INTERNATIONAL STANDARD

ISO 16425

First edition
2013-02-01

Ships and marine technology — Guidelines for the installation of ship communication networks for shipboard equipment and systems

Navires et technologie maritime — Lignes directrices pour l'installation de réseaux de communication des navires pour les équipements et systèmes embarqués

Reference number
ISO 16425:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16425 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 6, *Navigation and ship operations*.

Introduction

This International Standard gives guidelines relating to such matters as the communication network-system architecture, data requirements, administration, operation, commissioning, inspection and testing.

This International Standard also takes into account differences between shipboard communication networks and networks that are used outside of ships, and stipulates requirements and the like in clauses relating to matters unique to shipboard use.

Until now, there have not been comprehensive guidelines for connecting devices provided by many different manufacturers to a network via generic means, and this has impeded the wider use of shipboard networks.

This International Standard will make it possible to provide guidelines for all aspects of communication network-system design, commissioning, inspection, testing and operation, and improve convenience to all involved parties, including manufacturers, engineering firms, shipbuilders, and shipping companies.

This communication network for shipboard equipment connects equipment and shares information gathered from shipboard equipment and systems via a network. This communication network is connected to the navigational equipment network and engine-control network via an appropriate gateway.

The independence of such a network is ensured by using a gateway.

This network is intended for information sharing and is not directly related to safety of navigation. Also, it is not a system targeted for classification rules.

Additionally, Annex A is attached to provide detailed examples of technical information that serve as guidelines for some difficulties caused when the information network system is designed.

NOTE Requirements for wireless communication systems, which serve as an effective method of onboard wireless communication, is specified in IEEE 802.11, and national laws are established based on the aforementioned IEEE in each country. Different frequency and output range are allotted by each country, and regulations exist for such frequencies and ranges in some countries. Given the circumstances, it is possible that wireless communication systems cannot be used when calling at a port. Therefore, wireless communication systems are outside the scope of this International Standard.

Ships and marine technology — Guidelines for the installation of ship communication networks for shipboard equipment and systems

1 Scope

This International Standard specifies installation guidelines for ship communication networks for improving communication for shipboard equipment and systems that are independent from navigational equipment networks and engine-control networks.

This International Standard utilizes existing standards relating to protocols, and provides new guidelines for such aspects as communication network-system architecture, administration, operation, and installation.

The new guidelines specifically include: redundancy if necessary for a shipboard communication network system; network administration that does not require experts; physical as well as logical security; and network installation.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61162-450, *Maritime navigation and radio communication equipment and systems — Digital interfaces — Part 450: Multiple talkers and multiple listeners — Ethernet interconnection*

IEEE 802.3, *Ethernet (Formerly: Carrier Sense Multiple Access with Collision Detection)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
network
communication network restricted in scope to a ship

3.2
XML
eXtensible Markup Language
meta language for sending and receiving data via a network that is recommended by the WWW Consortium

3.3
gateway
communication device that connects computer networks to networks with differing protocols

3.4
collision domain
domain in a computer network where simultaneous transmission will cause collisions or congestion

3.5
broadcast domain
domain on a computer network where broadcasted frames (broadcasts) are received

3.6
STP
spanning tree protocol
method of control in a loop topology network for preventing data from entering endless loops

3.7
IP
internet protocol
protocol for sending and receiving information via the Internet

3.8
OSI reference model
Open Systems Interconnection reference model
model that divides the communication functions stipulated for computers by the International Organization for Standardization into layers

3.9
SNMP
Simple Network Management Protocol
communication rules that define methods for communicating information in order to monitor and control network devices on network

3.10
ICMP
Internet Control Message Protocol
communication rules that are used for such purposes as notifications of errors in the processing of datagrams, and notifications of information relating to communication

3.11
MIB
Management Information Base
type of database for managing devices in a network

3.12
port trunk
method of raising transmission speed by governing two or more physical cables

3.13
VLAN
Virtual LAN
method for configuring a network virtually, regardless of the physical network configuration

4 Abbreviations

UTC	Universal Time, Coordinated
RSTP	Rapid Spanning Tree Protocol
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
QoS	Quality of service
RIP	Routing information protocol
OSPF	Open shortest path first
CD	Compact Disc
DVD	Digital Versatile Disc
ECR	Engine Control Room
BR	Bridge
RM	Room
GEN	General
E/R	Engine Room
C/R	Control Room
IGMP	Internet Group Management Protocol
ASCII	American Standard Code for Information Interchange
MAC	Media Access Control
VPN	Virtual Private Network
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
UTP	Unshield Twisted Pair

5 Network system architecture

5.1 Network system design

The design of this network system shall give due consideration to such matters as the compatibility of the various devices in the network as a whole, and data transmission (amount of information, latency, and routes). Consequently, a network-system designer should have a grasp of the overall system, comprehensive knowledge, and consideration for shipboard use.

When designing the network system, the effective data volume and network load factor should be pre-calculated when the network media are under maximum load. In addition, provision should be made for further network expansion and increase of the data traffic.

The design shall also foresee the various potential system states, including initial state, failure state, and normal state, in order to define which communication is to be granted in various failure scenarios.

The network diagrams shall be equipped on the vessel. When the network design is changed, the network-system designer shall retest the network and update the network diagrams.

As a data requirement, it is extremely vital to consider such factors and to prevent ship equipment connected to the network that does not send or receive data from being excessively impacted.

Data requirements are specified in 6.2 and 6.3.

5.1.1 Scope of network system architecture

This network system shall be designed specifically for ships, with the purpose of sharing information between shipboard devices. It shall be independent from navigational equipment networks and engine-control networks.

The scope of the network system's architecture is not limited to the bridge. It extends to all key locations on the ship.

The network shall not operate (control) the ship's navigational equipment, however it should allow monitoring of navigational equipment.

Figure 1 shows a sample network-architecture scope. The typical implementation of the contents provided in this International Standard is specified in Annex A.

NOTE The following are some examples of areas within the scope of the network-system architecture:

-Navigation Bridge / Control Centre;

-Captain's Office;

-Officer's Office;

-Officer's Mess;

-Captain's Cabin;

-Officer's Day Room;

-Engine Control Room;

-Engine Room;

-Cargo Control Room;

-Field / Cargo.

5.1.2 Network system separation

The network system shall be separated from other networks by an L3 switch so that it will not be adversely affected by failures on other networks. The routing and filtering rules should be configured appropriately on the L3 switch for traffic and security. For more advanced security, a firewall for the upper layer may be used.

5.1.3 Network division

The network shall be divided into sub-networks (the broadcast domains) depending on the types of information handled, in order to control traffic and ensure security. In order to ensure the security and the control of traffic, the network shall be logically segregated to form sub-networks, depending on the

type of information to be handled. Each network should be designed so that network soundness can be maintained at all times, including when failures occur on other sub-networks.

NOTE The following are some examples of sub-networks formed from the main network:

-Navigational data collection sub-network;

-Engine data collection sub-network;

-Shipboard telephone sub-network;

-Imaging sub-network;

-General shipboard document-review sub-network.

5.1.4 Traffic division

The network shall be built to minimize the collision domain (the scope of packet collisions), and appropriately divide the broadcast domain (the domain reached by broadcasts).

The bandwidth used by the core network shall be designed appropriately, and a logical network system shall be built in order to use the network bandwidth more efficiently.

In order to utilize the network's available bandwidth efficiently, the logical network shall use a virtual LAN (VLAN) architecture, which forms the network from a virtual group that does not depend on the type of physical connections.

During ordinary use, the target traffic on a sub-network should preferably be around 25 % when using half-duplex, and 50 % when using full-duplex communication.

5.1.5 Redundancy

The connections within the network system shall use a redundant architecture that guarantees that information will be transmitted without failure. A loop architecture should be used for connections between sub-networks, employing such architecture as a rapid spanning tree protocol (RSTP) that should act as a spanning tree to quickly route around connection failures.

Using separate routes from the vessel's port and starboard systems for the network's connection cabling is also an effective way to prevent simultaneous network-connection failures.

5.2 Network interface for shipboard equipment and systems

5.2.1 Interface

The network system shall use the IEEE 802.3 Ethernet standard that is most frequently used for computer networks: Carrier Sense Multiple Access/Collision Detection (CSMA/CD).

The network shall also use the standard communication network internet protocol defined by this International Standard.

5.2.2 Connected equipment

The devices to be connected to the network system shall be devices that need to share information onboard the vessel.

NOTE The following are examples of devices eligible for connection to the network:

-Ship's clocks;

-Sensor information network converters;

-Network-capable multipoint displays;

-Engine monitoring systems;

-Container monitoring systems;

-Vessel monitoring camera systems;

-Shipboard IP telephone systems;

-VDSL shipboard network systems.

5.3 Equipment constituting communication network system

5.3.1 Network devices

Clearly indicate the specifications for network devices (switches and routers) connected to each of the nodes.

5.3.1.1 Switches

A switch is a computer network device with the same functionality as a bridge or more in OSI reference model layer 2. It is also called a "layer 2 switch" (or "L2 switch").

Some models of switch have intelligent functions for network management. The following are examples of such intelligent functions:

— Rapid Spanning Tree Protocol (RSTP);

— Virtual Local Area Network (VLAN);

— Simple Network Management Protocol (SNMP).

