with the technical criteria in Section 7.

Appendix A contains a detailed list of standards which this Recommendation makes reference to.

Appendix B contains a list of documents referred in Recommendation, describing for each document who is expected to develop the document and how it will be reviewed.

Appendix C contains a mapping of sub goals described in Section 5 to Technical & Verification items described in sections 7 and 8.

Annex A contains a guidance on operational aspects to be taken into account for the application of this Recommendation.

1.2.2 While a goal-based approach was used during the development of the Recommendation, it is also drafted to give recognition of the 5 elements of effective cyber risk management contained in MSC-FAL.1/Circ.3 “Guidelines for Maritime Cyber Risk Management:

- Identify
- Protect
- Detect
- Respond
- Recover

These elements are also common to and intended to be consistent with NIST “Framework for Improving Critical Infrastructure Cyber security[2]” and “Guidelines on cyber security onboard ship[3]”. Depending upon preferences for implementation, these can themselves be regarded as goals, or as objectives, for the cyber resilience program on a ship.

1.3 How to use this Recommendation

1.3.1 The recommendation can be regarded as a roadmap for developing a program for cyber resilient computer-based systems on board and then as a framework for that program. As the recommendation is goal based, any of the 5 elements identified should be able to be traced backwards and associated with one or more identifiable goals.

1.3.2 It must be recognized that many other activities and procedures beyond those in the scope of this recommendation should be put in place to the purpose of enhancing cyber resilience according to a desired level for the vessel, if necessary.

1.3.3 The most pertinent amongst these other activities and procedures are the ships safety management system, the associated shore based company procedures and a comprehensive appreciation of the risks associated with the deployment of computer-based systems. Unless all parties from the crew to the management are aware of, and remain vigilant to, the risks then weaknesses and vulnerabilities accumulate until the original program becomes inadequate.

1.3.4 Section 7 provides technical provisions for the implementation of the functional requirements as set out in Section 6, in order to ultimately meet the design and construction

No. 166 (cont)

goals as envisaged in Section 5.

1.3.5 Section 8 identifies the elements to be reviewed, witnessed and confirmed at the time of survey.

1.3.6 Annex A lists assumptions and expectations of procedures and operational aspects. Operational aspects are the responsibility of owners/operators, and are not within the scope of this Recommendation. The list is included solely to raise awareness of the elements that need to be maintained in place for designs which are in line with this Recommendation to be satisfactory.

2. Scope

2.1. The Recommendation is based on the application of IACS UR E22 "On Board Use and Application of Computer based systems[4]" and covers the use of computer-based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to requirements of Classification society.

2.2 The recommendation covers onboard OT systems and other systems which are connected to onboard OT systems in a way that may affect their operation (as identified by risk assessment). The recommendation also covers equipment that may have an impact on human safety, the safety of the vessel or the marine environment, as identified by the requirements of the International Convention for the Safety of Life at Sea (SOLAS) and the International Convention for the Prevention of Pollution from Ships (MARPOL). The risk assessment should consider requirements of the Classification Society and National Authority.

2.3 The recommendation is intended for vessels contracted for construction after publication. The recommendation may be used as a reference for ships in service prior to publication.

2.4 The recommendation addresses technical design, construction and testing aspects.

2.5 The operational aspects and management items set out in Annex A are intended as assumptions or expectations to support the technical and testing items identified in this recommendation and are indicated as guidance. The Operational aspects and management items will be under the responsibility of owners and operators.

3. Reference Guidelines and Standards

3.1 The following list provides references to international or industrial standards that may be considered as a primary technical background for this recommendation.

[1] IMO MSC-FAL.1/Circ.3, *"Guidelines on Maritime Cyber Risk Management"*, July 2017

[2] NIST *"Framework for Improving Critical Infrastructure Cyber security"*, version 1.1 2018

[3] *"The Guidelines on Cyber Security Onboard Ships"*, version 3.0, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, WSC and IUMI, 2018

[4] IACS UR E22 *"On Board Use and Application of Computer Based Systems"*, June 2016

A detailed list of standards which this Recommendation makes reference to, is indicated in Appendix A of this document.

No. 166 (cont)

4. Terms and Definitions

4.1 For the purposes of this document, the following terms and definitions apply.

4.1.1 **Access control:** 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.

4.1.2 **Attack surface:** The computer based systems which can be accessed externally either through network or locally.

4.1.3 **Bug:** Unintended functionality in software.

4.1.4 **Category of maintenance:** A category assigned to a software maintenance activity based upon the reason for undertaking the maintenance, which may be:

- Bug Fix (resolving software bugs);
- Feature Release (adding additional functionality);
- Compliance Update (maintaining conformity with regulations);
- Security Update (protecting against cyber threats);
- Obsolescence Update (addressing software and/or hardware that is no longer supported);
- Or some combination of the above.

4.1.5 **Computer based system:** Combination of interacting programmable devices and/or cyber systems organized to achieve one or more specified purposes. Computer based System may be a combination of subsystems connected via network. Onboard computer based System may be connected directly or via public means of communications (e.g. Internet) to ashore based computer based Systems, other vessels' computer based System and/or other facilities.

4.1.6 **Contingency Plan:** The plan which provides essential information and established procedures to ensure effective response and recovery in case of a cyber incident affecting computer-based system providing essential contribution.

4.1.7 **Critical System:** The technical systems that the sudden operational failure of may result in hazardous situation.

4.1.8 **Cyber attack:** 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 ship systems and data.

4.1.9 **Cyber incident:** An occurrence, which actually or potentially results in adverse consequences to an on-board system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

4.1.10 **Cyber resilience:** Cyber resilience means capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational

No. 166 (cont)

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.

4.1.11 **Cyber risk management:** 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 by stakeholders.

4.1.12 **Cyber safety:** The condition of being protected against vulnerabilities resulting from inadequate operation, integration, maintenance and design of cyber related systems, and from intentional and unintentional cyber threats.

4.1.13 **Data Quality:** Data Quality is intended as the activity, or set of activities, aimed at enforcing the security of data generated, processed, transferred and stored in the operation of computer based systems on board. The three terms below can be broadly defined as following:

1) CONFIDENTIALITY – a loss of confidentiality because of an unexpected or unauthorized disclosure of information.

2) INTEGRITY – a loss of integrity because of an unexpected or unauthorized modification of information.

3) AVAILABILITY – a loss of availability because of an unexpected or unauthorized destruction of the information or disruption of access to, or use of an information system.

4.1.14 **Data Provider**: The stakeholder that supplies data necessary for the functioning of the computer based system on board.

4.1.15 **Defense in breadth:** 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.

4.1.16 **Defense in depth:** An approach which uses layers of independent technical and procedural measures to protect IT and OT on board.

4.1.17 **Demilitarized zone (DMZ):** A physical or logical sub network that contains and exposes an organization's external-facing services to an untrusted network.

4.1.18 **DLP:** Data Loss prevention.

4.1.19 **Essential Systems:** Systems contributing to the provision of essential services for the safe operation of the ship.

4.1.20 **Failure Mode and Effects Analysis (FMEA):** 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.

4.1.21 **Firewall**: A logical or physical break to establish a barrier between a trusted and untrusted networks and which is designed to prevent unauthorized access.

No. 166 (cont)

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

4.1.23 **HMI:** Human Machine Interface.

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

4.1.25 **Integrated system**: Interconnected system combining a number of interacting shipboard equipment organized to achieve one or more specified purposes.

4.1.26 **Intrusion Detection System (IDS):** 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.

4.1.27 **Intrusion Prevention System (IPS)**: A device or software application that monitors network or system activities to prevent malicious activities or policy violations.

4.1.28 **Local Area Network (LAN):** A computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.

4.1.29 **Local control:** Control from a location in the immediate vicinity of the concerned machinery.

4.1.30 **Malware:** Generic term for a variety of malicious software, which may adversely impact the performance of computer systems.

4.1.31 **Managed Network:** 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.

4.1.32 **Media Access control (MAC):** A hardware address that differentiates one device on a network from another.

4.1.33 **M2M:** Machine to machine interface.

4.1.34 **Network:** A group of two or more computer systems linked together.

4.1.35 **Network Hub:** Network hub, is a common connection point for devices in a network.

4.1.36 **Network Router:** A network device which is responsible for routing traffic from one network to another network.

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

4.1.38 **Operational technology (OT):** Devices, sensors, software and associated networking that monitor and control onboard systems.

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

No. 166 (cont)

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

4.1.41 **Programmable device:** Physical component where software is installed.

4.1.42 **Producer:** The entity that manufactures the shipboard equipment and associated software.

4.1.43 **Protocols**: A common set of rules and signals that computers on the network use to communicate.

4.1.44 **Quality of Service (QoS):** The measurable end-to-end performance properties of a network service.

4.1.45 **RAID:** Redundant Array of Independent Disks.

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

4.1.47 **Removable media**: A collective term for different methods of storing and transferring data between computers without the aid of a network. This includes but not limited to laptops, USB memory sticks, CDs, DVDs and diskettes.

4.1.48 **Risk assessment:** 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.

4.1.49 **Risk management:** The process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

4.1.50 **Security Information Event Monitoring (SIEM):** 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.

4.1.51 **Service provider:** A company or person, who provides and performs software maintenance.

4.1.52 **Simulation test:** 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.

4.1.53 **System Categories (I, II, III):** System categories based on their effects on system functionality, which are defined in IACS UR E22.

I. Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

II. Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

III. Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

No. 166 (cont)

4.1.54 **System Integrator:** The stakeholder that combines shipboard equipment into an integrated system.

4.1.55 **Test Case**: 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.

4.1.56 **Unmanaged Network:** Network which uses unmanaged switches, that allows devices connected to a network to communicate with each other. It is a plug-and-play switch that does not require or allow any user intervention, setup, or configuration.

4.1.57 **Virtual Local Area Network (VLAN):** 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.

4.1.58 **Virtual Private Network (VPN):** 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.

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

4.1.60 **Wi-Fi:** All short-range communications that use some type of electromagnetic spectrum to send and/ or receive information without wires.

5. Goals for design and construction

5.1 The goal of this recommendation in terms of design and construction is to enable the delivery of cyber resilient ships whose resilience can be maintained throughout their life-cycles.

5.2 The sub goals (SG) of this recommendation in terms of design and construction are to:

5.2.1 Identify

SG1) Have a complete understanding of all the devices, systems, networks and data flows on board, in order to understand how to protect, detect, respond and recover.

