No. 158 Physical Security of onboard computer based system

(Oct 2018)

1. Introduction

1.1 General

Physical security of computer based systems is comprised of administrative and technical measures to safeguard against unauthorized physical access, theft, damage or interruption. Due to progress of computer technology, onboard equipment becomes dependent on computer based systems, and often, integrated in common system. Such computer based system may be placed at easily accessible location in order to increase efficiency of ship operation by crews.

Various persons are engaged in computer based systems through installation in building a new ship, operation in service, maintenance work, repair, or replacement with new one, etc. To avoid unintended accessing to computer based systems by unauthorized person or device, measures should be taken during design, production, shop test, installation, onboard test and operation, and maintained during whole ship's life.

1.2 Objective

This recommendation is intended to provide recommended measures for prevention from unauthorized physical access, theft, damage or interruption to onboard computer based systems.

1.3 Scope

1.3.1 These procedures:

- are supplemental to IACS UR E22 "On Board Use and Application of Computer based systems" and apply to the use of computer based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements.

- apply also to systems not subject to classification requirements but which, when integrated with or connected to classed equipment or equipment with an impact on safety, can expose the vessel to cyber-risks and have an impact on the safe and secure operation of the ship.

- are applicable to vessels built after the introduction of the recommendation but may also be applied to ships already in service.

- may be applied to additional systems at the request of the owner.

1.3.2 Shipboard equipment and associated integrated systems to which these procedures apply can include, but are not limited to:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Ballast water control system;

No. 158 (Cont)

- Communication systems; and
- Safety systems.

1.4. References

MSC-FAL.1/Circ.3
NIST 800-53 Rev.4
ISO/IEC 27002 2013
IEC 62443-3-3 2013
The Guidelines on Cyber Security onboard Ships (Version 2.0: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)

2 Secure areas

The shipowner (the term "shipowner" 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.

2.1 Physical security perimeter

The shipowner should define security perimeters to protect areas that contain computer based systems. The location and strength of each perimeter should depend on the result of risk assessment.

Where possible computer based systems should be located in rooms that can normally be locked to prevent unauthorized access. If this is not possible then the equipment should be located in lockable cabinets or consoles.

2.2 Physical entry controls

Secure areas should be protected by appropriate entry controls as below to allow authorized person to enter.

a) The date and time of entry and leave of person should be recorded. Especially, visitors such as service engineer from the system integrator or supplier should be authenticated by identification card, etc., and only be granted access for authorized purposes.

b) Entry record of all access should be securely maintained and monitored by the shipowner.

2.3 Physical security measures for Secure areas

The shipowner should design and apply physical security measures for secure areas taking into account that key computers and network devices connecting to systems of Cat. II and III should be installed in secure areas to avoid access by outsiders.

2.4 Working in secure areas

The shipowner should supervise all working in secure areas to prevent an event of malicious activities. When secure area is vacant, it should be physically locked and monitored by surveillance camera or patrol, etc.

No. 158 (Cont)

3 Equipment

3.1 Equipment siting and protection

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

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

3.2 Supporting utilities for equipment

Supporting utilities such as electric power supply, telecommunications, air conditioning, and ventilation should be provided 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, if necessary.

3.3 Cabling

Cables for power supply or network communication should be protected from mechanical damage adequately.

3.4 Equipment maintenance

Equipment should be correctly maintained to ensure its continuity of availability.

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

b) When maintenance carried out by external person, the person and its work should be sufficiently cleared prior to the maintenance by shipowner. Only authorized person should be permitted to carry out the maintenance.

3.5 Removal of equipment

Equipment should not be taken off-site without prior authorization. Shipowner 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.

3.6 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.

a) Mobile devices (e.g. laptop computer, tablet PC, smartphone, etc.) including portable storage devices (e.g. USB drive, HDD, CD, DVD, etc.) should not be permitted to connect to any equipment unless specially authorized.

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

No. 158 (Cont)

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

3.7 Cyber-enabled physical security equipment

a) Physical security equipment (e.g. surveillance cameras, intrusion detectors, electronic locks, etc.) should have strong authentication method such as password, smart card, tokens, etc., to logging into it. If applying password, it should be changed from default, and kept non-trivial and updated regularly.

b) Physical security equipment should be regularly carried out a test to ensure that it is kept working in normal operating state.

c) Recorded data of physical security equipment should be securely maintained and monitored by the shipowner.

4 Segregation of network

4.1 General

Onboard networks should be divided into separate network zones based on network communication documents (See IACS Rec. No. 156 “Network Architecture”). 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 zone should be well defined.

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).

4.2 Physical segregation of network

Physical segregation of the network may be applied in terms of security or performance aspects. In this case a physically segregated network should present following characteristics:

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

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

- 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.

4.3 Logical segregation of network

Logical segregation of the network may be applied in terms of security or network maintenance aspects. In this case a logically segregated network should present following characteristics:

- No data communication between different network zones through network devices separating network zones.

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

End of Document