5.3.1.2 Routers

A router is a communication device that connects different networks. It is responsible for OSI reference model layer 1 to layer 3 connections, and controls the transmission of IP packets between the various networks.

Protocol processing is implemented in software.

The basic functionality of a router is as follows:

— Filters IP headers and the like;

— Has quality of service (QoS) features, including prioritizing line capacity and throttling traffic;

— Manages routing information using route-information collection protocols routing information protocol (RIP) and open shortest path first (OSPF).

5.3.1.3 L3 switches

L3 switches mainly transfer data in OSI reference model layer 3. Their functionality is nearly equivalent to that of a router.

They should be faster than routers because they implement protocol processing in hardware.

5.3.2 Network cables

The cables used to connect devices shall be selected with consideration for communication speed and distance. Installation of shield cables (shield twisted pair cable, foil twisted pair cable, etc.) should be considered, depending on the installation environment.

Table 1 shows the standard for selecting standards of cables that connect devices, and the specifications for optical-fibre cables and metal cables used by the system. It is necessary to always pay attention to the latest standard.

Table 1 — Network cable standards

Protocol		Standard Protocol	Communication Speed	Cables Used	Range
10BASE-T		IEEE 802.3i	10 Mbps	UTP/Shield Twisted Pair cable: Cat3	100 m
10BASE-F	10BASE-FB	IEEE 802.3j		Multi mode optical fiber	2 000 m
	10BASE-FP				1 000 m
	10BASE-FL				2 000 m
100BASE-T	100BASE-TX	IEEE 802.3u	100 Mbps	UTP:Cat5	100 m
	100BASE-T4			UTP(4): Cat3	100 m
	100BASE-T2	IEEE 802.3y		UTP(2): Cat3	100 m
100BASE-F	100BASE-FX	IEEE 802.3u		Multi mode optical fiber	2 000 m
				Single mode optical fiber	20 km
1000BASE-T	1000BASE-T	IEEE 802.3ab	1000 Mbps	UTP(4): Cat5e	100 m
	1000BASE-TX	TIA-EIA/-854		UTP(4): Cat6	100 m
1000BASE-X	1000BASE-SX	IEEE 802.3z		Multi mode optical fiber	550 m
	1000BASE-LX			Multi mode optical fiber	550 m
				Single mode optical fiber	5 000 m
	1000BASE-CX			Coaxial cable(2)	25 m
10GBASE-T		IEEE 802.3an	10 GMbps	UTP(4):Cat6e	100 m
				UTP(4):Cat6a	100 m
				UTP(4):Cat7	100 m
10GBASE-R	10GBASE-SR	IEEE 802.3ae		Multi mode optical fiber	300 m
	10GBASE-LR			Single mode optical fiber	10 km
	10GBASE-ER			Single mode optical fiber	40 km

5.3.3 Relays

The relay devices used in shipboard communication networks are as follows:

— Using switch to divide collision domains;

— Using local routers and L3 switches to divide broadcast domains;

— Using gateway devices to connect to other networks;

NOTE A gateway in Figure 1 is an application gateway.

— Repeater HUB shall not be used as a data collision preventive measure.

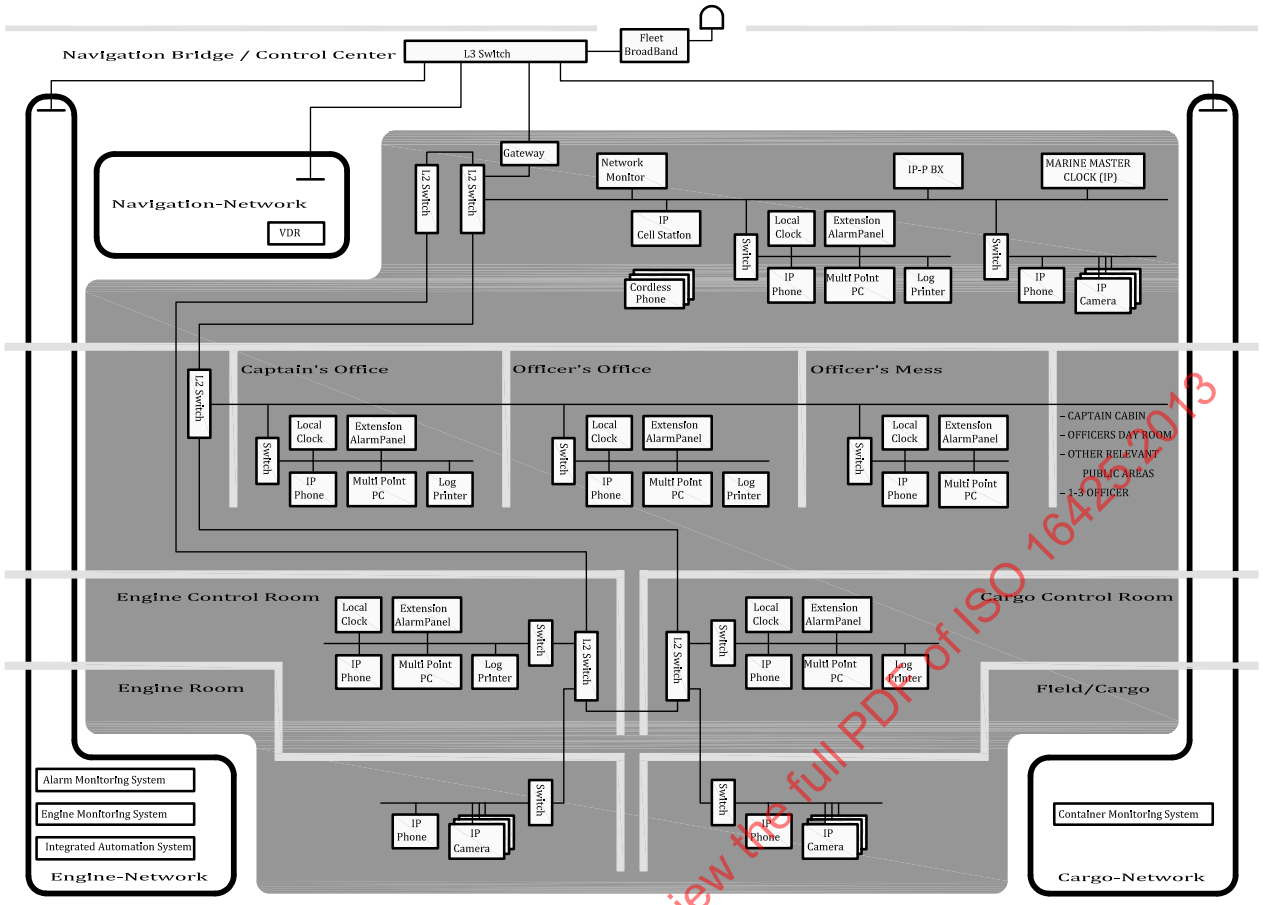


Figure 1 — Sample network architecture scope (Reference)

6 Data requirements

6.1 General

This clause specifies the data requirements that shall be implemented in the communication network system, but the system shall comply with this clause and any applicable international standards such as IEC 61162-450:2011.

6.2 Meaning of data and description of structure

Language shall be defined in order to specify the category, content, and structure of data prescribed by the data's attribute definition. By using a language that is currently used widely on the Internet many other computer applications become capable of increasing the convenience of developing device applications. This clause recommends the use of XML, a standard structure-description language that is easy for standard senders and receivers to parse and analyse the data structure. The use of a structure description language is expected to improve the convenience to the user, including ease of semantically analysing data, reusing data, and importing data into databases.

The data requirements specified in each data definition should preferably be determined after referring to 6.3 and 6.4.

NOTE Sample notations using XML for reference are as follows:

EXAMPLE 1 Sample notation for UTC time and date

Identifier	Meaning	Category	Year	Month	Day	Time
ZDA	UTC Time and Date	Analog	2009	10	15	20:10:19.95

< Navigation Data >

< *data_type* > UTC Time and Date < */data_type* >

< *identifier* > ZDA < */identifier* >

< *category* > Analog < */category* >

< *year* > 2009 < */year* >

< *month* > 10 < */month* >

< *day* > 15 < */day* >

< *time* > 201019.95 < */time* >

< /Navigation Data >

EXAMPLE 2 Sample notation for engine data measurement points

Channel No.	Channel Name	Cat.	Range Zero	Range Full	Range Unit	Low Alarm Value	High Alarm Value	Signal Type
0101	M/E T/C REVOLUTION	Analog	0	350	100min-1	–	135	4-20mA
0201	M/E FO INLET TEMP	Analog	0	200	°C	105	150	Pt100

< Engine Data >

< *measurement_point* >

< *channel_num* > 0101 < */channel_num* >

< *channel_name* > M/E T/C REVOLUTION < */channel_name* >

< *category* > Analog < */category* >

< *range_zero* > 0 < */range_zero* >

< *range_full* > 350 < */range_full* >

< *range_unit* > 100min-1 < */range_unit* >

< *low_alarm_value* > – < */low_alarm_value* >

< *high_alarm_value* > 135 < */high_alarm_value* >

< *signal_type* > 4-20mA < */signal_type* >

< */measurement_point* >

< *measurement_point* >

< channel_num > 0201 < /channel_num >

< *channel_name* > M/E FO INLET TEMP < */channel_name* >

< *category* > Analog < */category* >

< *range_zero* > 0 < */range_zero* >

< *range_full* > 200 < */range_full* >

< *range_unit* > °C < */range_unit* >

< *low_alarm_value* > 105 < */low_alarm_value* >

< *high_alarm_value* > 150 < */high_alarm_value* >

< *signal_type* > Pt100 < */signal_type* >

< */measurement_point* >

< /Engine Data >

6.3 Data attribute definitions

The attributes of data exchanged between senders and receivers over the network system shall be determined, and a summary of the defined information based on these set attributes should be disclosed to users. Consideration should be taken for information and specifications regarding equipment of the data senders and receivers when defining specific data attributes.