5.2.2 Protect

SG2) Harden systems and devices, to support in as many ways as possible for protection of OT systems and relevant information.

5.2.3 Detect

SG3) Detect cyber incidents in a timely and effective way.

5.2.4 Respond

SG4) Limit the extension and duration of effects of possible damage to OT systems and relevant information

No. 166 (cont)

5.2.5 Recover

SG5) Restore the functionality of OT systems in a timely manner to maintain the ship in a safe condition.

6. Functional Requirements

6.1 This section sets out general functional requirements. The functional requirements are categorized according to the five sub goals of the recommendation (Identify, Protect, Detect, Respond and Recover) and assumptions on operational aspects and management are indicated at annex A.

6.2 Identify (I):

Functional requirements

I1) Information that flows among the operation technology (OT) systems installed on board and between OT systems and other systems, should be identified.

I2) Interdependencies across critical systems and risks that can affect safety of vessel, human safety and environment when such systems are compromised should be identified.

6.3 Protect (P):

Functional requirements

P1) IT and OT systems should be designed to support secure configuration, secure integration and secure software maintenance.

P2) Interoperability of OT systems should be limited to identified critical functions.

P3) OT and IT network infrastructure should be segmented by division into network zones.

P4) Both physical and Logical access to OT systems should be restricted.

P5) The possibility of disruption to OT system which affect the availability of safety critical functions should be minimized.

6.4 Detect (D):

Functional requirements

D1) Means for the monitoring of normal operations of OT systems should be provided, based on continuous and/or on-demand self-diagnostics and connection quality and/or network performance monitoring tools should be available at least on networks connecting OT systems of Category II and III and on networks connecting IT systems to OT systems of Category II and III.

6.5 Respond (R):

Functional requirements

No. 166 (cont)

R1) Impact of cyber incidents should be contained to the network zone of origin.

R2) Minimize by isolating the extension of possible disruption to OT system which affects the availability of safety critical functions.

6.6 Recover (RC):

Functional requirements

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

7. Technical Considerations

This section identifies topics and processes that system designers or integrators may consider when developing computer-based systems in order to enhance the cyber resiliency of ships.

7.1 Asset identification

7.1.1 Inventory of Computer based systems

Computer based systems of category I, II and III on board are based on devices that are directly used to control, alarm and monitor ship systems and may include one or more, but not limited to, the following components:

1) Distributed control systems (DCSs) and associated devices;

2) Supervisory Control And Data Acquisition (SCADA) systems and associated devices;

3) Programmable logic controllers (PLCs) and associated devices;

4) Routers, switches;

5) Human Machine Interface (HMI) stations;

6) Networks on board

The actual components of systems may vary with each installation according to the systems being controlled, alarmed and /or monitored.

7.1.1.1 Towards an effective assessment and control, an inventory of computer based systems onboard of Category II and III should be created before vessel’s delivery.

7.1.1.2 The Inventory should be updated during the life of the ship. Software and hardware modifications should be tracked to check that new vulnerabilities and dependencies have not occurred or have been treated appropriately to mitigate the risk related to their possible exploitation.

7.1.2 System Documentation

7.1.2.1 Following documents should be developed during design /project concept phase for category I, II & III systems and other computer based systems interfaced with above.

No. 166 (cont)

1) Design philosophy document

A design philosophy document should be developed consisting of following information:

a. Purpose of the computer based system with brief functional description

b. A system block diagram or plan clearly identifying various systems which can be controlled should be developed showing following information;

i. Type of communication with external network for control, monitoring and administrative functions

ii. Dependent systems

2) Network Communication Document

Network communication document should be developed specifying means of communication between systems, sub systems and various components of sub system. Network Communication document should consist of following information.

a) Physical location of the system located (e.g. Marked on drawings or frame number and level)

b) Category I systems integrated with Category II and III of computer based systems

c) VLAN and IP scope (IP address range)

d) Type of communication network topology (e.g Series, Series star, Mesh etc)

e) Network technologies (e.g Ethernet, Fast Ethernet)

f) Network cables– twisted pair, coaxial, fibre optic etc

g) Details of Communication from field controllers to field devices MODBUS, Fieldbus etc.

h) Simple network diagrams showing the devices, nodes, network cable details and general locations of the equipment.

i) Networked IT and OT systems and their category according to UR E22

j) Data flows and network devices or resources potentially limiting them

k) Details of external connections for remote access

l) Access points and interfaces, including machine-to-machine (M2M) interfaces

m) Services (e.g. name, IP address, port number) establishing connections

n) Services (e.g. name, IP address, port number) listening to connections

o) Table showing connection relationships of all the network devices such as routers, firewalls and so on(e.g. device name, connection, access relation of devices, security measure)

No. 166 (cont)

p) network devices settings and access settings (such as router)

7.1.2.2 Inventories

Following inventories should be developed for various computer based system, before vessel's delivery and subsequently the document should be maintained on board.

1) For Communicating devices (e.g PLCs, remote I/O, sensors, operating systems, actuators, variable speed drives, meters, circuit breakers, switches, physical servers, desktops and storage units etc.) and Network communication devices (e.g switches, routers and protocol gateways) following should be specified for each:

a) Name

b) Brand/Manufacturer(supplier)

c) Model or reference, some devices contain several references

d) Version of the operating system and embedded firmware (software version)

e) Physical characteristics, if appropriate

f) Physical location (e.g Accommodation space/Engine room, cabinet)

g) List of switches connected

2) Logical inventories

a) IP address ranges with, for each one:

i. The list of switches concerned

ii. The functional description of the IP range

iii. Interconnections with other ranges.

b) Non IP addresses

i. the list of MAC addresses or addresses specific to the industrial protocols on the Network

ii. the list of switches concerned;

iii. Functional description of the network

iv. Devices connected to other networks (connectors).

c) Non-Ethernet access points with, for each one:

i. The list of access ports

ii. Addressing, if there is a special protocol

iii. The list of connected devices.

No. 166 (cont)

d) Logical servers and desktops with, for each one, if applicable:

i. IP addressing (network, mask, gateway)

ii. operating system version

iii. underlying physical server

iv. applications and their versions

v. Services and versions.

e) Connectors and communicating field devices (remote I/O, smart sensors, smart actuators, etc.)

i. IP address (network, mask, gateway), the associated MAC address and network or the specific address, if appropriate

ii. Applications.

3) Software Inventory

Inventory of software used for computer based systems should be developed before vessel's delivery and subsequently should be maintained onboard. Following information is recommended to be recorded:

a) software name and publisher

b) installation date, version number and functions

c) Maintenance type (Local/remote)

d) Accounts type (generic / dedicated)

e) Access control list with read, write and execution rights

f) IP/Ports destination. If unknown, information should be identified as "missing"

g) License number.

4) Network services structured for each equipment:

Following information should be developed

a) For IP based Services:

i. protocol name and version

ii. Listening ports and function

b) For non-IP based Services:

i. listening interface

No. 166 (cont)

7.1.3 Risk Assessment

7.1.3.1 A detailed risk assessment of onboard computer based systems should be carried out using standard risk assessment techniques. The risk assessment during new building phase should be carried out by the yard/system integrator and owners.

Risk analysis should identify immediate effect on the equipment and overall impact on ship operation which can affect human safety, safety of vessel and environment. The risk analysis should consider the effect on the systems integrated or interfaced to other systems.

7.1.3.2 The risk analysis could be qualitative or quantitative and the consequence should be graded in order of severity. (e.g. trouble to daily life, serious trouble to daily life, damage to life, impact on business activity, suspension of business activity). Risk acceptance criterion should be documented. Guidance can be taken from IACS UR E22 regarding severity categorisation of particular system.

7.1.3.3 The consequences should be analysed for availability, integrity and confidentiality of the data for the computer based system due to cyber threat, which could eventually affect human safety, safety of vessel and threat to environment.

7.1.3.4 Type of vessel, extent of connectivity between various systems and between ship and shore, should be considered in risk assessment. The assessment should include identification of each designed safe state.

7.1.3.5 The risk analysis should consider the effect on the systems integrated or interfaced to other systems, including the effects of systems not onboard, if remote access function from shore is provided.

7.1.3.6 Controls to mitigate the risk should be based on risk analysis document Clause 7.7 may be referred for Data specific risks.

7.1.3.7 A document containing a description of the safeguards (controls) and instructions on how to verify their effective implementation, or a rationale for those not implemented should be developed.

7.2 Communication and interfaces

7.2.1 The system should be designed to ensure authorized operation of the communication and interface functions.

7.2.2 The system design should include an assessment of the possibility and consequences of a fault in one system or equipment extending to another system and the identification of suitable technical safeguards. A defence in breadth approach, through implementation of additional controls, as identified in risk assessment should be considered.

7.2.3 Means to test technical safeguards for internal and external interfaces, and communication paths should be provided for use during equipment testing, ship commissioning, periodic testing and through the lifetime of the equipment.

7.2.4 System design should consider selection of equipment including sensors, communication hardware, data integrity and installation using risk assessment and operational requirements. Consideration on the location and proximity to areas detrimental to data (e.g. areas with high electromagnetic interference (EMI), exposed to weather vulnerable to accidental mechanical damage or human interference (or mischief), including supplier specific recommendations, if any, should be documented.

No. 166 (cont)

7.3 Network

7.3.1 Equipment standards

7.3.1.1 Network devices

Network devices and it's monitoring & alarm devices for Category II and III systems should be suitable for marine application and should be tested as specified in IACS UR E22 and E10 or relevant standards which are accepted by the Classification Society.

7.3.1.2 Networks cables

All network cables for categories I, II and III should be designed, manufactured and tested as per relevant National/International Standards acceptable to the Classification Society.

7.3.1.3 Wireless equipment

Wireless equipment should be designed and tested as per requirements specified in IACS UR E22.

7.3.1.4 To ensure desired performance and reliability of the network, suitable network monitoring and alarm systems should be deployed. The network monitoring systems should provide adequate information describing the cyber incident for the use of the intended user. When the ship has provision for remote connectivity it should be possible to identify a cyber incident originating external to ship.

7.3.2 Design

7.3.2.1 The network design should meet the intended data flow through the network. The data sizing calculations considering following should be carried out to identify:

1) Suitable network data throughput

2) Data Speed needs for particular application

3) Data format

7.3.2.2 Where required by classification societies or as concluded by risk assessment, redundant network should be provided.

