
No. 161 Inventory List of computer based systems

161

(Sep 2018)

1. Introduction

1.1 General

The Inventory List of computer based systems includes a set of documents as mentioned in para 2 of this recommendation.

1.2 Objective

For effective assessment and control of the cyber systems on board, an inventory of all of the vessel's equipment and computer based systems should be created during the vessel's design and construction and updated during the life of the ship: tracking the software and hardware modifications inside ship computer based systems enables to check that new vulnerabilities and dependencies have not occurred or have been treated appropriately to mitigate the risk related to their possible exploitation.

1.3 Scope

This recommendation is relevant when OT falling within CAT I, II or III to new building ships and as far as possible to existing ships.
All computer based system installed on board the ship should be considered in the Inventory List.

1.4 Exclusion

Navigation systems required by SOLAS Chapter V, Radio-communication systems required by SOLAS Chapter IV, and vessel loading instrument/stability computer are not in the scope of this requirement.

This Recommendation is not applicable to loading instrument/stability computer.

Systems may be excluded from this list according to a risk assessment.

As a basic recommendation:

- systems not connected to category II or III systems and not being category II or III systems according to UR E22 might be excluded

2. Inventory List of computer based systems

An inventory list of all the vessel's computer based systems should be created during the vessel's design and construction and updated during the life of the ship. The inventory list shall contain:

- equipment list
- physical map of the computer based systems
- logical map of networks

2.1 Equipment List

Any computer based systems on board the vessel, excluding the equipment mentioned in section 1.4 should be included in the list.

2.2 Physical map of the computer based systems

The computer based systems mapping should be recorded. This may be graphically or tables etc. The mapping should be managed under a formal control management system, and kept secure.

2.2.1 Physical Inventories

The list of communicating devices should be included in inventory list or included in each supplier's drawings/documents, for example: PLCs, remote I/O, sensors, actuators, variable speed drives, meters, circuit breakers, switches, physical servers, desktops and storage units. For each element, the following should be specified:

- name;
- brand;
- model or reference (some devices (e.g. modular PLCs) contain several references);
- the version of the embedded firmware (software version) and the product version if appropriate;
- physical characteristics, if appropriate;
- physical location (Accommodation space/Engine room, room, cabinet, bay);
- list of switches connected;

The list of network communication devices should be included in inventory list or included in each supplier's drawings/documents, for example, switches, routers and protocol gateways. For each device, the following should be specified:

- name
- brand;
- model and reference;
- embedded firmware version;
- physical location (Accommodation space/Engine room, room, cabinet, bay).

For Ethernet switches, also the VLAN numbers for each port should be specified.

2.2.2 Diagram

This is a representation of the various geographical locations, showing:

- switches, associated VLAN numbers;
- links between devices;
- interconnection identifiers (MPLS, VPLS, ...);
- devices.

2.3 Logical map of networks

The logical topology of networks (e.g. IP and non-IP addressing scheme, subnet names, logical links, principal devices in operation) should be recorded. This map can be organized in the form of inventories and a diagram, and may be included in each supplier's drawings/documents.

**No.
161**

(Cont)

2.3.1 Logical Inventories**2.3.1.1 List of IP address ranges with, for each one:**

- the list of switches concerned;
- the functional description of the IP range;
- interconnections with other ranges.

2.3.1.2 List of non-IP networks with, for each network:

- the list of MAC addresses or addresses specific to the industrial protocols on the network;
- the list of switches concerned;
- functional description of the network;
- devices connected to other networks (connectors).

2.3.1.3 List of non-Ethernet access points with, for each one:

- the list of access ports;
- addressing, if there is a special protocol;
- the list of connected devices.

2.3.1.4 List of logical servers and desktops with, for each one, if applicable:

- IP addressing (network, mask, gateway);
- operating system version;
- underlying physical server;
- applications and their versions;
- services and versions.

2.3.1.5 List of connectors and communicating field devices (remote I/O, smart sensors, smart actuators, etc.) with, for each one:

- IP addressing (network, mask, gateway), the associated MAC addressing and network or the specific addressing, if appropriate;
- applications.

2.3.2 Diagram

This diagram is a representation of the IP ranges (networks and sub-networks) and their interconnections, showing:

- the functional description of the IP range;
- interconnections with other ranges;
- routers, switches and firewalls;
- IT security devices (e.g. filtering gateways, sensors, intrusion detection sensors).

In particular, this map should show interconnection points with "external" entities (e.g. partners, service providers) and all interconnections with the Internet.