When defining data contents, user-friendliness, such as ease of semantically analysing data, shall be taken into account.

6.3.1 Data categories

Information for identifying data shall be defined when data are used between the sender's and receiver's devices.

6.3.1.1 Request/Information identifier

In order to distinguish the type of Request data and Information data, an identifier should be added to the attribute definitions.

a) Request data

Request data are data to request specific actions to other devices, or to request when using request/response as data-delivery format and procedures.

b) Information data

Information data are data to send the status or information of the sender's device for another device.

6.3.1.2 Classification information

Information to classify data shall be determined considering the data's meaning. The following are some example classifications: trend graph, bar graph, navigation, equipment alarms, etc.

6.3.1.3 Analog/On/Off signal identifier

If analog and On/Off signal information need to be distinguished, an identifier should be added to the attribute definitions that do so.

6.3.1.4 Equipment architecture information

Information shall be added for identifying nodes, considering equipment architecture information that identifies equipment communication nodes. Information for node address numbers, addresses, and device-specific types are the examples.

6.3.2 Data contents

In order to give the actual data values (e.g. engineering values or converted values), the name of the actual data value, the data being sent (analog or On/Off signal value), and the unit information (when using analog signal values) shall be defined.

6.3.2.1 Data name

The data name should preferably be any identifier that is easy for people to understand considering the meaning of the data being sent. The sender and receiver shall have identical interpretations of identifiers, because it enables the receiver to identify the data's value.

6.3.2.2 Values for data names

Actual values for data names shall be given. For analog signal data, the actual value will be determined by the specifications for the data stored on the device, including the notation (e.g. decimal or hexadecimal) and the handling of decimals. Although binary notation is generally used for On/Off signal values, the value shall be defined, including the significance of "0" and "1".

6.3.2.3 Unit information

If the data name is for an analog signal value, then unit information may also be assigned. The MKSA unit system should be used for unit information. It should be noted that unit systems other than MKSA are also used on shipboard systems. Therefore the unit system to use between the sender and receiver shall be determined in advance.

6.3.3 Data size

The data size (number of records) shall include information about the number of records in the data repeatedly delivered by the sender. If the number of records becomes extremely large, a large amount of data will be sent over the network. Therefore the maximum number of records should be ascertained. By adding the information about the number of records beforehand in order to explicitly state the amount of data, the identification of the data size will be facilitated.

6.3.4 Data encoding format

There are two main types of data encoding: ASCII and binary. ASCII features the strength of being easily understandable by humans, while having the weakness of increasing the amount of data to be sent. Binary data are hard for humans to understand, while having the advantage of reducing the amount of data to be sent. The format shall be determined with consideration for the data size in 6.3.3.

6.3.5 Use of data encryption

Data are sometimes sent in encrypted form in order to increase the confidentiality of the data. If the data are encrypted, both the sender and receiver shall be equipped with encryption and decryption algorithms.

6.4 Data delivery format

The data requirements for the network system shall take the following requirements into account.

6.4.1 Data delivery method and procedure

The method and procedure for delivering data are determined in accordance with the equipment specifications. The communication protocol shall be determined in accordance with the status between each device; for example, if a device stops processing when being turned off or reset, or if communication is conducted between devices continually.

The data-delivery format and procedures shall include one-way transmission (one-way stream), and request/response.

6.4.2 Data delivery format

The method of delivering the data that has the attributes determined in 6.3 shall be taken into account. The most common data-delivery formats for Ethernet are unicasting, broadcasting, and multicasting. Each format has its own strengths and weaknesses, and shall be selected in accordance with the purpose of the inter-device data communication. The delivery format shall be selected with consideration for such systems as the connected devices, delivery formats, and other elements as a whole, because the data-delivery format will influence the network load on other devices.

6.4.3 Data notification format

There are two main data-notification formats: event notifications, which are sent when an event occurs that the sender should send; and periodic communication, which sends data at regular intervals.

6.4.3.1 Event notifications

Event notifications have the advantage of reducing the amount of data to be sent, but should be dealt with caution, because the notification will not be made if the receiver fails to receive the data. Consideration is also required for the communication procedure when a receiver recovers from a state in which reception was not possible (e.g. powered off or malfunctioning).

6.4.3.2 Periodic notifications

Periodic notifications have a certainty of being capable of receiving data from other devices by waiting for a certain period of time. It has the disadvantage, however, of increasing the network load by sending large amounts of data periodically over the network. For this reason, data to be sent periodically shall be determined based on the level of demand for reliability in the sent data, and the network-load forecast. In particular, measures shall be taken to avoid flooding the network when sending initialization data to a large number of connected network terminals upon initialization.

In consideration of the data requirements in 6.2 and 6.3, the effective data volume and network load factor should be pre-calculated when the network media are under maximum load. The design should also preferably foresee the various potential system states, including initial state, failure state, and normal state, in order to operate normal data communications on the system in the worst-case scenario. It is also extremely vital to consider data requirements for equipment connected to the network that does not send or receive data from being excessively impacted.

7 Network administration requirements

7.1 Network administration requirements and definitions

Network administration is a mechanism for continually monitoring traffic and nodes, and enabling the crew to ascertain any anomalies.

The mechanism shall be so simple to handle that any crew may easily learn how to administer the network without being an expert.

7.2 Network administration scope

The scope of administration is the equipment's communication network only.

The following categories of network administration defined by the ISO OSI shall perform configuration management, performance management, and fault management and not perform billing management and confidentiality management.

7.3 Network administration items

Administer the following items:

a) Node status (included alive signal of network devices);

b) Traffic;

c) Cable disconnections.

7.4 Requirements for network monitoring devices

The crew shall be able to monitor from a network-monitoring device installed on the bridge or the like.

The crew shall be able to identify the locations of errors from the network-monitoring device.

The network monitoring device shall indicate appropriate countermeasures for problems.

7.4.1 Functionality of network monitoring devices

Network monitoring devices shall have the following functionality.

7.4.1.1 Function to display physical architecture of network

The network-monitoring device shall display a schematic of the physical architecture of the target network.

The network-monitoring device shall have a function to automatically display information using SNMP packets.

The network-monitoring device shall make it possible to register devices that do not support SNMP on the network-architecture schematic manually, and display the status as a response to ICMP communication.

The network-monitoring device shall be able to display the status (linked/not linked) of each node of the network device.

Use ping or traceroute for the response to ICMP communication.

7.4.1.2 Alarm function

The network-monitoring device shall have a function to detect abnormal state changes and notify the user of them:

a) When a link is disconnected or the power is turned off for a network device or network terminal;

b) When a link is connected or the power is turned on for a network device or network terminal;

c) When there are Packet loops;

d) When the traffic exceeds the threshold value;

e) When an otherwise defined network-device anomaly occurs;

f) When an otherwise defined network-terminal anomaly occurs.

7.4.1.3 Logging function

The network-monitoring device shall be able to record changes in emergency status, alarms, SNMP traps, and other events. An event log shall be kept for at least the past 24 h.

But, alarms and SNMP traps event logs should be stored for at least the past 30 days.

7.4.1.4 Traffic display function

The network-monitoring device shall be able to display the network traffic (between network devices and network terminals, and between network devices) in the form of a trend graph.

7.4.1.5 Setting configuration function

The network-monitoring device shall be able to change the settings of the network-monitoring devices and MIB of nodes on the network using SNMP.

7.4.1.6 Fault recovery support function

The network-monitoring device shall be able to provide information and suggest remedies in order to recover from failures.

7.4.1.6.1 Network information

The network-monitoring device shall be able to store and display a list of the device names, MAC address, IP addresses, and installation locations of network terminals.

The network-monitoring device shall be able to store and display a list of the device names, IP addresses (if any), and installation locations of network devices.

7.4.1.6.2 Failure remedies

Procedures shall be registered on the network-monitoring device as remedies for the following faults in network devices:

a) Network device stoppage;

b) Network device restart;

c) Packet loops.

7.5 Requirements for network nodes

There are two types of network node: network devices and network terminals.

Each network node shall have a self-diagnostics feature.

The network nodes shall notify the network-monitoring device of their status periodically or upon failure.

7.5.1 Network devices

Network devices shall relay network data from hubs, switches, routers, gateways and the like.

7.5.1.1 Network device management functions

Network devices shall have the following management function:

a) Support for SNMP;

b) Support for ICMP;

c) The network should have a function to detect loops in IP packets and Ethernet packet sub-frames

Use SNMP v2c (RFC1901-RFC1908) for SNMP.

Use ICMP v4 (RFC792) for ICMP.