7.3.2.3 The design should ensure that Networks for Category II and III (as defined by IACS UR E22) systems and integrated systems should be resilient. Fault in one part of ship network due to failure of network devices or cyber incident, should not affect the remaining systems connected to unaffected network.

7.3.2.4 The system should be adequately designed to allow the ship to continue its mission critical operations in a manner that preserves the confidentiality, integrity, and availability of the data necessary for safety of the vessel.

7.3.2.5 Basic design should address following criterion for OT and IT systems (when connected with OT systems):

1) Reliability

2) Maintainability

No. 166 (cont)

3) Extensibility

4) Interoperability

7.3.2.6 System design for Fault tolerances

1) For systems of Category II and III connections within the sub-systems and their networks should be resilient to faults with self-correcting properties that guarantee to provide data to be transmitted without failures.

2) Local controls and indicators should be part of the fault tolerance architecture. The design architecture should be based on risk assessment and requirements of Classification Society.

3) Equipment to be used in systems of Category II and III should be selected and configured to mitigate the risk related to cyber attacks, such as spread of exploits. Testing and certification should be according to requirements of the Classification Society.

4) The attack surface of Category II and III systems and data should be reduced by separating them from non-critical data and processes.

5) The aim should be to decouple capabilities in order to prevent ripple effects that can contaminate large portions of the systems as the result of a single cyber incident.

6) In the event of failure of any network equipment or impairment due to a cyber incident, the equipment should go to a defined safe state or maintain safe operation, as applicable.

7.3.2.7 Where required Failure mode effect analysis (FMEA) and vulnerability assessment of systems and networks, for essential services, should be carried out.

7.3.3 Installation

7.3.3.1 Equipment

The computer based systems should be installed in suitable enclosures unless the ingress protection of the device is according to the requirement of Classification Society. The enclosures should allow access for maintenance.

The devices should be located in well ventilated areas and should be installed at a sufficient distance from vibration sources so that they are not adversely impacted by external vibration exceeding values defined by IACS UR E10. Equipment should be installed at sufficient distance from electromagnetic interference (EMI) sources with level of interference exceeding value defined by IACS UR E10. Manufacture’s specific recommendations/requirements should be considered during installation design.

7.3.3.2 Cabling

The minimum bending radius specified for the cable should not be exceeded especially for optical fibre cables where it may lead to signal loss.

The network segregation from Electromagnetic Interference Sources (EMI) should meet Classification Society requirements and recommendation by the supplier and system integrator.

No. 166 (cont)

It is recommended to group and separate critical systems into network zones with common cyber security levels in order to manage appropriate risks and to achieve a desired target of cyber security level for each network zone**.**

7.3.4 Control, Monitoring and alarm

7.3.4.1 Control, monitoring and alarm systems implemented over networks are also subject to paragraph 7.3.1.4.

7.3.4.2 Network Access control system

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

7.3.4.3 Monitoring

The network devices for Category II and III systems should be able to detect 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 (only if the network device has a fan and a fan-stop detection function)

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

7.3.4.4 Alarm function

The network-monitoring device for Category II and III should provide functions to detect abnormal condition and notify the user:

1) When a link is disconnected or the power is turned off for a network device or network terminal

2) When a link not belonging to the network is connected or the power is turned on for a network device or network terminal

3) Loss of a network device.

7.3.4.5 Wireless Communication

1) The access control system should provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

2) The access control system should provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly acceptable industry best practices.

No. 166 (cont)

3) The wireless access point should provide the capability to employ encryption mechanisms to prevent loss of integrity and confidentiality of information during communication.

7.3.5 Segregation and segmentation of network

7.3.5.1 Segregation of networks should be carried out as per the philosophy document and risk assessment. The segregation can be done by using either physically different networks or by using different logical networks (e.g. virtual private networking). The perimeter of each network zone should be well defined.

7.3.5.2 When access between different network zones is allowed, it should be controlled at the perimeter by using appropriate boundary protection devices (e.g. proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels).

7.3.5.3 Physical segregation of network:

A physically segregated network should have following characteristics:

1) No permanent gateway to other network zone should be installed on the network perimeter.

2) No permanent wireless access should be connected to the network perimeter for OT systems of Category II and III except where specific approval is obtained from Classification Society.

3) Ports for removable devices should be logically made unusable. If sensitive data are contained inside the network it is recommended to provide physical locks in order to prevent the uncontrolled access to these ports.

7.3.5.4 Logical segregation of network

A logically segregated network should have following characteristics:

1) No data communication between different network zones except through appropriate boundary protection devices.

2) Ports for removable devices should be treated with the same measure as physical segregation.

7.3.5.5 Network segmentation

It should be possible to implement network segmentation into various zones as per identified risk level. Critical systems should 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.

For a computer-based system providing essential contribution for the availability of safety-critical functions or systems having remote access from shore, a demilitarised zone (DMZ) may be used in conjunction with a control zone to provide additional risk reduction opportunities between the low-security level business or administrative network and the high-security level control network. A DMZ eliminates or reduces all direct communication between the control zone and the other nonessential zones. Use of DMZ minimizes the number of people directly accessing critical control zone devices. Segmenting networks should be

No. 166 (cont)

consistent with risk management in accordance with IEC 62443 or relevant standard on industrial controls.

Following should be implemented:

1) For networks which include systems of Category II physical segmentation or logical segmentation on VLANs (Virtual LAN) should be provided.

2) For networks which include systems of Category III physical segmentation should be provided and independent switches should be used.

3) Segmentation should be such as to prevent loss of critical systems upon a single failure for Category III systems, which required redundancy by Classification Society.

4) Where interconnection between networks which include systems of Category I or II or III is considered necessary, the purpose and method should be documented. The interconnection between networks which include systems of lower Category and those of higher Category should result in all interconnected systems being treated as the highest Category included, e.g. if a network which includes systems of Category I is connected to a network which includes systems of Category III both networks should be regarded as Category III.

5) For networks which include systems of Category II or III, means should be provided to enforce availability and integrity of data, e.g. encryption or hashing.

7.3.6 Network protection safeguards

Suitable network protection and detection systems, based on network criticality analysis should be provided for inter network communication. Following controls should be provided:

1) Management of identities and credentials of network users, including M2M networks

2) Enhanced authentication control, or restricted privileges, for remote access or from access points of the lower level of security

3) Physical access control to network access points

4) Pervasive implementation of Least Privilege Policy

5) Encryption for data at rest (stored) and data in transit (exchanged)

6) Integrity checks for data at rest and data in transit

7) Separation of networks, firewalling, De-Militarized Zones (DMZs), etc.

8) Separation of networks supporting IT systems (e.g. for administrative tasks, passenger and crew connectivity, etc.), OT systems (e.g. for engine control, cargo control, etc.) and alarm systems

9) Event logging and Quality of Service (Quos)

10) Use of routing technology for ship to shore and ship to ship communication, where considered necessary through risk assessment, separation of CAT I, CAT II, CATIII systems networks should be implemented.

No. 166 (cont)

11) Where considered necessary through risk assessment additional layers of controls should be provided. (A defence in depth approach)

7.3.7 Cyber incident detection safeguards

A document containing description of the safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented is to be developed. Controls should be based on risk assessment of a particular network and appropriate safeguards should be identified to suit a particular system.

As most of the existing available detection methods are specific to IT system or specific to few communication protocols, implementation of various detection methods given below for OT systems should be implemented as per equipment manufacturer recommendations.

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

2) Connection quality monitoring tools

3) Event log auditing tools and procedures

4) Timely incident alert systems

5) Network Performance Monitoring System

6) Malicious code detection tools, e.g. antivirus, antimalware

7) Collection of all the events detected by the above listed systems, tools- from a) to g) - with dedicated network facility

8) Displaying of security events, e.g. Security Information Event Monitoring (SIEM)

7.3.8 Network and system Recovery Measures

7.3.8.1 Appropriate recovery measures for networks affected due to a cyber event should be developed by the supplier and/or system integrator as per industry standard practices. Critical systems should have the capability to support back-up and restore in a timely, complete and safe manner.

7.3.8.2 Following measures to restore network capabilities or service that has been impaired due to a cyber incident should be provided:

1) Redundancy or backup measure of data, network devices and communication media

2) Controlled shutdown, reset and restart of affected systems

7.3.9 Protection devices

7.3.9.1 Firewalls

1) Internal firewall should be applied between each network segment.

2) Perimeter Firewall between onboard network and external network should be applied.

3) If safety of life or safety of ship is dependent on communication between network segments through a firewalling system, then two different firewalls should be provided

No. 166 (cont)

and both the firewalls should operate in real time. They should be arranged such that in case of failure of one of the firewall units or cyber incident, the second unit can maintain the full security of the Ship's network.

4) Firewall should be applied for network between onboard computer systems of Category II or Category III.

5) The firewall rules should be designed to allow passage of data traffic that is essential for the intended operation of that network. To prevent any unintended communication taking place, the last rule of the firewall should be configured to deny all communication.

7.3.9.2 Routers and protocols

1) Each segment should have its own range of Internet Protocol (IP) address.

2) Protocols should be encrypted. Data transfer from systems for Category II and III through networks should be properly encrypted in the software.

3) Spanning Tree Protocol or similar should be applied to network switches.

7.3.9.3 Anti-virus

Where practicable Anti-virus software should be installed on each onboard computer based system or any programmable device having a standard operating system. The Anti-virus software should not affect performance of Category II and III systems. For PLCs or other equipment without standard operating system, security measures should be applied in accordance with manufacturer recommendations.

Anti-virus should include the following prevention:

1) anti-virus signature database

2) file pattern

3) file size

4) file type

5) grayware

6) heuristics

7) Virus scan. Means to identify the status of anti-virus database should be provided on each onboard computer.

8) updates and procedure for update of anti-virus software should be documented

7.3.10 Integration

7.3.10.1 Installation of any software in integrated systems (during integration phase onboard) should be carried out through the usage of controlled computer, removable media or DMZ. Direct connection to the internet should be avoided. Integration between Controlled and uncontrolled networks is to be minimal and controlled. Suitable network protection and detection systems, based on network criticality analysis should be provided for inter network

No. 166 (cont)

communication. Suitable network protection devices at perimeter level or between networks should be implemented.

