No. 159 Network security of onboard computer based systems

(Sep 2018)

1. Introduction

1.1. General

Network security of onboard computer-based systems consists in taking physical, organizational, procedural and technical measures to make the network infrastructure connecting Information Technology (IT) and/or Operational Technology (OT) systems resilient to unauthorized access, misuse, malfunction, modification, destruction or improper disclosure, thereby ensuring that such systems perform their intended functions within a secure environment.

1.2. Objective

This recommendation is intended to:

a) Provide a minimum set of recommended measures for the resilience of networks and networked systems onboard against cyber-related risks, vulnerabilities and threats, including awareness of operators about cybersecurity threats and procedures to prevent and react to cyber incidents.

b) Provide appropriate levels of implementation of such measures, according to a risk-based approach where the type of ship, its operation, navigation, cargo, etc., as well as the extent to which IT and OT networks are used on board, their complexity and the type of onboard systems they apply to are taken into account.

1.3. Scope

This recommendation is relevant to computer networks, connecting computer based systems onboard for -IT and OT systems, which are vulnerable to potential cyber events that could lead to dangerous situations for the safety of human life, vessel or cargo, or threat to the environment, or compromise the confidentiality, integrity and/or availability of information managed in such networks.

The provisions contained herein are relevant to networks connecting Cat. I, II and III systems according to the definition in UR E22, however, the extent and level of application should be proportional to the category of systems connected, considering the highest category as leading.

The extent and level of application may also be affected by 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. (see also chapter 3)

This recommendation is intended for new ships and may be applied to ships in service.

1.4. Exclusion

Items subject to statutory regulations, such as navigation systems required by SOLAS Chapter V, Radio-communication systems required by SOLAS Chapter IV, bridge systems and vessel loading instrument/stability computer are not considered as subject to the provisions contained in this recommendation (see also UR E22).

No. 159 (Cont**)**

Nonetheless, when the aforementioned systems are integrated with or connected to systems under the scope of Class, measures should be provided in order to prevent or reduce as much as possible the propagation of possible effects of adverse cyber events to and from such systems.

1.5. Types of onboard networks

Networks on board ships can be categorized according to many different properties:

a) Extension (local, ship-to-shore within the company, ship-to-shore with other companies, connected to public networks…),
b) technology (fieldbus, Ethernet, WiFi, mobile, short-range wireless…),
c) supported protocols (fieldbus protocols, IP, TCP, UDP…),
d) type of service (supporting IT or OT systems),
e) category of systems connected (Cat. I, II or III systems – see UR E22),
f) accessibility (restricted, controlled, public…),
g) and others.

Each network type has specific properties and can be affected by specific vulnerabilities; it can be subject to specific threats and, if compromised, its failure can lead to consequences that have different impacts on safety and/or security.

1.6. Network vulnerabilities and threats

Network vulnerabilities can be related to:

a) Access to and use of the information generated, archived or transported in the network;
b) Quality of the communication service implemented by means of the network.

Threats are targeted to the exploitation of vulnerabilities and may come from many different possible sources. Potential threat actors include: nation states; terrorists; cyber criminals; organized crime, competitors; activist groups; careless, disgruntled or malicious insiders; cyber vandals; opportunists and others.

Purposes and interests are different for each possible threat actor; likewise, their offensive capability and the probability of an attack, either intentional or accidental, are not the same and may depend on the ship type, operation, navigation, cargo, etc.

1.7. Responsibilities

The provisions of this Recommendation should be applied under the responsibility of the System Integrators, Suppliers, and/or Owner according to the specific phase of their implementation. Responsibilities of various stakeholders are detailed in the following paragraphs.

2. References

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

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

[2] ISO/IEC 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements”, 2013

[3] NIST “Framework for Improving Critical Infrastructure Cybersecurity”, version 1.1, 2017

No. 159 (Cont)

[4] "The Guidelines on Cyber Security On board Ships", version 2.0, BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI, 2017

[5] "The CIS Critical Security Controls for Effective Cyber Defense", version 6.0, Center of Internet Security, October 2015

[6] ISO/IEC 27033-1:2015, "Information technology, Security techniques – Network security – Part 1: Overview and concepts", 2015

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

3. Risk assessment

Under System Integrator and Supplier responsibility and supervision, a preliminary risk assessment should be carried out. Risks should be evaluated taking into account:

a) The possible impact of unauthorized access, misuse, modification, destruction or improper disclosure of the information managed in each network onboard.
b) The possible impact of degradation of data flow or complete loss of connection among network nodes.
c) 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.

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 that are likely to occur as a consequence thereof.

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.

4. Identification of key network resources and failure impact

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:

a) Networks on board
b) Network types according to criteria described in 1.5
c) Networked IT and OT systems and their category according to UR E22
d) Data flows and network devices or resources potentially limiting them
e) Connections with external systems or networks
f) Access points and interfaces, including machine-to-machine (M2M) interfaces
g) Roles and responsibilities of users
h) 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.

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.

The System Integrator should prepare a document including the above-mentioned items. This document could be part of, or an integration to an inventory of all of the vessel's computer

No. 159 (Cont**)**

based systems, and/or other documents, e.g. those describing the onboard network architecture. A copy of this/these document/s should be given to the Owner upon delivery, retained onboard and made available to the Classification Society upon request.

