No. 162 Integration

(Sep 2018)

Contents

1. General.

2. References.

3. Application.

4. Documentation.

5. Recommendations.
5.1 General.
5.2. Segmentation.
5.3 Firewalls
5.4 Switches and protocols
5.5 Safety functions in the integrated network
5.6 Interfaces
5.7 Stand-alone security appliances
5.8 Anti-virus
5.9 Authentication
5.10 Unmanaged networks
5.11 Physical security and Network security
5.12 Testing

No. 162 (cont)

1 General

1.1 Integration refers to an organized combination of computer-based systems, which are interconnected in order to allow communication and cooperation between computer sub-systems e.g. monitoring, control, Vessel management, etc.

1.2 Integration of otherwise independent systems increases the possibility that the systems responsible for safety functions can be subject to cyber events including external cyber-attacks and failures caused by unintentionally introduced malware. Systems which are not directly responsible for safety, if not properly separated from essential systems or not properly secured and monitored in an integrated system, can introduce routes for intrusion or cause unintended damage of important systems. It is necessary to have a record and an understanding of the extent of integration of vessels' systems and for them to be arranged with sufficient redundancy and segregation as part of an overall strategy aimed at preventing the complete loss of Ship's essential functions.

2 References

- Class Societies Rules for Classification and Construction of Sea-going Ships
- ISO/IEC 27001:2014 Information technology – Security techniques – Information security management systems – Requirements
- The Guidelines on Cyber Security onboard Ships (Version 2.0: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)
- IEC 61158 - Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for IEC 61158 and IEC 61784 series
- IEC 61784 - Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions
- IEC 62443 - Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

3 Application

This Recommendation is intended for Vessels with interconnected Category II or III systems or where the interconnection of systems includes at least one Category II or III system.

UR E22 should be applied for each system individually and Category I systems that are interconnected to each other.

Note: For Vessels with systems without interconnections only UR E22 should be applied to each system individually.

4 Documentation

The following documentation should be developed by the System integrator and Supplier, and a copy should be given to the ship owner on delivery and made available to the Classification Society upon request:

1) Inventory list for computer based systems on board.

2) Networks list (with segmentation)

No. 162 (cont)

3) Network(s) topology/layout

4) Interconnections of networks – block diagram and list of interconnections

5) Update of virus database document – time of update and procedures of an update

6) Cyber risk assessment document (intrusion of malware, DDoS attack, etc.)

7) Test procedure (FAT procedure) – simulation of the operation of integrated systems including typical failures simulation (at the integrator workshop)

Note: after additional consideration by Classification Society this testing can be carried out onboard.

5 Recommendations

The system integrator or supplier, when integrating computer-based on-board systems to allow their communication and cooperation, should take into account the recommendations in 5.1 to 5.12 below.

5.1 General

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.

5.2 Segmentation

5.2.1 Segmentation of the network should be arranged and documented. Division according to IEC 62443-2-1 should be referred to as a guideline (high-security network architecture): Level 1 to Level 4 (segments).

5.2.2 For networks which include systems of Category II logical segmentation on VLANs (Virtual LAN) may be provided instead of physical segmentation.

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

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

5.2.5 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.

5.2.6 Encryption should be provided for networks which include systems of Category II or III. This encryption should be of the “end to end’’ type.

5.2.7 For networks which include systems of Category II or Category III systems recommendations in 5.3 to 5.12 should be applied.

No. 162 (cont)

5.3 Firewalls

5.3.1 Internal firewall should be applied between each network segment.

5.3.2 Perimeter Firewall between onboard network and external network should be applied. *See also item 5.7 below.*

5.3.3 Firewall between the onboard network and the internet should be duplicated and both should operate in real time. They should be arranged such that in case of failure of one of them the second will maintain the full security of the Ship's network.

5.3.4 Safety policy (rules) should be set on each firewall: setting should be provided to enable only essential or important data to be transferred between switches.