7.3.10.2 Interfaces

Standard interfaces should be used for data exchange between different networks. Each network should be designed in compliance with recognized Standards such as IEC 61158 or IEC 61784, etc or equivalent.

7.3.10.3 Advanced Security Measures

Following advanced security measures as applicable should be implemented on board (especially where IT system is integrated with OT systems) and should be based on risk analysis specific to an installation.

1) Virtual private network (VPN) should be deployed into the network. VPN protocols should encrypt traffic going from sender to receiver.

2) Intrusion prevention system (IPS) should be deployed into the network. IPS should issue an alarm in case of starting to record events that may affect security. It should also block unwanted traffic.

3) Alarm from IPS should be generated at the relevant and centralized station which is normally considered to be manned.

4) IPS should contain predefined signatures (database of attack signatures), custom signature entries, out-of-band mode, packet logging.

5) Data loss prevention (DLP) software should be implemented to prevent “leakage’’ of important data.

6) Content filtering technology module should be installed. This device should block traffic to and from a network by IP address, domain name/URL and type of content.

7) Anti-spam filtering should be applied.

7.3.10.4. Safety functions in the integrated network should be implemented in dedicated hardware units (switches, etc.) where considered necessary by risk analysis.

7.3.10.5. Safety functions should be arranged with redundancy as per Class requirement.

7.3.10.6. Redundant system, upon failure, should have sufficient self-diagnostics to effectively transfer active execution to the standby unit.

7.3.10.7. A single fault should not cause any function of the critical system in the integrated network to be unavailable. (For systems indicated at UR E22 the criterion should be as per UR or else as per Class requirement).

7.3.10.8. Any failure should be indicated as an alarm as per Class requirement and at the same time all functions should be maintained in order to achieve operation of the critical system(s) in an integrated network.

No. 166 (cont)

7.3.11 Cyber Incident Response measure

The System Integrator and Suppliers should consider and implement measures aimed to take appropriate actions regarding detected cyber security events on networks so as to limit the cyber incident impact to the network zone of origin. The measures should be aimed to minimise the possibility of disruptions to OT systems, which could have effect on availability of systems required for safety critical functions. The measures along with test plan should be developed.

7.4 Computer based system Physical Access control

7.4.1 Installation

Computer based systems may be installed at a location which may be easy to access to facilitate effective and efficient operation of ship by the crew and various stakeholders who need to access to computer based systems for installation, integration, maintenance, repair, replacement, disposal etc.

Design document showing physical location of computer based system should be developed. Information on physical security perimeter (see 7.4.2), measures to restrict physical access (see 7.4.3 to 7.4.7) and supporting utilities (see 7.4.4.2) should also be included in the design document.

7.4.2 Physical security perimeter

Where possible computer based systems of category II and III should be located in rooms that can normally be locked or restricted space to prevent unauthorized access (e.g. wheelhouse, electric room, machinery spaces are considered as limited space.). If this is not possible then the equipment should be located in lockable cabinets or consoles.

7.4.3 Measures to restrict physical access to secure areas

The ship owner (the term "ship owner" should be read as "shipbuilder" while the vessel is under construction) should design and apply physical security measures to restrict physical access such as lock, surveillance camera, etc. for secure areas housing key computers and network devices for systems of Cat. II and III.

7.4.4 Equipment

7.4.4.1 Equipment installation and protection

1) Equipment should be installed to minimize the risk of potential physical threats, such as theft or mechanical damage.

2) Equipment should be safeguarded to avoid unauthorized access or misuse by applicable physical security means (e.g. physical blocking device or locking device).

7.4.4.2 Supporting utilities for equipment

Supporting utilities such as electric power supply, telecommunications, air conditioning, and ventilation should be according to equipment supplier’s requirement with alarms for their malfunctions. In case of failure of supporting utilities, UPS (Uninterruptible Power Supply), emergency power backup or multiple feeds should be provided according to equipment supplier’s requirement if serious impact to computer based system will be caused by failure of supporting utilities.

No. 166 (cont)

7.4.5 Cabling

Installation of cables should be as per Classification requirements.

7.4.6 Use of mobile devices and portable storage devices

The connection to the network should be physically or logically blocked except when connecting an external device for maintenance.

7.4.7 Equipment to restrict physical access

Physical security equipment (Equipment to restrict physical access e.g. surveillance cameras, intrusion detectors, electronic locks, etc.) should have strong authentication method such as password, smart card, tokens, etc.

7.5 Software Assurance

7.5.1 Design & Development

7.5.1.1 Design, development and testing of software should be carried out in a structured manner following well laid procedures /standards to ensure reliable operation of software.

7.5.1.2 Software should be developed in accordance with a strategy for functionality in accordance with IACS UR E22.

7.5.1.3 Computer based systems which provide control, alarm, monitoring, safety or internal communication functions are subject to requirements of the Class Society.

7.5.1.4 A global top to bottom approach should be undertaken regarding software and the integration in a system, spanning the software lifecycle. The validation and verification approach for the software should be accomplished according to software development standards as per IACS UR E22, recognised IEC/ISO or an equivalent standards recognized by the Class Society.

7.5.1.5 System security

For Category I, II, and III systems, logical security measures such as authorisation and authentication procedures should be in place to prevent unauthorized or unintentional modification of software, whether undertaken at the physical system or remotely.

7.5.1.6 When a software revision can lead to hardware change, the hardware used should be suitable for the equipment or system according to applicable requirements of the Classification Society.

7.5.1.7 The backup and recovery of software and data should be considered in design phase.

7.5.2 Software maintenance

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

7.5.2.2 Following should be considered essential during software execution process and should be implemented as per general industry practices Industry standards on Software maintenance of computer based systems.

No. 166 (cont)

1) Maintenance access
2) Roll back
3) Diagnostic reports

7.6 Remote Access (from locations not onboard the ship):

7.6.1 Ship to shore interface

7.6.1.1 The items in this sub section should be applied to onboard Information Technology (IT) and Operation Technology (OT) systems which can be accessed from a remote location (not onboard the ship).

7.6.1.2 Data transmission to Computer based systems on board of category II and III, which is critical for the safety of navigation, power and cargo management, should be protected against unauthorized access and should have the necessary capabilities to mitigate the risks arising due to remote access. The equipment should have the capability to terminate a connection from the onboard terminal and revert to the known and uncorrupted state. Where equipment does not have the capability, the same should be arranged through installation of additional network devices, which support such functions.

In case of cyber incident, the system is to ensure that, locally it is possible to restore to a situation delivering a full and safe local access to the operations. A risk assessment should take into account threats and mitigation measures associated with remote access.

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

7.6.1.4 A test plan should be developed to test the satisfactory functioning of remote access feature. The test program should be prepared and executed by the Supplier or System Integrator The test program should include procedures for functional tests and failure tests. Relevant results/ observations should be recorded in a test report.

7.6.2 Configuration of network devices

Networks, that are provided with remote access should be controlled (i.e. designed to prevent any security risks from connected devices by use of firewalls, routers and switches (reference IEC 61162-460)External access of such connections should be secured to prevent unauthorised access.

The network devices, such as switches should be provided with configuration parameters, such as,

1) Password encryption
2) Password protected console ports
3) Configurable session timeouts
4) Flow control enabled
5) Unused ports closed

7.6.3 Remote maintenance

Vessels provided with facility for remote access for maintenance should implement following safeguards:

No. 166 (cont)

7.6.3.1 A hardware or software mechanisms is to be provided on board to manage the acceptance of remote maintenance. The use of these mechanisms relies on the results of the risk assessment.
7.6.3.2 It should be possible at all times to cancel remote maintenance from ship.

7.6.3.3 Initiation of maintenance session should be authenticated by the external maintenance personnel. Passwords should not be transmitted in unencrypted form. Tunnelling traffic through an encrypting virtual private network (VPN) should be adopted.

7.6.3.4 Activation of maximum-trial period in the event of failed access attempts should be provided.

7.6.3.5 Activation of a lock-out period in the event of inactivity should be provided.

7.6.3.6 The system should have the feature to Block the access for remote maintenance feature during normal operation. Express approval should be limited and should be accorded only for a precisely defined period of time.

7.6.3.7 If the connection to the remote maintenance location is disrupted for some reason, access to the system should be terminated by an automatic logout function.

7.7 Data Quality

7.7.1 Data security

7.7.1.1 The general objective of Data Security is to ensure the confidentiality, integrity and availability 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 prioritise availability and then integrity. The three terms can be broadly defined as below.

1. CONFIDENTIALITY – a loss of confidentiality is the unauthorized disclosure of information.

2. INTEGRITY – a loss of integrity is the unauthorized modification or destruction of information.

3. AVAILABILITY – a loss of availability is the disruption of access to, or use of an information system

7.7.1.2 The scope of application of Data Assurance covers data whose lifecycle is entirely within on board computer based system, as well as data exchanged with shore systems connected to the on board networks. While the consequences of un-authorised 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 machinery control and safety with a safety or environmental impact), where data transfers and updates are implemented using a network, these data security objectives share common features and should be considered for the system as a whole.

7.7.2 Data Categorisation

Data categorisation document identifying the risks for various categories of data should be developed.

No. 166 (cont)

7.7.2.1 Data should be categorized by the supplier or system integrator according to the possible consequences of a breach of data assurance on the three security objectives defined at 7.7.1.1.

7.7.2.2 The potential impact of loss of data assurance should be categorized as follows:

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

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

7.7.2.3 The following table (Table 1) shows how to assign system with categories based on their effects on system confidentiality, integrity and availability.

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

No. 166 (cont)

7.7.2.4 The categorization described above should be used as guidance and definitions should be assessed on a case by case basis.

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

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

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

7.7.3 Secured and encrypted data

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

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

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

7.7.4 Data storage

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

7.7.4.2 Devices used to store data for category II or III systems should be appropriate for intended use and suitable for the marine environment (ref UR E10). Data stored on such devices should be appropriately replicated to minimize data loss in case of device single failure.

7.8 System Recovery

7.8.1 Manual Operation

7.8.1.1 The need for manual backup as defined in SOLAS, plus the additional considerations specific to Cyber Concerns should be considered during design stage. 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 clusters of affected systems for planning manual response

2) Identification of potentials for cascading failure after critical gear fails

While evaluating the single failure requirement of SOLAS, cyber incidents in local control system should also be included in list of failure.