7.5.1.1.1 Detection and notification of management status of network devices

The network devices shall be able to detect the following states by performing self-diagnostics, and the network-monitoring device of the following information using SNMP trap communication shall be notified.

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) Loop guard (only if the network device has a loop detection function);

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).

7.5.1.1.2 Network device management information

The management information of the network devices shall be compatible with the MIB. The network device's management information shall also be sent to the network-monitoring device periodically.

Use MIB or MIB II (RFC1213).

7.5.2 Network terminals

Terminals are connected to the network and perform data communications.

7.5.2.1 Network terminal management functions

Network terminals shall have the following management function:

a) Support for ICMP;

b) May also support SNMP;

c) If it has a function to notify network-monitoring device of log, the log messages shall use a standard communication protocol.

Use SNMP v2c (RFC1901-RFC1908).

Use ICMP v4 (RFC792) for ICMP.

Use syslog (RFC3164) as the standard log-message communication protocol.

8 Operational guidelines

8.1 Notes for network operations

8.1.1 Protection from malware

a) Computers shall not be connected to the shipboard network that are not controlled by the shipboard network, and registered computers shall not be removed from the ship. This does not apply to systems that operate with compact, portable terminals that move on and off ship, but in this case take measures to prevent connection to other than determined networks. Additionally, before replacing a device due to failure or upgrade, the new device shall be checked for viruses to ensure that it does not contain malware.

b) Antivirus measures on the network terminal shall be installed to prevent infection by computer viruses, worms, spyware, and other malware. Examples of malware attack vectors include network

ports, as well as USB, connection ports for communication with IEEE 1394 and other external devices, and CD/DVD/Blue-ray Disc reader drives installed on the network terminal. A virus check shall be taken before making these connections.

c) When receiving external data in order to perform data exchange, the imported data shall be ensured whether it is appropriate for the purpose. The imported data should be checked in order to prevent expecting viruses.

d) Antivirus software shall be installed on each computer, and the virus-definition files updated periodically. The OS should be updated periodically in order to improve security. Automatic updates of the virus definitions and OS shall be performed periodically, and shipboard computers shall be configured to perform auto updates. In order to save communication costs, an update service application to update operating systems and antivirus onboard the vessel should be installed. This does not apply, however, to anti-malware operating systems.

8.1.2 Protection from illicit access

a) In order to prevent illicit remote access, login IDs and passwords shall be stored for startup, communication, and the like in encrypted or otherwise protected form.

b) Login IDs and passwords shall be different strings. Passwords shall be at least eight characters long and consist of a random combination of uppercase letters, lowercase letters, and numbers. Passwords should be updated periodically.

c) User accounts shall be created for remote access with administrator privileges. Remote logins using commonly known administrator account names, such as “Administrator” or “Admin” shall not be allowed.

d) Firewall or other means is recommended to close unused ports, in order to avoid attacks against vulnerabilities in unused ports using TCP or UDP.

e) A log of login status shall be kept in order to enable users to check this log in the event of problems.

f) Network equipment such as L3 switch and router, shall be monitored for unauthorized access, and it shall be reported when there are attempts of such access to monitored areas.

8.2 Notes for exchanging data

8.2.1 Using a VPN

Before using an Internet VPN, the connection shall be tested first thoroughly and assurance is required whether connection with the target environment is possible.

8.2.2 Using FTP

A login record shall be kept on the FTP server. An administrator should check this log periodically.

8.2.3 Downloading data via HTTP or HTTPS

When downloading data via HTTP or HTTPS, suitability of the imported data shall be ensured for purpose. The imported data should also be checked in order to prevent expecting viruses.

8.2.4 Telnet

Remote logins using the telnet command should be prohibited.

8.2.5 Using shared folders

Access to shared folders should be limited to registered users.

A log of accesses to shared folders should be kept. An administrator should check this log periodically.

8.2.6 Using email

When sending email from the ship, SMTP port 587 should be used in order to reduce the possibility of the email being mistaken as spam.

When receiving email on a shipboard network terminal, the suitability of the imported data should be ensured for the purpose. The imported data for viruses should also be checked if code in the body of the email or a program attached to the email is to be used.

8.3 System maintenance

a) The methods for maintaining and testing devices and networks should be defined explicitly, and the operational status of network-monitoring devices and the like should be periodically monitored and tested. A log of these checks shall be kept simultaneously. Simple instructions for updating software installed on each computer should be given, in order to check for software updates and prevent failures.

   EXAMPLE The following are some examples of areas within the scope of the network-system architecture:

   -Day-to-day device-maintenance method;

   -System-status checking method;

   -Software update method;

   -Data backup method;

   -Backup data recovery method.

b) The status of the network is to be monitored so as to identify the location of abnormalities on the vessel.

c) Network equipment such as L3 switch and router, shall be monitored for unauthorized access, and it shall be reported when there are attempts of such access to monitored areas.

d) A user/operation manual and specifications should be provided on the vessel for the network.

9 Installation procedure

9.1 General

Unlike land-based offices, the shipboard environment in which network devices are used shall take external factors into account, chief among them water, vibration, and heat. Given these special circumstances, the methods for installing, protecting, and testing the network shall be defined.

9.2 Network installation procedure

9.2.1 Device installation

9.2.1.1 Environmental resistance

The main network devices shall unexceptionally be installed in protective cases in order to protect the devices. This does not apply, however, to living quarters and other locations where consideration for the ambient environment is not required. The protective cases shall be designed for the ambient environment and ease of operation and maintenance of the device.

Table 2 shows a desirable environment for locations of network devices.

Table 2 — Ambient environment

Parameter	Specification
Ambient temperature	0°C to 45°C
Max. ambient humidity	90 %
Other	There shall be no condensation. There shall be no corrosive or inflammable gases. Dust shall be minimal.

9.2.1.2 Considerations for temperature

Ventilation should be taken into account so that heat does not accumulate inside the protective case.

Protective cases should generally be naturally ventilated, but if the internal temperature of the case can reach 50°C or more, then a ventilation fan or other forced ventilation shall be installed. If the temperature inside the case can rise substantially, a panel cooler or other cooling device shall be installed.

Heat-generating equipment shall not be installed near network devices (especially on top).

9.2.1.3 Considerations for vibration

Install equipment sufficiently distant from vibration sources so that it is not adversely impacted by external vibration, or install such vibration-proofing measures as rubber vibration insulation.

9.2.1.4 Considerations for noise

Equipment shall be installed sufficiently distant from noise sources so that it is not adversely impacted by external noise.

9.2.1.5 Considerations for power source and noise from power source

Use of uninterruptible power supply (UPS) is an effective countermeasure against noise from power source, as well as being a high-availability power source for important network devices. However, stand by type UPS is inferior to other types of UPS in filtering function. Back-up source may be used for enhanced availability. Installation of noise filter or isolation transformer should be considered to protect devices from noise from power source.

9.2.1.6 Considerations for cabling routes

Consideration should be taken not to use the same routes as the main cabling when installing backup cabling.

9.2.1.7 Considerations for cabling in protective cases

Consideration should be taken to use a marine cable with tension member constantly when using optical cables. Cables have to satisfy the requirements from classifications and flag states.

9.2.1.8 Managing installed equipment

Installed equipment and the cables that connect it shall be managed by a list.

The version of list should be managed appropriately.

a) Equipment management items:

   1) Equipment ID number;

   2) Equipment type (L2/L3/router);

3) Manufacturer;
4) Model;
5) Installation location (panel ID number);
6) Power/backup power;
7) IP Address (note address for auto/manual);
8) If the STP type (STP/RSTP) is STP:
9) Port information:
    i) Connector shape (RJ45/SC connector);
    ii) Communication Speed (10/100/1000);
    iii) Compliant protocol (1000BASE-T/1000BASE-SX/1000BASE-LX);
    iv) Optical cable communication wavelength (850nm/1300nm/1350nm);
    v) Optical cable maximum transmission loss;
    vi) VLAN number;
    vii) STP enabled;
    viii) Port trunk;
    ix) Connection cable ID number;
    x) Connected nodes (information about connected devices);
10) IGMP information;
11) Boot configuration file name and version;
12) Routing method (e.g. STATIC/RIP/OSPF/IGRP);
13) IP filter routing information;
14) Optional add-ons;
15) VLAN type (tag/port/none); if a VLAN is not configured, leave the following items blank:
    i) VLAN name;
    ii) VLAN ID;
    iii) IP address;

b) Cable management items:
1) Cable ID number (used in 9.4.4);
2) Cable type (optical/metal);
3) Cable specifications (category, Shield Twisted Pair cable/UTP);
4) Cable connection (straight/cross);
5) Optical cable connector shape;
6) Optical cable mode (multi/single);

7) Optical cable code diameter;

8) Optical cable cladding diameter;

9) Optical cable material (quartz/plastic);

10) Optical cable communication wavelength (850nm/1300nm/1350nm);

11) Optical cable maximum transmission loss;

12) Manufacturer;

13) Model;

14) Cable length;

15) Date installed;

16) Results of conductivity test;

17) Wire map;

18) Transmission loss;

19) Near end crosstalk loss;

20) Optical cable optical loss;

9.2.2 Equipment protection

9.2.2.1 Target equipment

The target equipment is network devices for purposes of connecting to the equipment information network.

