No. 156
(Sep 2018)

Network Architecture

Contents

1. Introduction

1.1 General

Ship control networks have evolved from simple stand-alone systems to integrated systems over the years and the demand for ship to shore remote connectivity for maintenance, remote monitoring is increasing.

Incorporation of Ethernet technology has resulted in a growing similarity between the once disconnected fieldbus and Internet technologies. This has given rise to new terms such as industrial control networking, which encompasses not only the functions and requirements of conventional fieldbus, but also the additional functions and requirements that Ethernet-based systems present.

1.2 Objective

The objective of the present recommendation is to develop broad guidelines on ship board network architecture. The recommendation broadly covers various aspects from design to installation phases which should be addressed by the Supplier, system integrator and yard.

Networks for Category II and III (as defined by IACS UR E22) systems and integrated systems should be resilient. The design should be such that in the event of a fault in one part of ship network due to failure of network devices or cyber incident, the remaining systems connected to unaffected network should be adequate 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 the safety of the vessel.

Suitable methods/arrangements should be considered during design phase to improve the network resilience. Towards above, network segregation and definition of appropriate levels of privileges, need careful consideration during conceptual phase.

2. Scope

The recommendations may be applied to ship's network systems using digital communication including ship to shore gateway, where provided. The scope includes both information technology (IT) and operation technology (OT) networks. The recommendation does not apply to standalone navigation systems. However, where navigation systems and /or

Category I systems , IT systems are integrated with category II and III systems, then such systems should be included in the scope of the present recommendation.

For devices, which are connected to computer based systems through analog transmission, the monitoring, installation and safety requirements should be as per existing Classification rules as applicable to the particular system.

3. Documentation

3.1 Design Philosophy Document

The basic design philosophy of the system (All OT systems and IT systems as defined in Scope of this recommendation should be documented during conceptual phase in Design Philosophy Document (DPD). The DPD can be referred for any subsequent changes to confirm that the intent of the original design philosophy is maintained or not compromised, due to new changes. (The changes may also arise due to modifications carried to address field problems or technology changes).

3.1.1 Following information should be documented in DPD

a) Purpose of the integrated system with brief description of functional recommendations;
b) Block diagram of the system clearly identifying various systems which can be controlled;
c) Type of Information exchange with external network to Control, monitoring, administrative functions;
d) Details of various hardware devices and software applications used in network;
e) Dependent systems which could be effected by changes in design philosophy.
f) Failure Mode Effect Analysis (FMEA) and vulnerability assessment for networks dedicated to essential services (as defined in UI SC134) in order to identify the need of redundancy and testing.

3.2. Network Communication Document

Network communication document should be used for specifying means of communication between various sub systems and various components of sub system.

The criterion for communication network design should be based on following:
- Reliability;
- Maintainability;
- Extensibility;
- Interoperability.

3.2.1 Following information should be documented in Network Communication Documents

a) Physical areas covered by the system (engine room, bridge, accommodation etc.);
b) Systems integrated (propulsion, steering, power, safety, navigation etc.);
c) Whether the integrated system is confined to single LAN or interconnected with more than one LAN or Connected to WAN;
d) Type of communication network topology: ex Series, Series star, Mesh etc.;
e) Network LAN technologies ex Ethernet, Fast Ethernet;
f) Connection media – twisted pair, coaxial, fibre optic etc.;
g) Details of Network communication software;
h) Communication from field controllers to field devices MODBUS, Fieldbus etc.;
i) Location of each network device;
j) Software configuration version control;

k) Simple network diagrams showing the major devices, nodes network cable details and general locations of the equipment, should be indicated.

4. Network architecture overview

A network generally may comprise of one or more of following components:

- Distributed control systems (DCS) and associated devices;
- Programmable Logic Controller (PLC) and associated devices;
- Routers, switches;
- HMI stations;
- Computers.

The list above is only indicative, the actual components or systems can vary with each installation according on the systems being controlled and or monitored.

4.1 Network categories

Ship network can be broadly categorized according to their basic functionality as ‘ship administrative network’ and’ ship control network’. Suitable network protection and detection systems, based on network criticality analysis should be provided for inter network communication.

4.1.1 Ship administrative Network

Ship administrative network would typically consist of computers intended for general administrative tasks including communication with shore offices. Where required, the network may provide a gateway to outside ship connectivity for remote monitoring and or maintenance. Typical examples could be IT systems used for reporting, scheduling, inventory management, capacity planning, operational and maintenance management, e-mail, phone, print services.

4.1.2 Ship Control Network

The ship control network could consist of individual and integrated systems. The control network may be logically further separated into layers or zones. Such division would be specific to an installation and factors which may need to be considered during logical division could be, extent of automation, redundancy and security requirements.

In many applications, the field devices are integrated with main controller using standard industrial protocols such as Fieldbus, Profibus etc. The main controller may be connected directly to field devices or through remote terminal units (RTU) using Ethernet connection. Typical systems could be main engine control system, valve control system etc.

An integrated network would consist of multiple systems of different process segments. In an integrated network, the data transfer requirements may vary from monitoring of connected systems to partial or full control of connected systems from control stations. Typical example could be vessel performance monitoring system, dynamic positioning systems, integrated bridge systems etc.

4.2 Network redundancy

Based on the risk analysis and the system philosophy, network should be designed for physical redundancy and to prevent simultaneous loss of both networks; it is recommended to install the redundant network cables as per Classification Society requirements. The requirement should be applied to systems as identified under scope.