7.8.1.2 The main purpose of this subsection is to consider the above mentioned SOLAS requirement on complex programmable control systems for propulsion machinery. Design recommendations given in this section can be also applied to manual/local control of Category II / Category III systems other than propulsion systems. The items identified are

No. 166 (cont)

intended to address the need for cyber resilience for critical onboard computer based systems.

7.8.2 Design recommendations for machinery systems

1) The individual local control systems should include necessary Human Machine Interface (HMI) for effective local operation.

2) Local control systems should be of a robust design suitable for the environmental exposure and the intended operation.

3) Local control systems should be self-contained and not depend on other systems or external communication links for its intended operation.

4) Failure in remote control systems (from a location onboard the ship) should not prevent local operation.

5) Unused communication ports should be disabled.

6) Facilities for selecting “local” at or near the machinery should be provided for. When local control is selected, any control signal(s) from the remote control system (from a location onboard the ship) should be ignored.

8. Verification Testing

General

The verification and testing should be carried out at different stages, such as Design verification, testing on board following installation and during ships life. Subsequent to construction of new builds the Vessel computer based system testing should be carried out to verify satisfactory performance of the system. The section specifies methodology to verify the topics and processes identified in Section 7, as part of Goal based standard approach.

The testing should be carried out after complete installation of network cables and all devices. The simulation tests should demonstrate how the commands from the computer based system may be executed.

Scope of testing

The scope of verification & testing of the computer based system should at least include the following:

1) All cabling and network devices

2) All functionality relating to network communication by nodes connected to the network system

3) All external and internal communications

4) Monitoring and alarm systems

5) Backup procedures and results

6) Verify effective response and recovery in an event of failure of critical computer based system used for Cat I,II and III systems (contingency plan)

No. 166 (cont)

7) Local control ability in case of cyber incident.

8.1 Asset Identification

8.1.1 Inventory of assets

An inventory of all computer based systems According to Clause 7.1.1 should be submitted to Classification Society for verification. The list could be initially developed by shipbuilder and subsequently by owner/company during life of ship, whenever there are major changes in inventory.

8.1.2 System Documentation

8.1.2.1 Following plans/documents should be submitted to Classification society towards design verification:

1) System Philosophy document

2) Network communication diagram

3) Logical map of networks

8.1.2.2 Following list of inventories specifying the details as indicated at Clause 7.1.2 should be maintained on board and submitted to surveyor when requested.

1) Inventory of communicating devices

2) Inventory network communication devices

3) Logical map of networks

    IP addresses

    Non IP addresses

    Non Ethernet access points

    Desk tops and servers

    Connectors and communicating filed devices

4) Software inventory

5) Inventory of network services for each equipment.

8.1.3 Risk Assessment

Risk assessment document indicating the identified risks and the proposed measures to mitigate the risk should be submitted for Classification society review.

8.2 Communication and interfaces

Technical items should be verified as part of system design review. The testing for communication and interfaces should be covered as part of network testing at 8.3.

No. 166 (cont)

8.3 Network.

8.3.1 Equipment Standard

The objective of the verification is to confirm through review of certificate and /or plans, the suitability of the network device for the intended operation in a marine environment. When requested, during onboard survey, the shipyard/system integrator should submit relevant certificates to confirm that the equipment is designed, manufactured and tested as per the related standard.

8.3.2 Design

8.3.2.1 Network Design Document

Basic network design document showing details of all OT and IT network systems (when interfaced with OT systems) should be submitted to Classification societies for review.

8.3.2.2 Where the design philosophy includes FMEA, the analysis document should be submitted for classification society review and the results should be demonstrating through FMEA trials.

8.3.2.3. Following tests to verify the network functionality and response should be demonstrated during survey.

1) Network loading

2) Network storm test.

3) Redundancy tests where system is designed with redundant network and network devices

8.3.3 Installation

Satisfactory installation of the network devices as per the approved plan should be verified during onboard survey.

8.3.4 Control, Monitoring and alarm

The objective of the tests is to ensure reliability and quality of the network systems and the provision of suitable alarms and monitoring systems to detect abnormal incidents, including provision of such monitoring system at suitable locations. The list of controls, alarms and parameters/incidents to be monitored should be, as a minimum, as listed in Section 7.3.4 and should be verified during onboard survey.

8.3.5 Segregation and segmentation of network

8.3.5.1 Design review

The network diagram indicating provision to divide onboard networks into separate network zones based on network communication documents, clearly specifying the philosophy of segregation should be submitted for Classification society review.

8.3.5.2 Installation and operation of appropriate boundary protection devices (e.g. proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) between network zones should be verified during onboard survey.

No. 166 (cont)

8.3.5.3 Where Physical segregation of network is adopted, it should be ensured through design that:

1) No permanent gateway to other network zone should be installed on the network perimeter.

2) No permanent wireless access should be connected to the network perimeter.

3) Ports for removable devices should be logically made unusable.

The performance of the network should be verified during on board survey as per reviewed test plan.

8.3.5.4 Logical segregation of network

Where Logical segregation of the network is provided following characteristics should be verified onboard.

1) No data communication between different network zones through network devices.

2) Ports for removable devices should be treated with the same measure as physical segregation.

8.3.5.5 Network segmentation

Implementation of network segmentation into various network zones as per identified risk level should be demonstrated on board. The testing should include verification of security levels between zones. Where DMZ is used, the arrangement and installation plan should be reviewed and satisfactory functionality of DMZ to eliminate or reduces all direct communication between the control network zone and the other nonessential network zones should be verified during onboard survey as per reviewed test plan. The test plan should include testing of redundant networks.

8.3.6 Network protection safeguards

The System Integrator and Supplier should prepare a document to demonstrate satisfactory implementation of safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented.

A test plan to verify the implemented control as given at 7.3.6 should be developed and tested during onboard survey. A copy of above documents should be retained onboard and made available to the Classification Society for subsequent verification during ship life.

8.3.7 Cyber incident detection safeguards

The System Integrator and Supplier should prepare a document to demonstrate satisfactory implementation of safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented.

A test plan to verify the implemented control as given at 7.3.7 should be developed and tested during onboard survey. A copy of above documents should be retained onboard and made available to the Classification Society for subsequent verification during ship life.

No. 166 (cont)

8.3.8 Network and System Recovery measures

8.3.8.1 The System Integrator and Supplier should prepare a document to demonstrate satisfactory implementation of safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented.

A test plan to verify the implemented control as given at 7.3.8 should be developed and tested during onboard survey. Restoration of critical systems in a timely, complete and safe manner should be verified.

A copy of above documents should be retained onboard and made available to the Classification Society for subsequent verification during ship life.

8.3.9 Protection devices

Satisfactory implementation of protective devices should be verified on board survey. A test plan to verify the implemented control as given at 7.3.9 should be developed and tested during onboard survey. The document showing configuration of the tested device/system should be retained onboard and made available to the Classification Society for subsequent verification during ship life.

8.3.10 Integration

8.3.10.1 Integration is generally foreseen between OT systems. Segregation is between OT and IT as far as possible. However where the OT networks are integrated with other OT and /or IT network, the network communication functionality should be verified as per reviewed test plan. Continuous operation of critical systems due to loss of one of the interconnected system / network should be verified as per FMEA trial procedure.

8.3.11 Cyber Incident Response Measures

The System Integrator and Supplier should prepare a document to demonstrate satisfactory implementation of safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented.

A test plan to verify the implementation of control as given at clause 7.3.11 should be developed and tested during onboard survey. A copy of above documents should be retained onboard and made available to the Classification Society for subsequent verification during ship life.

8.4 Computer based systems Physical Access control

8.4.1 Installation

Design document mentioned in 7.4.1 should be submitted to Classification Society for verification. Verification of the physical location and access control for various onboard computer based systems, should be carried out through verification of design documentation and subsequently during on board survey.

8.4.2 Physical Security Perimeter

The Design verification and testing of the security perimeter should be in accordance with each Classification Society’s requirements.

No. 166 (cont)

8.4.3 Measures to restrict physical access to secure areas

Measures implemented to restrict physical access to secure areas should be verified during survey.

8.4.4 Equipment

Design verification and certification of the equipment should be in accordance with each Classification Society's requirements.

8.4.5 Cabling

Certification and installation verification of cables should be in accordance with each Classification Society's requirements.

8.4.6 Use of mobile devices and portable storage devices

Test to verify that network cannot be accessed by unauthorized mobile and portable storage devices should be carried out on board.

8.4.7 Equipment to restrict physical access

Cyber-enabled equipment to restrict physical access should be tested to ensure that it is kept working in normal operating state.

8.5 Software assurance

8.5.1 Design & Development

The design development and testing of software for category I, II and III systems should be carried out as per IACS UR E22.

8.5.2 Software maintenance

8.5.2.1 Subsequent to execution of software maintenance, following tests should be carried out by the Service Provider for validation:

1) Regression tests

2) New functionalities and/or improvements tests;

3) Load tests.

8.5.2.2 The classification society should witness the testing of software maintenance as appropriate or review the results of testing.

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

8.5.2.4 During the software maintenance planning the Producer of software or System Integrator and/or the Data Provider should issue a Test Plan specifying the tests to be executed. Test Cases covering both normal operation and failure conditions should be specified in the Test Plan.

No. 166 (cont)

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

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

8.5.2.7 The Load test should be conducted to verify the behaviour of the system under a specific expected load, under both normal and peak conditions.

8.5.2.8 The tests should cover each equipment which are subject should be subdivided into the following activities:

1) The Test Plan should determine the scope and risks associated with the software maintenance, and identify the objectives of testing, the method of testing, the expected time and resources required for the testing process. It should provide clear information on how the tests are carried out and how to verify the success or failure of each test.

2) Test cases should be selected based on applicable requirements, design specifications, risk analysis and interfaces of the equipment subject to software maintenance.

3) After the tests have been executed, the results of the executed tests should be recorded, including the versions of the software under tests.

4) Test of procedures that can roll back to a previous software version and configuration during software maintenance, after a software update has been attempted to the shipboard equipment without success.

5) The results of the executed tests should be discussed and analyzed in order to check which planned software updates can be delivered and to confirm that no failure has been detected during the test activities. In case of failure, corrective action should be planned, and an updated Test Plan should be issued.