5. Network protection safeguards

The System Integrator and Suppliers should consider and implement the following safeguards aimed to prevent the occurrence of adverse cyber events on onboard networks. The level and extent of implementation should be in accordance with the criteria described in 1.3.

a) Management of identities and credentials of network users, including M2M networks
b) Enhanced authentication control, or restricted privileges, for remote access or from access points of the lower level of security
c) Physical access control to network access points
d) Pervasive implementation of Least Privilege Policy
e) Bring-your-own-device (BYOD) management policy
f) Encryption for data at rest (stored) and data in transit (exchanged)
g) Integrity checks for data at rest and data in transit
h) Separation of networks, firewalling, De-Militarized Zones (DMZs), etc.
i) 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
j) Event logging and Quality of Service (QoS)
k) Data backup procedures
l) Network configuration change and patch management
m) Use of certified approved and/or appropriate products suitable for their intended operational environment
n) Use of routing technology for ship to shore and ship to ship communication

The System Integrator and Supplier should prepare a document containing a description of the above-mentioned safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented. A copy of this document should be given to the Owner upon delivery, retained onboard and made available to the Classification Society upon request.

6. Cyber incident detection safeguards

The System Integrator and Suppliers should consider and implement the following safeguards for a timely identification of adverse cyber events on onboard networks. The level and extent of implementation should be in accordance with the criteria described in 1.3.

a) Intrusion Detection System (IDS) and Intrusion Protection System (IPS)
b) Connection quality monitoring tools
c) Event log auditing tools and procedures
d) Timely incident alert systems
e) Network Performance Monitoring System
f) Malicious code detection tools, e.g. antivirus, antimalware…
g) Periodic vulnerability scans, security audits
h) Collection of all the events detected by the above listed systems, tools and procedures - from a) to g) - with dedicated network facility
i) Displaying of security events, e.g. Security Information Event Monitoring (SIEM)
j) Roles and procedures about security event monitoring

The System Integrator and Supplier should prepare a document containing a description of the above-mentioned safeguards and instructions on how to verify their effective implementation,

No. 159 (Cont)

or a rationale for those not implemented. A copy of this document should be given to the Owner upon delivery, retained onboard and made available to the Classification Society upon request.

7. Cyber incident response measures

The System Integrator and Suppliers should consider and implement the following measures aimed to take appropriate actions regarding detected cybersecurity events on networks. The level and extent of implementation should be in accordance to the criteria described in 1.3.

a) Development of a response plan in case of breach, including measures for confining the breach to the minimum extension
b) Procedures for a timely acknowledgment and management of incident alerts
c) Assignment of roles and responsibilities
d) Continuous training of personnel
e) Periodic cyber incident drills
f) Preservation of logs and any elements related to cyber incidents (e.g. digital forensics)

The System Integrator and Supplier should prepare 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 documents mentioned in the points above should be given to the Owner upon delivery, retained onboard and made available to the Classification Society upon request.

8. Network and system recovery measures

The System Integrator and Suppliers should consider and implement the following measures aimed to restore network capabilities or service that has been impaired due to a cybersecurity event. The level and extent of implementation should be in accordance with the criteria described in 1.3.

a) Development of a service recovery plan and procedures
b) Assignment of roles and responsibilities
c) Training of personnel on a cyber incident recovery plan
d) Redundancy of data, network devices and communication media
e) Information backup policy and restore procedures
f) Timely communication and information to responsible personnel
g) Controlled shutdown, reset and restart of affected systems

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

9. Testing and assessment

Under the responsibility of System Integrator and Suppliers, for networks connecting systems of Cat. II and III, vulnerability assessment and test campaigns should be carried out in the operational configuration at least once before delivery, aimed at verifying the actual resilience of onboard networks to cyber incidents.

The System Integrator, in cooperation with the Suppliers, should prepare a test plan and execute the tests at least once before delivery in all the configurations and conditions specified in the test plan. Relevant results should be recorded in a test report. In case of significant identified breach or vulnerability, the System Integrator and Suppliers, possibly in cooperation

No. 159 (Cont)

with the executor of the tests or other experts, should identify, design and implement suitable countermeasures. Tests aimed to verify the effectiveness of such countermeasures should be executed and relevant results recorded in the test report.

For networks connecting systems of Cat. II and III, specific tests simulating selected single failures and/or exceptional conditions should be carried out at least once before delivery, aimed at verifying the effectiveness and efficiency of countermeasures as designed and implemented.

Specific tests should be carried out to verify the clear separation between networks connecting Cat. I systems, or other uncontrolled networks, and Cat. II / Cat III systems.

A copy of the test plan and test report should be given to the Owner upon delivery, retained by the Owner and made available to the Classification Society upon request. The Classification Society may request to witness the execution of tests and/or execute additional tests.

10. Change management

If changes are made to the network configuration, network components or other items identified as per paragraph 4:

- Details should be submitted by the Owner (for ships in service) or by the System Integrator (before delivery) to the Classification Society in advance.

- If deemed necessary by the Classification Society, a vulnerability assessment and/or test campaign may be required to be carried out on the new configuration.

- The Owner (for ships in service) or the System Integrator (before delivery) should update countermeasures and relevant documentation according to the changes made. A clear description of changes should be given and kept as documentation.

End of Document