9.2.2.2 Devices equipped with protective cases

The protective case should have a lockable construction in order to prevent equipment malfunctions due to improper operation. The key to the protective case should be managed appropriately by a vessel administrator.

9.2.2.3 Password protection

A password for devices with soft protection (password) function should always be set in order to prevent external modification of settings and the like. A password string must not be easily inferred from others.

9.2.2.4 Protection of open ports on switching hubs, routers, etc

Open ports of switching hubs, routers, and the like shall be protected with a locked protector to prevent improper connections by network devices. This may not be necessary, however, if the switching hub, router, or the like is installed in a protective case.

NOTE Protectors are also effective as dust covers.

9.3 Cabling procedure for network cables

9.3.1 Cabling with metal cables

9.3.1.1 Minimum bending radius

The minimum bending radius specified for the cable shall not be exceeded.

NOTE If the minimum bending radius is not complied with, performance can be harmed and the cable can be broken.

9.3.1.2 Tensile load

When the cable is pulled or hung, the cable's specified tensile load shall not be exceeded.

Whenever possible, cabling routes shall be secured after other cabling has been installed. Metal network cables should be installed with care (e.g. cables shall be installed separately). The metal network cables should not be wrapped with other cables, bended or twisted excessively. If cabling is installed vertically, install supports at regular intervals in order to keep the cable's own weight from exceeding the rated tensile load.

9.3.1.3 Bundling

When bundling cables in a cable way, excessive load should not be put onto the cables.

9.3.1.4 Segregation from EMI sources

Separate and isolate cabling from routes for 480 V and lower power lines as is shown in Table 3. (See TIA/EIA-569).

Table 3 — Separation and segregation from noise sources

Status		Minimum Separation		
Power line route/equipment	Signal line (or route)	2 kVA or less	2 to 5 kVA	5 kVA or more
No shield	No shield	127 mm	305 mm	610 mm
No shield	Shielded	64 mm	152 mm	305 mm
Shielded	Shielded		76 mm	152 mm

9.3.2 Cabling with optical cables

9.3.2.1 Minimum bending radius

Optical cables shall not exceed the specified minimum bending radius, in order to prevent transmission loss due to bending of the cables.

NOTE The excess of minimum bending radius could harm performance or cause the cable to break. There are two types of minimum bending radius: the fixed bending radius, which indicates the bending radius after the cabling is installed; and the extension bending radius, which indicates the momentarily tolerable bending radius.

9.3.2.2 Tensile load

When the cable is pulled or hung, the cable's specified tensile load shall not be exceeded.

On instalment of cables, pull on the tension member and the cables themselves shall not be pulled on. Secure cabling routes after other cabling has been installed. The optical cables should not be wrapped with other cables, bended or twisted excessively; for example by installing optical cables separately.

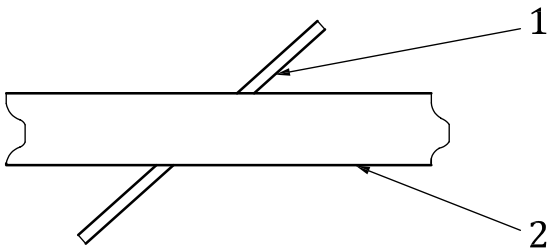
If cabling is installed vertically, install supports at regular intervals in order to keep the cable's own weight from exceeding the rated tensile load.

9.3.2.3 Bundling

When bundling optical cables in a cable way, excessive load should not be put onto the cables.

9.3.2.4 Other forces

As shown in Figure 2, if power lines or other cables are installed together with optical cables in a cable way, excessive pressure should not be applied to the optical cables. Particular care is required to ensure that heavy power cables pass over optical cables at an angle.



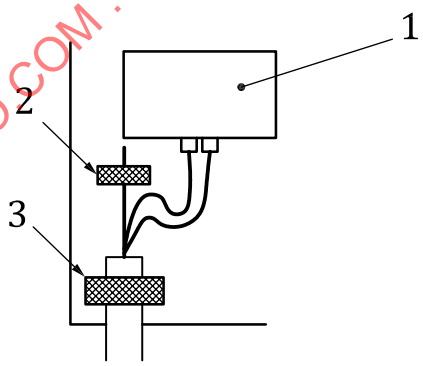
Key

1 optical cable
2 power line

Figure 2 — Caution for cabling with optical cables

9.3.2.5 Terminating optical cables

As shown in Figure 3, lock optical cables and their tension members in place using metal clamps, in order to prevent damage due to vibration and tension.



Key

1 optical cable HUB
2 metal clamp for tension member
3 cable clamp

Figure 3 — Terminating optical cables

9.4 Network testing procedure

Perform testing after the cabling has been completely installed and terminated, and make sure that the network performance does not fall below the minimum value in the standard.

9.4.1 Scope of network testing

An end-to-end test (connector to connector) on the network shall be performed. A report of the test results shall be submitted.

9.4.2 Metal cable testing procedure

The following tests using a cable tester shall be performed. All tests shall be passed.

9.4.2.1 Conductivity test

A conductivity test should be performed to ensure that there are no breaks in the cable.

9.4.2.2 Wire map test

Test shall be performed to ensure that each pair's connector is in the proper location (TIE EIA 568-A/B compliant). At this time, the test shall be performed to check appropriate straight/cross connection in accordance with the specifications.

9.4.2.3 Length test

This test shall be performed to ensure that the cables are not longer than 100 m, and that the cables are not shorter than the originally planned length. If a cable is shorter than the originally planned length, it may be treated as the breakage distance.

NOTE Nearly all cables have better performance than the standard, so a distance longer than the actual length is sometimes shown.

9.4.2.4 Transmission loss test

Transmission loss (db/100 m) shall be tested, and the test shall also be performed to ensure that the transmission loss for each cable is within the rating for that cable (TIE EIA 568-A/B).

9.4.2.5 Near end crosstalk loss

Near end crosstalk loss (db) shall be tested, and the test shall also be performed for near end crosstalk loss greater than the rating for each cable (TIE EIA 568-A/B).

9.4.3 Optical cable testing procedure

9.4.3.1 Testing with power meter

Measurement of the transmission loss (db) using a power meter is required. The measured optical loss shall be within the allowable dissipation for the device used (optical hub or media converter). When measuring the transmission loss, the appropriate calibration wavelength shall be selected for that cable type.

9.4.4 Cable ID number check

Before installing network cables, a check shall be required to see whether an item indicating each cable's ID number is attached. After installing the network cables, a check shall also be required to see whether all characters in the cable's ID numbers can be correctly recognized. These procedures shall be performed regardless of the cable type.

10 Testing

10.1 General

When building the network system, the following tests shall be performed in order to evaluate the test results on each network device making up the network system, and each node connected to the network system.

10.2 Testing procedure

10.2.1 Testing details

Testing of the network system shall be performed upon a testing procedure that clearly states the tests to perform, testing method, testers, and scope of testing, in accordance with this procedure.

10.2.2 Testing method

The testing method, confirmation method, and judgment criteria for each test in the testing procedure shall be clearly defined.

10.2.2.1 Testing procedure

a) 100 % inspection;

b) Sampling inspection.

10.2.2.2 Confirmation method

The procedures and confirmation method should be clearly stated in accordance with the type of test.

10.2.2.3 Judgment criteria

The judgment criteria should be clearly stated in accordance with the type of test.

10.2.3 Tester

a) Shipyard or customer (ship owner);

b) Network system vendor;

c) Node vendor.

10.2.4 Scope of testing

The scope of testing of the network system is 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.

10.3 Network device connection testing

The operation and function of network device connections shall be confirmed. A "network device" is a device forming part of the network system that relays network data. Examples of network devices are hubs, switches, routers, and gateways.

Network device connection testing shall check layer 2 and layer 3 connections. See 9.4 for details about testing cables, connectors, and cabling connecting network devices. Also see 10.5 for details about testing network-system management functions.

10.3.1 Testing details

The following tests on the network-device connections shall be performed, in order to confirm the connections between the network devices and the availability of normal communication shall be ensured.

10.3.1.1 Scope of testing

10.3.1.1.1 Network device interconnection test

The following tests on connections between devices in the same domain, in order to confirm the connections between the network devices, and the availability of normal communication shall be ensured.

10.3.1.1.2 Spanning tree function test

Confirmation shall be carried out for the normal operation of the spanning-tree function used to ensure network redundancy.

10.3.1.1.3 Routing function test

If the network system is connected to another network, and the network system is divided into multiple domains, the routing functionality shall be tested to ensure that the necessary routing functions properly.

10.3.1.2 Testing method

a) Essentially, the testing method shall be 100 % inspection.

b) The confirmation method shall be checking the communication status using the network device's console or a terminal connected to the network device (ping, trace route, etc.).

c) The judgment criteria shall confirm the ability to perform normal communication, and a normal TTL (Time To Live) value.

d) The testing shall be performed by the network system vendor. However, if the network system is connected to another network, then the routing function test for connecting the network system to the other network shall be performed under the responsibility of the shipyard or customer (ship owner), with support from the network system vendor.

10.3.2 Network device interconnection test

Connections between the network devices and the availability of normal communication shall be ensured. The scope of testing shall be the confirmation of connections between all network devices making up the network system. However, if the network system is divided into multiple domains, availability of normal communications within each domain shall be checked.

The testing method shall be essentially 100 % inspection, but a sampling test may be used for connections treated as equivalent in the network.