5. Equipment standards

5.1 Network Cable

All Network cables for category I, II, III systems (as defined by IACS UR E 22) should be flame retardant and should be designed, manufactured and tested as per relevant National or International Standards. Cables should be fire resistant type where required by Classification Society.

5.2 Network devices

The network devices for Category II and III systems should be suitable for marine application and should be tested to requirements specified in IACS UR E10.

5.3 Wireless equipment

Wireless equipment should be designed and tested as per requirements specified in UR E10.

6. Data

The data sizing calculations considering following factors should be carried out to identify suitable network data throughput

- Data Speed requirement for particular application;
- Data format.

The data sizing calculations should be submitted for review on request.

The data categorisation, data classification, data format and data content should be as per acceptable international standards such as IEC 61162 or other equivalent standards.

7. Network Access Control, Monitoring and alarm

7.1 Access control system

Access control is the system for controlling who or what resources can be accessed and permissible type of access.

There are three key aspects associated with access control:
Account administration, authentication and authorization.

All three aspects should work together to establish a sound and secure access control strategy.

The access control system should provide the capability to protect the integrity of sessions and reject any usage of invalid session IDs.

7.2 Monitoring

The network devices for Category Ⅱ and Ⅲ systems should be able to detect the following states by performing self-diagnostics:

a) Link up of each port on the network device;
b) Link down of each port on the network device;

c) Power on or hardware reset;
d) Network storm detection;
e) Fan halt (only if the network device has a fan and a fan-stop detection function);
f) Abnormal temperature (only if the network device has an abnormal-temperature detection function.

7.3 Alarm function

The network-monitoring device for Category Ⅱ and Ⅲ should have a function to detect abnormal state changes and notify the user:

a) When a link is disconnected or the power is turned off for a network device or network terminal;
b) When a link not belonging to the network is connected or the power is turned on for a network device or network terminal;
c) Loss of a network device.

7.4 Wireless Communication

a) The access control system should provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication;
b) 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;
c) The access control system should provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.

7.5 Installation recommendations

The network devices (Hubs, routers, switches etc) should be installed in protective cases unless the ingress protection of the device meets the requirements of Classification Society. The protective cases should be designed for the ambient environment and ease of operation and maintenance of the device.

The installation of network devices should be as per Classification Society requirements.

The ventilation and temperature at device location should comply with device manufacturer recommendations.

7.6 Cabling

The minimum bending radius specified for the cable should not exceed, especially for optical cables where it may lead to signal loss. Cable installation including segregation from electromagnetic sources should be as per Classification society requirements.

7.6.1 Network segmentation

Network segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level. The zone may be an isolated standalone network segment or a network segment separated from the organization’s network by some sort of network barrier device.

Key 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 high risk control systems, 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. The security level for the DMZ is higher than a network with which has provision for internet connectivity. For new build ships in addition to separation of IT and OT networks, separations between CATOGERY I,II and III systems is recommended.

A DMZ eliminates or reduces all direct communication between the control zone and the other non-essential zones. Use of DMZ minimizes the number of people directly accessing critical ship control zone devices.

8. Testing

Network testing to verify the intended operation of network should be carried out after complete installation of network cables and devices.

8.1 Scope of testing

The scope of testing of the network system should be as follows:

a) All cabling and network devices making up the network system;
b) All functionality relating to network communication by nodes connected to the network system;
c) If the network system is connected to other networks, test the communication functionality with the connected network(s), and blocking of communication (packets) that should be blocked;
d) Network monitoring (administration) devices and functionality;
e) Network loading;
f) Network storm test.

8.2 Network device connection testing

The objective of the test is intended to verify operation and function of network device connections.

The network-monitoring devices and monitoring functions should operate normally in the network system, as follows:

a) Function to display physical architecture diagram;
b) Alarm function;
c) Logging function;
d) Traffic display function;
e) Setting configuration function;
f) Fault recovery support function.

Appendix I

Definitions

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

Control Networks: These are used for peer to peer connections between control systems such as SCADA/DCS/Analyzer/Safety PLC systems.

Critical systems
Cyber incident: Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Demilitarised zone: Common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones.

Fieldbus Networks: These are used to connect analog and smart field devices such as valve actuators, sensors and other field control systems.

HMI (Human Machine Interface): The operators interface to the concerned process /or machinery.

Integrated systems: A combination of computer based systems interconnected for communication between various sub systems for vessel control and monitoring.

Local area network (LAN): A network infrastructure that provides access to users and end devices in a small geographical area.

Network devices: Various components or equipment forming part of network. Examples: Computers, PLC, Switches, routers etc.

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

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.

Network Topology: The geometric arrangement of a computer system. The network topology can be of various types and should be designed as per system integrator or manufacturer rrecommendations. Examples of such topologies could be Ring, Star, Mesh, hybrid, and Tree.

Network: A network is defined as a group of two or more computer systems together.
There are many types of computer networks, including the following:
Campus-area networks (CANs): The computers are within a limited geographic area, such as a campus or military base.

Programmable device: Physical component where software is installed. (E22)

Protocols: A protocol defines a common set of rules and signals that computers on the network use to communicate.

Ship board Network Architecture: Comprises of network devices, cables to carry out data communication between various on board systems.

Software: Programs and operating instructions used in shipboard equipment, including firmware.

System Categories: (I, II, III) Those systems, failure of which (E22):
I. will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
II. could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
III. could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

System Integrator: The stakeholder, who is responsible for the integration of systems and products provided by the supplier. The responsibilities of the Integrator should be as indicated in UR E22.

Wide-area network (WAN): A network infrastructure that provides access to other networks over a wide geographical area.

End of Document