6) The process should consider the implications and any risks associated that could result from the rollback and identify appropriate testing performed post roll back in order to satisfy the administration and class of satisfactory working condition of the system.

7) Rollback procedures should be demonstrated to the classification society when required.

8) Documentation of the outcome of testing should be made available to the ship-owner and when required to system integrators, data providers and the classification society.

8.5.2.9 Execution of tests

Extracts from the updated software log or OSMLS for the on board for software should be submitted to classification society during onboard survey.

8.5.2.10 A report from the Service Provider that can be used to record software maintenance activity covered by IACS UR E22 performed on computer-based systems to be submitted to classification society during onboard survey.

8.5.2.11 When the society is acting as approver of the on-board systems as part of the execution, onboard tests should be conducted to check that a computer-based system operates as expected in its final environment, integrated with all other systems with which it interacts.

No. 166 (cont)

8.5.2.12 The test should ensure that the system under test:

1) Performs functions the system was designed for

2) Reacts safely in case of failures originated internally or by devices external to the system

3) Interacts safely with other systems implemented on board vessel

8.5.2.13 For Category II and III systems test programs and procedures for functional tests and failure tests should be done in accordance with the requirements in IACS UR E22.

8.5.2.14 For Category II and III systems test programs and procedures should include checking of the equipment (e.g. software, versions and configuration) as explained in 7.5.2.1.

8.6 Remote Access (from locations not onboard the ship)

8.6.1 Ship to Shore Interface

8.6.1.1 The test program and test report mentioned in 7.6.1.4 should be made available to the Classification Society upon request. The Classification Society may request to witness the execution of tests and/or execute additional tests.

8.6.1.2 Patches and updates should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. A confirmation report from the software supplier towards above should be obtained, prior to undertaking remote update. They should also be prevented from installation unless signed with recognized and approved certificates.

8.6.1.3 A log should be provided for all information needed to successfully audit system activity.

8.6.2 Configuration of network devices such as firewalls, routers and switches
The satisfactory operation of network devices to prevent unauthorised access from remote locations should be verified during on board survey, as per approved test plan.

8.6.3 Remote maintenance

Authorisation and disconnection of remote maintained systems including following features should be demonstrated during on board survey:

1) Session lock

2) Auto log out function

3) Blocking access during normal operation

4) Monitoring remote maintenance activity

8.7 Data Quality

8.7.1 Data Security

Document showing how the confidentiality, integrity and availability of data residing in or flowing to critical systems is addressed should be submitted for classification society review.

No. 166 (cont)

The controls for data storage and transfer should be verified during onboard survey as per reviewed test plan.

8.7.2 Data Categorisation

Data categorisation document identifying the risks for various categories of data should be submitted to Classification societies for review.

8.7.3 Secured and encrypted data

Networks protocols should ensure the integrity of control, alarm, monitoring, communication and safety related data, and provide timely recovery of corrupted or invalid data. Verification of origin and destination of data should be considered as in the scope. Evidence should be provided to the Classification Society of the above mentioned measures upon request.

8.7.4 Data Storage

Evidence should be provided to the Classification Society of the measures specified at 7.7.4 upon request.

8.8 System Recovery

8.8.1 Manual Operation

8.8.1.1 Tests to demonstrate the necessary independence, functionality and operability of critical system as detailed at section 7.8 should be carried out during onboard survey.

8.8.1.2 Verify that provision for a suitable HMI (communication means, controls, indications, alarms, etc as required) at each location where manual or local control is provided.

8.8.1.3 Review of each system to identify if safety functions are independent of control which could be affected in a Cyber Incident.

8.8.1.4 Verify that Cyber Incident would not be destructive to equipment to the extent that it is unusable under manual backup.

8.8.2 Design recommendations for Machinery systems

Documents showing independency of local controls, effect of single failure, interfaces to other systems should be submitted for classification society for verification.

No. 166 (cont)

Appendix A: Detailed list of Standard

1. ISO/IEC 14764:2006 - Software Engineering -- Software Life Cycle Processes -- Maintenance
2. NIST Special Publication 800-34 Rev.1 - Contingency Planning Guide for Federal Information Systems
3. NIST Special Publication 800-53 Rev.4 - Security and Privacy Controls for Federal Information Systems and Organizations
4. NIST Special Publication 800-82 Rev. 2 - Guide to Industrial Control Systems (ICS) Security
5. IEC 62443-2-1: 2010 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
6. IEC 61162 - Digital interfaces for navigational equipment within a ship
7. FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems
8. ISO 8000-8:2015 - Data quality -- Part 8: Information and data quality: Concepts and measuring
9. ISO/IEC 27002 2013 - Information technology -- Security techniques -- Code of practice for information security controls
10. IEC 62443-3-3 2013 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
11. ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements
12. ISO/IEC 27033-1:2015 - Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
13. IEC-60050 - International electro technical vocabulary
14. ISO/IEC 27000:2018 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
15. ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls
16. IEC 61162- 460 (2018) Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security
17. IEC 6162 450 - Maritime navigation and radio communication equipment and systems – Digital interfaces
18. ISO 16425 - Ships and marine technology -- Guidelines for the installation of ship communication networks for shipboard equipment and systems
19. Industry Standard on Software Maintenance of Shipboard Equipment” Version 1.0. CIRM/BIMCO
20. ISO 24060 “Software maintenance of shipboard equipment” (Awaiting publication at the time of writing)

No. 166 (cont)

Appendix B: Documents referred in Recommendation

			Requested by Class for			
Sr no	**Document Description**	**Developed By**	**Design review**	**Installation review**	**onboard review**	**Remark**
1	Inventory list of computer based system	Designer	X			
2	Design philosophy document	Designer	X			
3	Network communication document	Designer	X			
4	Logical map of networks	Designer	X			
5	inventories	Designer	X			
6	communicating device	Designer	X			
7	network communication devices	Designer	X			
8	logical inventories	Designer	X			
9	Software inventory	Designer			X	
10	Inventory of network services for each equipment	Designer	X			
11	Risk assessment	Designer	X			
12	Equipment certificates	OEM / Class			X	
13	Network Design document	Designer	X			
14	Network design FMEA	Designer	X			
15	Installation plan	Designer	X	X		
16	Control, monitoring & Alarm	Designer	X		X	
17	Segregation and segmentation of network	Designer	X	X		
18	Network protection safeguards	Designer	X		X	
19	Cyber incident detection safeguards	Designer	X		X	
20	Integrated network system	Designer	X		X	
21	Network and system recovery measures	Designer	X		X	
22	Protection devices	Designer	X		X	
23	Cyber incident response and measures	Designer			X	
24	Security perimeter	Designer	X		X	
25	Software maintenance Test results	OEM			X	on request
26	Execution of tests - Updated software log or OSMLS	OEM			X	on request
27	Software maintenance plan	OEM	X			
28	Ship to shore interface test program	Designer	X		X	
29	Data security	Designer			X	
30	Data Categorisation	Designer	X			

No. 166 (cont)

31	Data Storage	Designer	X		X	
32	Design recommendations for machinery systems	Designer	X		X	
Note						
1	**Design review:** The document would be required for Class review.					
	Installation review: The document would be required by Class during new build installation stage.					
	Onboard review: The document would be referred during onboard verification of systems during new build stage and subsequently during operations.					
2	During new build stage the initial philosophy documents will be generally developed by designer, system integrator. Subsequently OEM inputs would be required towards development of detailed engineering drawings.					
3	Documents for inventories, software maintenance, risk assessment and protection measures would be initially developed by designer and subsequently maintained by owner/ship management company.					
4	Where documents are required for onboard verification during life of ship, a copy of the same should be made available to surveyor onboard.					

No. 166 (cont)

Appendix C: Mapping of Sub goals to Technical & Verification items

Sub Goal (SG)	Functional requirement	Scope/areas to be addressed	Technical item	Verification Testing	Review methodology		
					Design review	Equipment certification	Onboard survey
SG1	Identify-1	Inventory of systems, data, risk assessment to ensure normal operations and address cyber risks	7.1.1 7.1.3 7.7.2	8.1.1 8.1.3 8.7.2	X X X	- - -	- - -
	Identify-2	Essential OT systems inventory, identify inter dependencies, risk analysis	7.1.2 7.1.3	8.1.2 8.1.3	X X	- -	- -
SG2	Protect-1	Secure config – equipment, suitability for location, availability of data Secure interfacing s/w assurance	7.2 7.3.1 7.3.2 7.3.3 7.3.9.2 & 7.3.9.3 7.4 7.5 7.7	8.2 8.3.1 8.3.2 8.3.3 8.3.9 8.4 8.5 8.7	X X X X X X X	- X X - - - - -	- X X X - X X X
	Protect-2	Integration	7.3.10	8.3.10	X	X	X
	Protect-3	Segmentation	7.3.5	8.3.5	X	-	X
	Protect-4	Restrict logical access to OT	7.3.6 7.6	8.3.6 8.6	X X	- X	X X
	Pprtect-5	Minimise Disruption to safety systems	7.3.9.1	8.3.9	X	-	X
SG3	Detect-1	Monitoring, Detect cyber events	7.3.4 7.3.7	8.3.4 8.3.7	X X	X -	X X
SG4	Respond-1	Contain impact	7.8	8.8	X	X	X
	Respond-2	Isolation of safety critical functions	7.3.11	8.3.11	X	-	X
SG5	Recover	Data backup and restore	7.3.8 7.7.4	8.3.8 8.7.4	X X	- -	X -

No. 166 (cont)

Annex A

Guidance on Operational Aspects addressed in Recommendations

Assumptions on operational aspects and management

Identify

- All Operation technology (OT) assets and Information technology (IT) assets (when they are connected with OT systems), including network devices, data communication flows to and between the assets should be inventoried;
- Cyber risks arising out of cyber incidents that can affect safety of vessel, human safety, and environment should be identified and documented (from owners point of view systems required for business can be included);
- Risk management strategy to mitigate the risks for identified IT and OT vulnerable systems should be formulated and documented.

Protect

- Physical access to OT, data used by OT, and network infrastructure should be restricted and controlled;
- Procedures and controls are to be developed and implemented to ensure network resilience;
- Controls to address cyber risks due to remote shore connectivity should be implemented;
- Hardware and software upgrades should be planned for intended functionality and verified;
- Event logs should be analysed to help identify suspicious or unauthorised activity.