5.3.5 To prevent any unintended communication taking place, the firewall should be configured by default to deny all communication. Safety policy (Rules) should be implemented. The Safety policy (rules) should be designed to allow passage of data traffic that is essential for the intended operation of that network.

5.3.6 Firewall should be applied on each onboard computer used in Category II or Category III networks. For Category I networks connected to any Category II or Category III networks this requirement should be also fulfilled.

5.4 Switches and protocols

5.4.1 Network switches should be applied between each network segment.

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

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

5.3.4 Spanning Tree Protocol should be applied to network switches to prevent network storms and network becoming paralyzed.

5.5 Safety functions in the integrated network

5.5.1 Safety functions implemented in the integrated network should be implemented in dedicated and autonomous hardware units (switches, etc.).

5.5.2 Safety functions should be arranged with redundancy.

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

5.5.4 A single fault should not cause any function of the essential system in the integrated network to be unavailable.

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

No. 162 (cont)

5.6 Interfaces

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

5.7 Stand-alone security appliances

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

5.7.2 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.

5.7.3 Alarm from IPS should be generated at the relevant and identified manned station.

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

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

5.7.6 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.

5.7.7 Anti-spam filtering should be applied.

5.7.8 In case of any of a.m. prevention systems activation relevant information should be presented on master selected computer onboard. All incidents should be recorded/saved in software for later analyze by cyber-security Specialist (e.g. Ship Owner representative).

5.8 Anti-virus

5.8.1 Anti-virus software should be installed on each onboard computer or any programmable device having a standard operating system. For PLCs or other equipment without standard operating system, security measures should be applied in accordance with manufacturer recommendations.

5.8.2 Anti-virus should include the following prevention:
- anti-virus signature database;
- file pattern;
- file size;
- file type;
- grayware;
- heuristics;
- virus scan.

5.8.3 Means to identify the status of anti-virus database should be provided on each onboard computer (this is not intended to apply to computers installed onboard and not interconnected to any network).

5.8.4 Time of required updates and procedure of update of anti-virus software should be documented – see “Documentation’’ in item 4 above.

No. 162 (cont)

5.9 Authentication

Software changes in systems for Category II and III (modification of data by service) should be secured by two-factor authentication.

5.10 Unmanaged networks

Unmanaged (uncontrolled) networks (e.g. crew or passenger entertainment network) should not be connected to controlled networks (communication between uncontrolled networks and controlled networks is forbidden). The uncontrolled network is considered as unsafe. See also item 5.2.5.

5.11 Physical security and network security

Requirements for Physical security and Network security can be found in IACS Rec. No. 158 “Physical Security of onboard computer based systems” and IACS Rec. No. 159 “Network Security of onboard computer based systems”.

5.12 Testing

5.12.1 Most probable failures detection should be simulated (they should be listed in test procedure – see item 4 above).

5.12.2 Redundancy tests should be performed. See also item 5.5.

No. 162 (cont)

Appendix

Definitions

Switch – module that connects devices in the network, by using packet switching to receive, process and forward data to the destination device

Firewall – network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

VLAN – the network separated logically as part of another network

DLP (Data loss prevention) – technology that helps prevent the intentional or unintentional transfer of information to someone outside the network

IPS (Intrusion Prevention System) - a device that increases the security of networks by detecting or detecting and blocking attacks in real time.

Essential system – system applied on the Ship which operation provides essential services (as defined in UI SC134) for safety onboard and propulsion and steering in the normal running state (e.g. those ship's systems necessary for the propulsion and safety of the ship)

Network - a combination of equipment used in the system(s) – e.g. propulsion control system which uses switches, DPUs, PCs, etc.

DMZ (perimeter network) - physical or logical subnetwork that contains and exposes a Ship's external-facing services to an untrusted network, usually a larger network such as the Internet.

FAT – Factory acceptance tests

End of Document