**No.
161**

(Cont)

2.4.1 Software Inventories**2.4.1.1 List of desktop software structured per equipment:**

Desktop applications are software editors' applications used on the equipment. Desktop applications may be reserved to a local usage (e.g. notepad) but Desktop applications may also connect to remote computers (e.g. FTP client). But desktop applications cannot accept connections. Application using entering connections are called "Network Services" and are addressed in [2.4.1.2]. The following information is to be delivered regarding desktop applications:

- software name and publisher;
- installation date, version number and motivations;
- local and remote roles;
- generic accounts;
- dedicated accounts;
- access control list with read, write and execution rights;
- when existing, outgoing connections shall be considered (IP/Ports destination). If unknown, information shall be identified as "missing"
- license number.

2.4.1.2 List of network services structured per equipment:

Network services are application using entering connections through listening interface (e.g. called ports for TCP/IP) over the network or any serial connection. In addition to the list of information listed in [2.4.1.1] the following information is to be delivered.

For IP based Services:

- protocol name and version;
- listening ports and motivation.

For non-IP based Services:

- listening interface and motivation.

2.4.1.3 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.

2.4.1.4 Integration Documentation:

The latest editions of the documentation required to be provided to classification societies following integration testing for CAT II and III systems required by 3.1.3 of UR E22 is to be provided with the ship on delivery.

**No.
161**

(Cont)

3. Physical Support**3.1 Nature of the physical support**

The information required by this recommendation should be made available upon request in a paper document or a digital application. If the second option is chosen, a clear status of the ship configuration should be able to be determined at a fixed date on request.

3.2 Access to the physical support

Access to information required by this recommendation should be limited to the strictly necessary persons and organizations.

4. Responsibilities

The system integrator should be in charge of creating and updating the Inventory List, with the help of the suppliers and under the responsibility of the owner, at any moment of the ship life cycle. The system integrator may change during the ship life cycle. If no entity is assuming this role, the owner should be able to provide an updated Inventory List.

5. References

UR E22 (Rev. 2 June 2016)

MSC-FAL.1/Circ.3

NISTSP 800-53 (Rev.4)

ISO/IEC 27002:2013

ANSSI Cybersecurity for Industrial Control Systems – Detailed Measures Version 1.0 January 2014

Appendices**Appendix I - Definitions**

Communication Device: A computer based equipment, ensuring service or function for the ship, connected to the network, either receiving information and/or sending information. This includes an operating system based computers from operational and information systems as programmable logic controllers from industrial control systems.

Computer Based System: The system based on computer technology which may be comprised of hardware, software and the associated interfaces for input and output.

Local Area Network (LAN): A LAN is a network of connected devices that exist within a specific location.

Media Access Control (MAC): A media access control address of a device is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

MultiProtocol Label Switching (MPLS): MPLS is a type of data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name "multiprotocol"

Network Communication Device: A computer based equipment, ensuring service or function for the Communication Devices of the ship, who handles, manages and routes packets over the networks.

Virtual Local Area Network (VLAN): A VLAN is a custom network created from one or more existing LANs. It enables groups of devices from multiple networks (both wired and wireless) to be combined into a single logical network. The result is a virtual LAN that can be administered like a physical local area network.

Virtual Private LAN Service (VPLS): VPLS is a way to provide Ethernet-based multipoint to multipoint communication over IP or MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires.

**No.
161**
(Cont)**Appendix II - Stakeholders**

Owner: The Owner should be responsible for contracting the system integrator and/or suppliers to provide a hardware system including software according to the owner's specification. The Owner could be the Ship Builder Integrator (Builder or Shipyard) during initial construction. After vessel delivery, the asset owner may delegate some responsibilities to the vessel operating company.

System integrator: The role of system integrator should be taken by the yard before vessel delivery unless an alternative organization is specifically contracted/assigned this responsibility. The system integrator should be responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements specified herein and for providing the integrated system. The system integrator may also be responsible for the integration of systems in the vessel.

If there are multiple parties performing system integration at any one time a single party should be responsible for overall system integration and coordinating the integration activities. If there are multiple stages of integration different System Integrators may be responsible for specific stages of integration but a single party should be responsible for defining and coordinating all of the stages of integration.

The role of system integrator should be taken by the Owner after vessel delivery unless an alternative organization is specifically contracted/assigned

Supplier: The Supplier is any contracted or subcontracted provider of system components or software under the coordination of the System Integrator or Shipyard. The supplier should be responsible for providing programmable devices, sub-systems or systems to the system integrator. The supplier should provide a description of the software functionality that meets the Owner's specification, applicable international and national standards, and the requirements specified herein.

End of Document