10.3.3 Spanning tree function test

Confirmation shall be taken on whether the spanning-tree functionality is operating normally. Also confirmation shall be taken on whether the network will operate normally in the event of a quasi route failure.

10.3.4 Routing function test

When building the network system, confirm that the routing function operates normally for connecting the network system to other networks, and connecting domains within the network system. Also confirm that there are no connections from inaccessible devices, and that unneeded packets cannot be routed.

10.4 Inter-node connection testing

10.4.1 Testing details

Confirmation should be taken on whether network communication between nodes connected to the network system is performed normally. However, testing of nodes that do not send or receive data shall be outside the scope of these tests.

10.4.1.1 Scope of testing

Data shall be sent and received normally between nodes connected to the network system.

10.4.1.2 Testing method

a) Essentially, the testing method shall be 100 % inspection.

b) The confirmation method shall cover normal performance of communication and data sending/receiving between nodes, and between terminals connected to the nodes.

c) The judgment criteria shall cover the confirmation of the availability of normal communication, and that the data are sent and received normally.

d) The testing shall be performed by the concerned vendor of the node, in the presence of the network system vendor. If, however, a node installed in the network system is connected to another network connected to the network system, then the test shall also be performed under the responsibility of the shipyard or customer (ship owner), with support from the network system vendor.

10.5 Testing of network monitoring devices and functionality

The network-monitoring devices indicated in 7.4 shall be confirmed whether the devices operate correctly.

10.5.1 Scope of testing

The network-monitoring devices and monitoring functions shall operate normally in the network system.

Required functions are as listed below:

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.

10.5.2 Testing method

a) Essentially, the testing method shall be a 100 % inspection.

b) The confirmation method shall check the functionality of network-monitoring devices.

c) The judgment criteria shall confirm that the network monitoring devices function normally.

d) The testing shall be performed by the network system vendor.

Annex A
(informative)

Implementation of the content provided in this International Standard

A.1 Introduction

When configuring shipboard equipment and systems in accordance with standardized installation guidelines for ship communication networks for improving communication for shipboard equipment and systems where numbers of shipboard equipment with various information platforms is installed, it is important to give due consideration to the design of hardware, firmware and software to interconnect separate systems, as well as to the configuration of systems. For example, some of the shipboard equipment has information platforms equivalent to computers, while some others, including embedded equipment such as control equipment, do not have such platforms, and both of the two coexist in a single ship.

In general, it is considered to be technically very challenging to interconnect that equipment in accordance with the guidelines of information network systems for shipboard equipment.

This Annex is intended to provide detailed examples of technical information that serves as guidelines for areas where the difficulty is expected.

In this Annex, detailed examples of requirements for the components of communication network systems for shipboard equipment are described for each grade of information platform (high, middle, low).

A trial design of the information network system is provided herein for the system architecture, data design and administration, installation and testing of network.

NOTE "Information platform/platform" is a base of hardware and software to perform information processing.

A.2 Network system architecture

A.2.1 Network system design

Refer to separate sheets for the components of the network system discussed herein, compatibility with other equipment (interface) and data regarding information transmission (amount of information, latency and routes):

— Table A.1: Design data for ship communication network systems;

— Table A.2 to Table A.4: Traffic calculation sheet.

A.2.1.1 Scope of network system architecture

This network system should be designed specifically for ships, with the purpose of sharing information between shipboard devices. It should be independent from navigational equipment networks and engine-control networks.

The network should not operate (control) the ship's navigational equipment.

Refer to Figure 1 for the scope of network system architecture.

A.2.1.2 Network separation

The network should be separated from other networks by L3 switch (HUB1) so that they do not impact each other.

A.2.1.3 Traffic division

In order to utilize the network's available bandwidth efficiently and to divide the traffic, the logical network should use a virtual LAN (VLAN) architecture.

A.2.1.4 Network division

The network should be divided by the types of information being handled as stated below:

— Navigational data collection network;

— Engine data collection network;

— Shipboard telephone network;

— Imaging network.

A.2.1.5 Redundancy

Connections between sub-networks should use loop architecture, and RSTP (Rapid Spanning Tree Protocol) should be employed.

To prevent simultaneous disconnection failures, network cabling should take two routes, on both sides of the board.

A.2.2 Network interface for shipboard equipment and systems

A.2.2.1 Interface

This network system should comply with Ethernet standard IEEE 802.3.

A.2.2.2 Connected equipment

The following is the equipment to be connected to the network:

— VDR;

— Network Monitor;

— Rea Time Monitor (PC);

— Data Logger;

— Data Logger EXT Alarm;

— Engine Telegraph;

— Engine Remote Controller;

— Generator Controller;

— Ballast Controller;

— Sensor Box;

— IP-PBX;

— IP Phone;

— Master Clock (IP);

— Local Clock (IP);

— IP Camera.

A.2.3 Equipment constituting communication network system

A.2.3.1 Network devices

The following is the network equipment used on the network:

— HUB1: L3 Switch;

— HUB2: L2 Switch;

— HUB3: L2 Switch.

Table A.1 — Design data for the communication network systems

No.	Equipment Name	Unit Name	Installation location	Connection HUB	Management type	Network transmission setting			Transmission method					
						Connection shape	Speed	Type	Destination	Protocol	Max Traffic Bandwidth	TX Cycle	Max TX Cycle	
1	Navigation EQ	VDR	Bridge	BR	ICMP	RJ45	10/100	Full Duplex	1	Multicast	2.5 Mbps	Always	15 sec	
2	Navigation EQ	Rea Time Monitor	CAP. RM.	BR	ICMP	RJ45	10/100 /1 000	Full Duplex	0	Multicast	0	0	0	
3	Engine Monitor	Data Logger	ECR	ECR	ICMP	RJ45	10/100	Full Duplex	1	Unicast	10 Kbps	Always 1 sec		
									4	TCP/IP	15 Mbps/Equipment	at Initial		
									5	Unicast	2 Kbps	1 sec		*1
4	Engine Monitor	Data Logger Display Unit	CAP. RM.	BR	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		
5	Engine Monitor	Data Logger EXT. Alarm 1	C/E	BR	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
6	Engine Monitor	Data Logger EXT. Alarm 2	2nd/E	BR	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
7	Engine Monitor	Data Logger EXT. Alarm 3	Bridge	BR	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
8	Engine Monitor	Data Logger EXT. Alarm 4	MESS RM.	B DECK	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
9	Engine Monitor	Data Logger EXT. Alarm 5	SALOON	B DECK	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
10	Engine Monitor	Data Logger EXT. Alarm 6	SHIP'S OFF.	B DECK	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
11	Engine Monitor	Data Logger EXT. Alarm 7	GIM	B DECK	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
12	Engine Monitor	Data Logger EXT. Alarm 8	CAP. RM.	B DECK	ICMP	RJ45	10/100	Full Duplex	3	Unicast	0,1 Kbps	Always		*1
13	Remote control	Engine Telegraph	Bridge	BR	ICMP	RJ45	10/100	Half Duplex	14	Unicast	0,1 Kbps	Always		*3
14	Remote control	Engine Remote Controller	ECR	ECR	ICMP	RJ45	10/100	Half Duplex	13	Unicast	0,1 Kbps	Always		*3
15	Generator Controller	Generator Controller	ER/ECR	ECR		RJ45	10/100	Full Duplex	3	Unicast	1 Kbps	1 sec		

Table A.1 — *(Continued)*

No.	Equipment Name	Unit Name	Installation location	Connection HUB	Management type	Network transmission setting			Transmission method					
						Connection shape	Speed	Type	Destination	Protocol	Max Traffic Bandwidth	TX Cycle	Max TX Cycle	
16	Ballast Controller	Ballast Controller	U/D	BR		RJ45	10/100	Full Duplex	3	Unicast	4 Kbps	1 sec		
17	Analog Data	Sensor Box	E/R	B DECK		RJ45	10/100	Half Duplex	3	Broadcast	6 Kbps	5 sec		
18	IP Phone	IP-PBX	BR	BR		RJ45	10/100	Full Duplex	19	Unicast	3 Kbps	at Call		
19	IP Phone	IP Phone	Bridge	BR		RJ45	10/100	Full Duplex	18	Unicast	94 Kbps	at Call		
20	Clock (IP)	Master Clock	Bridge	BR		RJ45	10/100	Half Duplex	21	Unicast	0,1 Kbps	30 sec		*3
21	Clock (IP)	Local Clock				RJ45	10/100	Half Duplex	20	Unicast	0,1 Kbps	30 sec		*3
22	IP Camera	IP Camera	E/R	ECR		RJ45	10/100	Full Duplex	3	Multicast	5 Mbps			*2
23	IP Camera	IP Camera	E/R	ECR		RJ45	10/100	Full Duplex	3	Multicast	5 Mbps			*2
24	IP Camera	IP Camera	Outside	BR		RJ45	10/100	Full Duplex		Multicast	5 Mbps			*2
25	IP Camera	IP Camera	Outside	BR		RJ45	10/100	Full Duplex		Multicast	5 Mbps			*2
26	Digital data	Fire alarm		ECR		RJ45	10/100	Full Duplex	3	Broadcast	0,1 Kbps	Always		*3
27	Digital data	Flood warning		ECR		RJ45	10/100	Full Duplex	3	Broadcast	0,1 Kbps	Always		*3
28	Digital data	Door status		ECR		RJ45	10/100	Full Duplex	3	Broadcast	0,1 Kbps	Always		*3
29														

*1: The communication with the Data Logger EXT is an assumption value for the replacement of RS485 serial communications with LAN (unicast).