Detect

- Controls to enable timely discovery of cyber events should be developed. The cyber events should be evaluated at periodical intervals.

Respond

- Appropriate safeguards should be developed and implemented to ensure continuity of critical services to limit or contain the impact of a cyber event;
- Response processes and procedures should be executed and maintained, to ensure timely response to detected cyber events;
- Response activities should be coordinated with internal and external stakeholders, as appropriate, to seek external shore support as deemed necessary;
- Analysis should be conducted to ensure adequate response and support recovery activities. Such activities should be aimed to prevent expansion of an event, mitigate its effects, and eradicate or contain the incident;

No. 166 (cont)

- Appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber events are to be developed and implemented;
- Recovery procedures should be tested, executed, and maintained.

Recover

- Back-up data necessary to restore critical systems should be readily available. The availability should be ensured through manual or automatic data back ups.

A.1 Asset Identification

A.1.1 Inventory of Assets

A.1.1.1 Change Management:

When software is being maintained, the inventory list should include a record of the previous and current software versions installed, including a repository of related electronic service report documents.

A.1.1.2 Effect due to hardware or software changes should be analysed.

A.1.2 System Documentation

Under the responsibility of System Integrator and Suppliers, the following items should be identified to develop a suitable understanding and management of onboard networks and their security. The objective would be to Identify of key network resources and failure impact as follows:

1) Networks on board
2) Networked IT and OT systems and their category according to UR E22
3) Data flows and network devices or resources potentially limiting them
4) Connections with external systems or networks
5) Access points and interfaces, including machine-to-machine (M2M) interfaces
6) Roles and responsibilities of users
7) Network vulnerabilities and threats, including those related to information security and those related to the quality of communication service, e.g. leveraging vulnerability scan tools, security information databases, etc.
8) Network configuration

A.1.3 Risk assessment

A.1.3.1 As part of the risk assessment, acceptability thresholds should be defined, taking into account the probability of occurrence of cyber incidents and the effects on safety and security

No. 166 (cont)

that are likely to occur as a consequence thereof. The risk assessment during life of the ship should be carried out by the owner/company.

Following factors are also to be considered during risk evaluation:

1) The possible impact of unauthorized access, misuse, modification, destruction or improper disclosure of the information managed in each network onboard.

2) The possible impact of degradation of data flow or complete loss of connection among network nodes.

3) Factors related to the ship as a whole, like type of service and navigation, overall level of digitalization on board, extension and interconnection of different networks, etc.

A.1.3.2 The System Integrator and Supplier should prepare a risk assessment report. A copy of the report should be given to the Owner upon delivery, retained by the Owner and made available to the Classification Society upon request.

A.1.3.3 The potential impact of network failures on safety and security should be analyzed and acceptable risk thresholds should be defined. The definition of acceptable risk threshold is functional to estimate the level and extent of application of safeguards and risk mitigating measures described in the following paragraphs.

A.2 Communication and interfaces

A.2.1 Communications and system interfaces to onboard IT and OT systems, including communications methods originating from company or affiliated organization shore side locations, should support the establishment of policies and procedures on cyber risk management.

A.2.2 Clear guidelines identifying who has permission to access, when they can access, and what they can access through shipboard communication and networking paths should be developed.

A.3 Network

A.3.1 Equipment Standards

This Para of subsection intentionally left blank as published recommendations do not address any operational aspects for this clause.

A.3.2 Design

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects for this clause.

A.3.3 Installation

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.3.4 Control, Monitoring & Alarm

A.3.4.1 Network Access control system

No. 166 (cont)

Policies and procedures should be developed towards control of network access. There are three key aspects associated with access control:

1) Account administration;

2) Authentication;

3) Authorization.

A.3.5 Segregation and segmentation of network.

This para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.3.6 Network protection safeguards

1) Bring-your-own-device (BYOD) management policy

2) Data backup procedures

3) Network configuration change and patch management

4) Use of certified approved and/or appropriate products suitable for their intended operational environment

A.3.7 Cyber incident detection safeguards

1) Event log auditing tools and procedures

2) Periodic vulnerability scans, security audits

3) Collection of all the events detected by the above listed systems, procedures

4) Roles and procedures for security event monitoring

A.3.8 Network and System recovery measures

A.3.8.1 Network and system recovery measures

1) Development of a service recovery plan and procedures

2) Assignment of roles and responsibilities

3) Training of personnel on a cyber incident recovery plan

4) Information backup policy and restore procedures

5) Timely communication and information to responsible personnel

6) Recovery plan drill

A.3.8.2 The System Integrator and Supplier should provide a document containing a description of the above-mentioned measures and instructions on how to verify their effective implementation, or a rationale for those not implemented. A copy of this document and of the

No. 166 (cont)

documents mentioned in the points above should be given to the Owner upon delivery and made available to the Classification Society upon request.

A.3.9 Protection Devices

This para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.3.10 Integration

This para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.3.11 Cyber Incident Response measure.

1) Development of a response plan in case of breach, including measures for confining the breach to the minimum extension

2) Procedures for a timely acknowledgment and management of incident alerts, including incident for reporting

3) Assignment of roles and responsibilities

4) Continuous training of personnel

5) Periodic cyber incident drills

6) Preservation of logs and any elements related to cyber incidents (e.g. digital forensics)

7) Continuous improvement of response plan

A.4 Computer based systems physical Access control

A.4.1 Installation

A.4.1.1 Secure Areas

The ship owner (the term "ship owner" should be read as "shipbuilder" hereinafter while the vessel is under construction) should establish policies and procedures for control of accessing areas where computer based systems are installed according to a risk assessment. Clear guidelines should identify who has permission to access, when they can access, and what they can access. Risks should be assessed taking into account the possible impact of unauthorized or unintended access to areas containing computer based systems.

It is recommended to Define 5 levels of access; every ship should have procedures in place which ensure that only authorized people can access each of these levels:

1. Access to the ship

2. Access to the control stations (e.g. bridge, engine control room, cargo control room, etc.)

3. Access to equipment MMI

No. 166 (cont)

4. Access to electric components or category II and III systems (processors, gateways, firewalls, plugs)

5. Access to data ports (USB, Ethernet and others)

A.4.2 Physical security perimeter

A.4.2.1 The ship-owner should define security perimeters to protect areas that contain computer based systems for category II and III. The location and strength of each perimeter should depend on the result of risk assessment.

A.4.2.2 Physical entry controls

Secure areas should be protected by appropriate entry controls as laid down in ship security plan.

A.4.3 Measures to restrict physical access to secure areas

The ship owner should establish methods supervising all work in secure areas to prevent an event of malicious activities.

A.4.4 Equipment

A.4.4.1 Equipment maintenance

Equipment should be correctly maintained to ensure its continuous availability.

1) Equipment should be maintained in accordance with the supplier's recommended maintenance program.

2) Only authorized person should be permitted to carry out the maintenance. When maintenance is carried out by external person (other than authorised service provider), the capability and credentials of the person and company should be verified prior to the maintenance. The ship owner should establish procedures towards the same.

A.4.4.2 Removal of equipment

Equipment should not be taken off from installations in vessels without prior authorization. Ship owner should identify the responsible persons who have authority to permit off-site removal of equipment (including component of equipment). Equipment should be recorded as being removed off-site with time limit and recorded when returned.

To prevent data loss associated with disposal of equipment, data should be encrypted. Self-Encryption Disks (SED) are recommended.

A.4.5 Cabling

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.4.6 Use of mobile devices and portable storage devices

When using mobile devices or portable storage devices, the following special care should be taken to ensure that equipment is protected.

No. 166 (cont)

1) Any device or portable storage device used in maintenance or updating of computer based system should be proven to have been malware scanned as per predefined interval prior to use. Computer and other devices should have up to date patches applied.

2) When portable storage devices are used for software maintenance, the devices should be authorized by responsible person prior to use.

A.4.7 Cyber-enabled equipment to restrict physical access

The owner of the company operating the ship should develop and implement procedures to restrict access to equipment.

1) If the equipment has password control, then it should be changed from default password and should follow password policy set by the company.

2) Recorded data of physical security equipment (cyber-enabled equipment to restrict physical access) should be securely maintained and monitored by the ship owner.

A.5 Software assurance

A.5.1 Design and Development

A.5.1.1 Software Assurance is an ongoing process and goes beyond development, installation and testing as per relevant Classifications rules and standards. The software should be maintained during a ship life cycle and requires a systematic approach.

A.5.1.2 Various stakeholders are involved in the software maintenance process with each stakeholder having a specific role rile. The industry standard on “software maintenance of shipboard equipment” details the roles of stakeholders. The present section elaborates on the activities recommended in initiation and planning of software maintenance. Software testing is covered in Section 8.

A.5.1.3 In case a classification society is involved in software maintenance computer based system of category II and III, the relevant ISO standard should be followed.

A.5.2 Software maintenance

A.5.2.1 Initiation of software maintenance can be made by the data provider, the producers or the ship owner. The initiator has the responsibility to inform other stakeholders when the maintenance event starts and the type of maintenance.

A.5.2.2 The ship-owner, data provider or the producer of software developed and installed as per as per IACS UR E22, should inform the classification society of software maintenance relevant to class related services.

A.5.2.3 Documentation as per IACS UR E22 should be submitted prior to the execution of maintenance for consideration by an individual classification society.

A.5.2.4 A classification society responsible for testing systems before and/or after the execution of the software maintenance should approve the functionalities of the systems.

A.5.2.5 The software maintenance shall be properly planned before it is executed in order to optimize its arrangements and to achieve the best possible outcome. Close communication between all relevant stakeholders shall be ensured.

No. 166 (cont)

A.5.2.6 Intra-system integration testing shall be done between system and sub-system software modules before being integrated on board.

A.5.2.7 For Category II and III systems test programs and procedures for functional tests and failure tests shall be done in accordance with the requirements in IACS UR E22.

A.5.2.8 The society should ensure that the software producer assesses each software update to determine and describe new functionalities, changes and improvements.

A5.2.9 Stakeholders quality systems

1) Data provider

Data provider should carry out data production and distribution operations in accordance with a quality system, covering:

a) Data quality (production, delivery, testing and integration);

b) Standardization of data import;

c) Means to ensure the continuous availability of data maintenances;

d) Prevention/detection/protection from unauthorized modification;

e) Prevention of the distribution of malware.