*2: Bandwidth of The IP Camera is a reference value.

*3: Actual traffic is 0,1 Kbps or less.

The communication of the engine monitor always communicates repeatedly.

Table A.2 — Traffic calculation seat (BR)

Location	BR				
Port No.		In Packets(Bytes/S)			Out Packets (Bytes/S)
		Type	Destination	MAX	MAX
1	VDR	Full	4	2 500,0 Kbps	
2	Real Time Monitor/Live Player	Full	ECR	35,0 Kbps	25 000,0 Kbps
3	Data Logger Display Unit	Full	ECR	0,1 Kbps	15 000,0 Kbps
4	Data Logger EXT. Alarm Panel 1	Full	ECR	0,1 Kbps	2,0 Kbps
5	Data Logger EXT. Alarm Panel 2	Full	ECR	0,1 Kbps	2,0 Kbps
6	Data Logger EXT. Alarm Panel 3	Full	ECR	0,1 Kbps	2,0 Kbps
7	Engine Telegraph	Half	ECR	0,1 Kbps	0,1 Kbps
8	Ballast Controller	Full	ECR	4,0 Kbps	0,1 Kbps
9	IP-PBX	Full	ECR/GEN	3 102,0 Kbps	3 102,0 Kbps
10	Master Clock	Half	ECR/GEN		
11					
12	IP Phone1(CAP. BED RM)	Full	11	94,0 Kbps	94,0 Kbps
13	IP Phone2(CAP. DAY RM)	Full	11	94,0 Kbps	94,0 Kbps
14	IP Phone3(C/OFF. RM)	Full	11	94,0 Kbps	94,0 Kbps
15	IP Phone4(2/OFF. RM)	Full	11	94,0 Kbps	94,0 Kbps
16	IP Phone5(3/OFF. RM)	Full	11	94,0 Kbps	94,0 Kbps
17	IP Phone6(3/OFF. RM)	Full	11	94,0 Kbps	94,0 Kbps
18	IP Phone7(C/ENG. RM)	Full	11	94,0 Kbps	94,0 Kbps
19	IP Phone8(2/ENG. RM)	Full	11	94,0 Kbps	94,0 Kbps
20	IP Phone9(3/ENG. RM)	Full	11	94,0 Kbps	94,0 Kbps
21	IP Phone10(OWNER'S RM)	Full	11	94,0 Kbps	94,0 Kbps
22	IP Phone11(OFF'S SP.RM)	Full	11	94,0 Kbps	94,0 Kbps
23					
24					
25	L2 SW(172.20.1.253) Gen	Full		19 142,2 Kbps	3 141,5 Kbps
26					

Table A.3 — Traffic calculation seat (General)

Location	General				
Port No.		In Packets			Out Packets
		Type	Destination	MAX	MAX
1					
2	Data Logger EXT. Alarm Panel 4	Full	ECR	0,1 Kbps	2,0 Kbps
3	Data Logger EXT. Alarm Panel 5	Full	ECR	0,1 Kbps	2,0 Kbps
4	Data Logger EXT. Alarm Panel 6	Full	ECR	0,1 Kbps	2,0 Kbps
5	Data Logger EXT. Alarm Panel 7	Full	ECR	0,1 Kbps	2,0 Kbps
6	Data Logger EXT. Alarm Panel 8	Full	ECR	0,1 Kbps	2,0 Kbps
7					
8	IP Phone12(NO.1 OILER RM)	Full	BR	94,0 Kbps	94,0 Kbps
9	IP Phone13(OILER (A) RM)	Full	BR	94,0 Kbps	94,0 Kbps
10	IP Phone14(OILER (B) RM)	Full	BR	94,0 Kbps	94,0 Kbps
11	IP Phone15(OILER (C) RM)	Full	BR	94,0 Kbps	94,0 Kbps
12	IP Phone16(ORD. S/M. (A) RM)	Full	BR	94,0 Kbps	94,0 Kbps
13	IP Phone17(ORD. S/M. (B) RM)	Full	BR	94,0 Kbps	94,0 Kbps
14	IP Phone18(ORD. S/M. (C) RM)	Full	BR	94,0 Kbps	94,0 Kbps
15	IP Phone19(AB. S/M. (A) RM)	Full	BR	94,0 Kbps	94,0 Kbps
16	IP Phone20(AB. S/M. (B) RM)	Full	BR	94,0 Kbps	94,0 Kbps
17	IP Phone21(AB. S/M. (C) RM)	Full	BR	94,0 Kbps	94,0 Kbps
18	IP Phone22(C/STEW. RM)	Full	BR	94,0 Kbps	94,0 Kbps
19	IP Phone23(BOS'N RM)	Full	BR	94,0 Kbps	94,0 Kbps
20	IP Phone24(SALOON)	Full	BR	94,0 Kbps	94,0 Kbps
21	IP Phone25(OFF'S MESS RM)	Full	BR	94,0 Kbps	94,0 Kbps
22	IP Phone26(SHIP'S OFF.)	Full	BR	94,0 Kbps	94,0 Kbps
23					
24					
25	B/R	Full		3 141,5 Kbps	16 974,2 Kbps
26	C/R	Full		15 564,2 Kbps	16 974.7 Kbps

Table A.4 — Traffic calculation seat (E/R, C/R)

Location	E/R, C/R				
Port No.		In Packets			Out Packets
		Type	Destination	MAX	MAX
1					
2	Data Logger (Main)	Full	BR	15 000,0 Kbps	35,0 Kbps
3	Data Logger (Option)	Full	BR/GEN	0,1 Kbps	20,0 Kbps
4					
5	Engine Remote Controller	Full	BR	0,1 Kbps	2,0 Kbps
6	Generator Controller	Full	4	0,1 Kbps	2,0 Kbps
7	Sensor Box	Half	4	0,1 Kbps	0,1 Kbps
8					
9	IP Camera 1	Full	BR/GEN	5 000,0 Kbps	2,0 Kbps
10	IP Camera 2	Full	BR/GEN	5 000,0 Kbps	2,0 Kbps
11					
12	Fire alarm	Full	4	0,1 Kbps	0,1 Kbps
13	Flood warning	Full	4	0,1 Kbps	0,1 Kbps
14	Door status	Full	4	0,1 Kbps	0,1 Kbps
15					
16	IP Phone27(ECR)	Full	BR	94,0 Kbps	94,0 Kbps
17	IP Phone28(ENGINE SIDE)	Full	BR	94,0 Kbps	94,0 Kbps
18	IP Phone29(HOSPITAL)	Full	BR	94,0 Kbps	94,0 Kbps
19	IP Phone30(GYM SPACE)	Full	BR	94,0 Kbps	94,0 Kbps
20	IP Phone31(CREW'S SMOK. RM)	Full	BR	94,0 Kbps	94,0 Kbps
21	IP Phone32(CREW'S MESS. RM)	Full	BR	94,0 Kbps	94,0 Kbps
22					
23					
24					
25	L2 SW(172.20.1.253) Gen	Full		623,3 Kbps	15 564.2 Kbps
26					