2) Service Provider

Service Provider should carry out maintenance-related operations in accordance with a quality system, covering:

a) Competence management;

b) Coordination and call-entrance procedures;

c) Remote maintenance procedures (if applicable);

d) Reporting procedures;

e) Shipboard operations safety briefing;

f) Cyber-security.

3) Ship-owner

a) The Ship-owner should ensure that software maintenances are carried out in accordance with an appropriate International Safety Management (ISM) Code system and operational procedures. If the software maintenance is relevant to class related services, the Ship-owner should inform the Classification society before the operation of the software maintenance is carried out.

b) The Ship-owner should have procedures in place in order that software is kept up to date with the requirements of the Producer of software, System Integrator, or Data Provider.

No. 166 (cont)

c) The Shipowner should maintain on board a software log listing the current and previous software versions installed on shipboard equipment.

d) The Ship-owner should have procedures in place to protect shipboard equipment from malicious or unintentional security threats. Safety procedures should include, but not limited to, the following considerations:

i. Ensuring secure communications and remote access;

ii. Access management for technician(s) from Service Provider

iii. Confirmation from the Service Provider that any portable computers, removable media/storage devices intended to be used in the maintenance process have been subject to a malware check before the maintenance is carried out.

e) The Ship owner should record each software maintenance activity performed on computer based system in the on board software log and link it to the associated electronic service report provided by the Service Provider. Such recordings may be made available on request by the Service Provider in support of future software maintenance.

f) Following maintenance, if the Producer of software, Provider or System Integrator has confirmed that new functionalities, changes or improvements have been implemented, the Ship-owner should ensure that crew familiarization with the upgraded system is carried out.

A.5.2.10 Failure recovery

1) The process of software rollback recovery should be made available prior to any software maintenances by Service Provider.

2) The intent of the rollback process is to return the failed state of the system to a previous known stable state.

3) The process should consider the implications and any associated risks that could result from the rollback and identify appropriate testing performed post roll back in order to demonstrate the administration and class of satisfactory working condition of the system.

4) Proposals for alternative solutions should be presented to the classification society.

A.5.2.11 Validating updates when carried out from remote location

The following consideration should be included in the procedure for validating updates:

1) Remote update should only be carried out by authorised personnel;

2) Update signatures ensure the integrity and authenticity of the update;

3) Update data transfer protection (encryption or cyclic redundancy check - CRC) to prevent exposure of software image;

4) Update data decryption or CRC;

No. 166 (cont)

5) Malware scanning;

6) Update data validation ensures update integrity;

7) Post-update verification ensures that the system is performing appropriately.

Rollback strategy should be determined prior to updating process and previous versions of software should be stored and available to be installed in emergency situations. The system should have the ability to revert simply to earlier revisions in the case of corruption.

A.6 Remote Access

A.6.1 Ship to shore interface

A.6.1.1 The ship-owner should establish policies and procedures for control of remote access to onboard IT and OT systems. Clear guidelines should identify who has permission to access, when they can access, and what they can access. Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel.

Remote access must be strictly controlled and only provided to suppliers or third parties after an information security assessment has been satisfactory completed by the supplier/third party. If possible, remote access should be initiated and confirmed by a responsible person onboard, and it should be possible at all times to terminate the remote connection by the responsible personnel onboard.

All remote access events should be recorded for review in case of a disruption to an IT or OT system. Systems should be clearly defined, monitored and reviewed periodically.

The procedures for activities on board should include steps to:

1) Document allowed methods of remote access to the information system;

2) Establish usage restrictions and implementation guidance for each allowed remote access method;

3) Monitor unauthorized remote access to the information system;

4) Authorize remote access to the information system prior to connection;

5) Enforce controls for remote connections to the information system.

A.6.1.1 The system integrator, producers and service providers should have cyber security company policy, which includes training and governance procedures for IT and OT onboard systems.

A.6.1.2 The Company should implement appropriate procedures for managing remote access / update.

A.6.1.3 The ship-owner should include in contracts with system integrator, producers and service providers clauses to requiring evidence of their internal governance for cyber network security.

No. 166 (cont)

A.6.2 Configuration of network devices

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.6.3 Remote maintenance

A.6.3.1 Clear procedures and protective measures shall be implemented to regulate this type of operations.

A.6.3.2 Where remote maintenance is used, access monitoring and control must be reinforced.

A.6.3.3 A maintenance plan should be developed by the Owner, and made available to all stakeholders involved. Where remote software maintenance is allowed, the procedures specified in section 7 on software maintenance should be followed,

A.6.3.4 Software update versions should be stored and following records should be logged:

1) versions that are in use,

2) versions that were in use

3) Versions those are stored.

A.7 Data Quality

A.7.1 Data Security

Data quality has many stakeholders and each stake holder has a level of responsibility which needs to be assigned based on impact and appropriate risk assessment due to potential break in Data security:

1) Computer based system manufacturer/provider ("Supplier", according to UR E22 2.1.3)

2) Computer based system component manufacturer/provider ("Supplier", according to UR E22 2.1.3),

3) System Integrator/Shipyard ("System Integrator" according to UR E22 2.1.2),

4) Ship Owner / Ship Master ("Owner" according to UR E22 2.1.1)

A.7.1.1 The responsibilities of various stakeholders should be defined.

A.7.1.2 As part of Cyber Risk Management, the Owner should also provide appropriate training on risks related to data security to the personnel authorized to interact with computer based systems covered by this recommendation

A.7.1.3 In general where the system has the capability for direct user interaction appropriate authorization and authentication along with diagnostics and logging should be in place.

A.7.1.4 The data securing methodology should be fit for purpose using technology currently available for the industry practice.

No. 166 (cont)

A.7.2 Data Categorisation

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.7.3 Secured and encrypted data

A.7.3.1 As part of Cyber Risk Management, the Owner should also provide appropriate training on risks related to data security to the personnel authorized to interact with computer based systems covered by this recommendation.

A.7.3.2 In general where the system has the capability for direct user interaction appropriate authorization and authentication along with diagnostics and logging should be in place.

A.7.3.3 The data securing methodology should be fit for purpose using technology currently available for the industry practice.

A.7.4 Data storage

Physical devices brought on-board the vessel for the purpose of the updating or upgrading Category I, II or III systems should be free from corruption. There should be a process in place to verify the data integrity before introduction to the ship's systems.

A.8 System Recovery

A.8.1 Manual Backup

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.8.2 Design recommendations for machinery systems

This Para of subsection intentionally left blank as published recommendation do not address any operational aspects.

A.8.3 Contingency Plan

A.8.3.1 The ship-owner has overall responsibility of developing the contingency plan based on essential information which should be provided by the associated system integrators and suppliers to enable effective contingency planning. The Contingency Plan should contain a set of predetermined instructions or procedures for crew to detect respond and limit consequences of cyber incidents in a timely manner, and for how crew will recover the affected systems after securing the ship’s safety by suitable response actions. In this context, the following response process in the event of a cyber incident should be considered.

1) Detect a cyber incident and identify the failed system;

2) Determine effective response options and take appropriate actions;

3) Recover the failed system;

4) Investigate and document the cyber incident;

5) Evaluate the effectiveness of response options and update the contingency plan.

No. 166 (cont)

A.8.3.2 The consideration of the full scope of a vessel's contingency plan will extend beyond the scope of class to include management systems and crew training. In the context of this recommendation, the use of the term 'contingency plan' is intended to capture the design, installation and documentation provided in order that the management systems and crew are provided with the facilities and information needed to support their response actions in the event of a cyber incident. The basis of the contingency plan and description of the documentation to be handed over on delivery of the vessel should be reviewed by the classification society at the initial stage.

A.8.3.3 The Contingency Plan should include the following information as a minimum:

1) List of computer based systems covered by the Contingency Plan;

2) System configuration and descriptions for systems covered by the Contingency Plan;

3) Incident response plan;

4) Recovery plan;

5) Periodic testing plan;

6) Maintenance procedure for the Contingency Plan.

A.8.3.4 During the preparation of the contingency plan, input should be obtained from the various stakeholders including ship operators, system integrator, system support vendors and IT/OT engineers.

A.8.3.5 When a cyber incident failure condition on computer based system on board is discovered, it is important that all relevant personnel are aware of the correct procedure to follow. It is vital that contingency plans, and related information, are available in a form which cannot be rendered ineffective by an onboard incident. A hard copy or an electronic device which is independent of the vessel's networks could be considered acceptable.

A.8.3.6 The contingency plan should be formatted to provide quick and clear directions in the failure event for use of onboard personnel unfamiliar with the plan or the system. A concise and well formatted plan reduces the likelihood of creating an overly complex or confusing plan.

A.8.3.7 Developing the Contingency Plan

At the initial stage of developing a contingency plan, it is very important to identify and to include all computer based systems on board. The provision of application scope of contingency plan among all computer based systems on board should be clearly defined based on their effects in a failure situation. At a minimum, all Category III systems according to UR E22 should be included in the plan. Category II systems should be also reviewed, if specific provision for contingency needs to be available, such systems should be included in the plan.

A.8.3.8 Incident Response Plan (IRP)

An incident response plan should contain a predetermined set of instructions or procedures to detect, respond to, and limit consequences of cyber incidents of computer based systems required for essential services according to UI SC 134.

No. 166 (cont)

A quick assessment of a cyber incident should be performed to evaluate the consequence and the options to respond. To assist crew to quickly find effective response option and take timely action quickly an incident response plan for the identified systems should be developed in clear, concise, and easy format which can be implemented in the event of a failure.

The incident response plan should, as a minimum, include the following information:

1) System for response and breakpoints

2) Alarm indication or abnormal symptom caused by a cyber incident;

3) Failure consequence;

4) Effective response options which do not rely on either shut down or transfer to independent or local control, if any.

5) Independent and local control should be capable of operating independently from the system that failed due to the cyber incident

Note: the example template in Appendix A may be used for developing Incident Response Plan.

A.8.3.9 Recovery Plan (RP)

Recovery plans should be easily understandable by the internal personnel and potential 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 should be available.

When developing recovery plans, it is important to specify the recovery objectives for the various systems and subsystems involved. There are two distinct types of objectives as below:

1) System recovery: it involves the recovery of communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.

2) Data recovery: it involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential cyber incidents should be created and the recovery procedure developed and described. Recovery plans may be supported through access to the following information;

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

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

No. 166 (cont)

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

End of Document