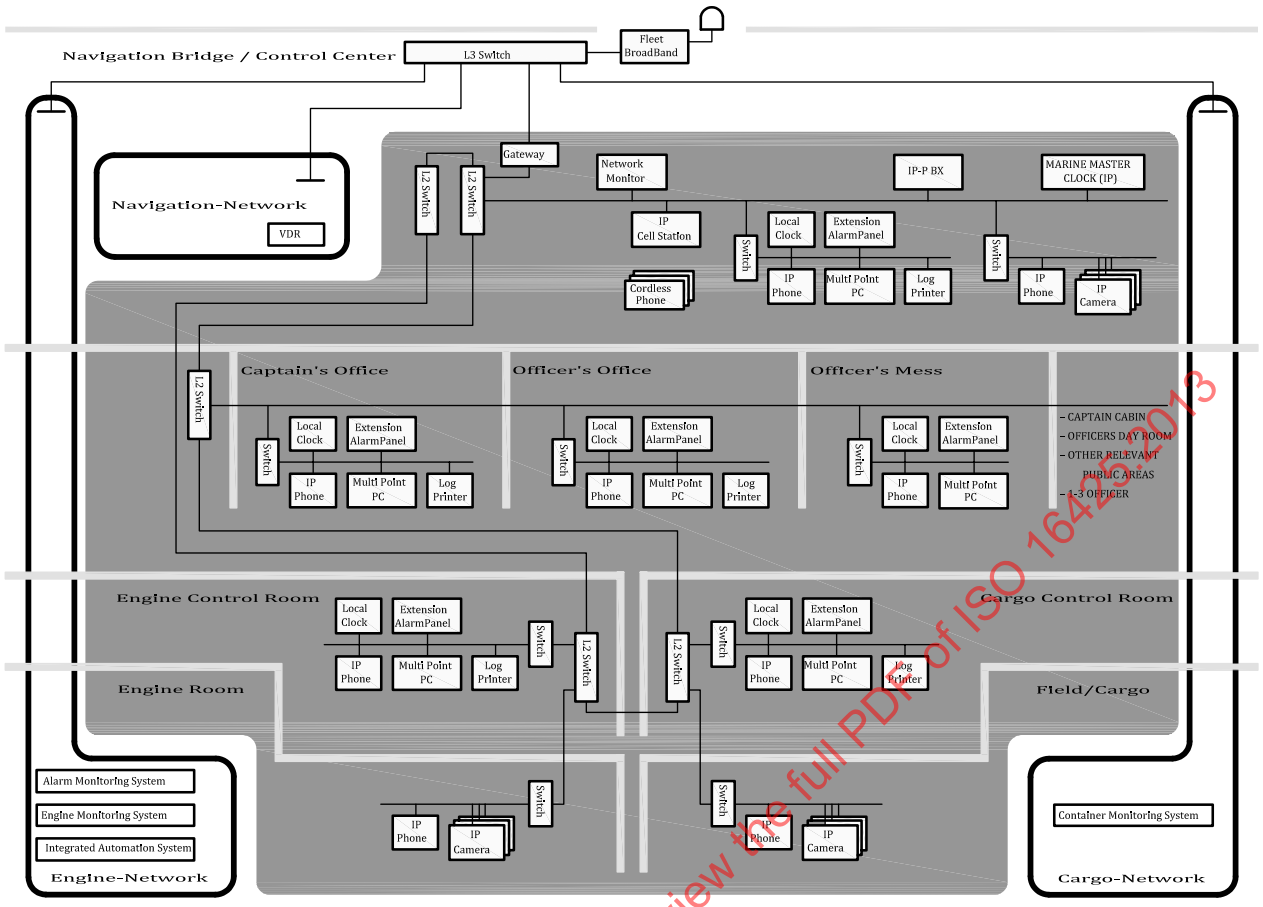


Figure A.1 — Sample network architecture scope (Reference)

A.3 Data requirements

A.3.1 Data transmission

The network handles information on other sub-networks, and information on the communication network systems. Other sub-networks include navigational equipment network, engine network, and cargo network, and information equipment used on the information network includes IP Phone, IP Camera, Clock(IP).

Table A.5 specifies network division and a sample of traffic, a data type, and a protocol.

Communication between shipboard equipment via these communication network systems should be performed through network gateways such as L3 switches.

A.3.2 Communication data format

The following should be taken into consideration when choosing the data format:

A.3.2.1 Communications regulated by international standards

For communications for which communication methods are stipulated in international standards such as the IEC 61162 series (IEC 61162-1 or IEC 61162-450), applicable standards should be complied for the format.

A.3.2.2 Communications that should use standardized data format from the perspective of compatibility with the counterpart device

For those for which a communication protocol is not specified in international standards such as equipment in engine network and, equipment in cargo network, data format should conform to the stipulation in Clause 6 in consideration of the interoperability between the source equipment and destination equipment.

In case XML is selected for the data format, which is recommended in Clause 6, the definition of data attribute should be standardized between the source side and destination side in order to use identical identifiers between the two.

A.3.2.3 Communications for which arbitrary format may be used

An arbitrary format may be used for communication in an identical information equipment or in case processors for which the aforementioned standards are not applicable are used.

A.3.3 Data format, protocol and delivery format in each network

A.3.3.1 Navigational data

Data sentence should be used for the data format. This format is defined in international standards such as the IEC 61162 series. UDP/IP multicast should be used as the delivery format in order to reduce the network communication bandwidth load.

A.3.3.2 Engine data

Data sentence, which is stipulated in the IEC 61162 series, or XML, which is recommended in Clause 6 should be used for the data format except for communications between identical shipboard equipment including communication between Extension Alarm Panel and engine monitor.

Data sentence stipulated in the IEC 61162 series, should be used for communications between shipboard equipment for real time performance is required, such as alarm monitoring system.

A.3.3.3 Cargo and ballast data

Data sentence, which is stipulated in the IEC 61162 series, or XML, which is recommended in Clause 6 should be used for the data format.

For communication between shipboard equipment for which real time performance is required, data sentence, which is specified in IEC 61162 should be used.

A.3.3.4 Audio data (IP Phone)

Audio data should be communicated after being compressed in accordance with speech coding standards such as G711. To achieve a good real time performance required for communication of audio data, UPD/IP unicast should be used for such communication and the network should be separated from other networks by VLAN.

A.3.3.5 Image data (IP camera)

Image data should be communicated in formats such as MPEG and Motion JPEG. UDP/IP multicast should be used for communication of image data to reduce the communication bandwidth load and should have the network separated from other networks by VLAN.

A.3.3.6 Clock Data (Clock(IP)

Clock Data should be communicated through UDP/IP unicast and broadcast in compliance with NTP protocol. The communication between shipboard Clocks should be separated from other networks by VLAN. NTP protocol should be complied for communication with other networks as well.

A.3.4 Encryption

In principle, encryption is not required for information handled on information network for shipboard equipment except for confidential data. Encryption methods such as S/MIME for emails should be used for such confidential data.

Table A.5 — Data requirements

Source network terminal			Destination device No.	Data format			Delivery		Notification frequency	Maximum communication load	Encryption
Device No.	Device name	VLAN ID		Data type	Protocol		Communication method	Delivery format			
1	Navigation / VDR	1	2	Navigational data	UDP/IP	NMEA	Multicast	Unidirectional	Constant	2,5 Mbps	None
2	Navigation / Real Time Monitor	1	-	-	-	-	-	-	-	-	-
3	Engine monitor	2	1	Engine data	UDP/IP TCP/IP	NMEA /XML	Unicast	Unidirectional	Constant	10 Kbps	None
			4	Engine data	TCP/IP	arbitrary	Unicast	Request/ Respond	Upon start-up	15 Mbps	None
				Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	1 Mbps	None
			5	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			6	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			7	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			8	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			9	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			10	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			11	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
			12	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
4	Engine monitor Display Unit	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None

Table A.5 — *(Continued)*

Source network terminal			Destination device No.	Data format			Delivery		Notification frequency	Maximum communication load	Encryption
Device No.	Device name	VLAN ID		Data type	Protocol		Communication method	Delivery format			
5	Engine monitor EXT. Alarm 1	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
6	Engine monitor EXT. Alarm 2	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
7	Engine monitor EXT. Alarm 3	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
8	Engine monitor EXT. Alarm 4	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
9	Engine monitor EXT. Alarm 5	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
10	Engine monitor EXT. Alarm 6	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
11	Engine monitor EXT. Alarm 7	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
12	Engine monitor EXT. Alarm 8	2	3	Engine data	UDP/IP	arbitrary	Unicast	Unidirectional	Every 1 sec	0,1 Kbps	None
13	Telegraph	2									
14	M/E Remote Controller	2									
15	Generator Control System	2	3	Engine data	UDP/IP	NMEA	Unicast	Unidirectional	Every 1 sec	2 Kbps	None
16	Ballast Control System	2	17	Engine data	UDP/IP TCP/IP	NMEA /XML	Unicast	Unidirectional	Every 1 sec	4 Kbps	None
17	Analogue Sensor Data	2	*	Engine data	UDP/IP	NMEA	Broadcast	Unidirectional	Every 1 sec	2 Kbps	None
18	IP-PBX IP Phone / IP-PBX	3	20	Audio data	UDP/IP	Speech coding	Unicast	Unidirectional	Constant when line is busy	64 Kbps	None

Table A.5 — *(Continued)*

Source network terminal			Destination device No.	Data format			Delivery		Notification frequency	Maximum communication load	Encryption
Device No.	Device name	VLAN ID		Data type	Protocol		Communication method	Delivery format			
19	IP Phone / IP Phone	3	19	Audio data	UDP/IP	Speech coding	Unicast	Unidirectional	Constant when line is busy	64 Kbps	None
20	Clock (IP) / Master Clock	4	22	Clock Data	UDP/IP	NTP	Unicast / Broadcast	Unidirectional	Periodically when answered	1 Kbps	None
21	Clock (IP) / Local Clock	4	20	Clock Data	UDP/IP	NTP	Unicast	Unidirectional	Upon request	-	-
22	IP Camera / Camera #1 (E/R)	5	*	Image data	UDP/IP	Image (movie) (compressed)	Multicast	Unidirectional	Constant	5 Mbps	None
23	IP Camera / Camera #2 (E/R)	5	*	Image data	UDP/IP	Image (movie) (compressed)	Multicast	Unidirectional	Constant	5 Mbps	None
24	IP Camera / Camera #3 (Outside)	5	*	Image data	UDP/IP	Image (movie) (compressed)	Multicast	Unidirectional	Constant	5 Mbps	None
25	IP Camera / Camera #4 (Outside)	5	*	Image data	UDP/IP	Image (movie) (compressed)	Multicast	Unidirectional	Constant	5 Mbps	None
26	Fire Alarm (Binary Data)	6	*	Hull / Loading Data	UDP/IP TCP/IP	NMEA/XML	Broadcast	Unidirectional	Constant		None
27	Flood Alarm (Binary Data)	6	*	Hull / Loading Data	UDP/IP TCP/IP	NMEA/XML	Broadcast	Unidirectional	Constant		None
28	Watertight Door Condition(Binary Data)	6	*	Hull / Loading Data	UDP/IP TCP/IP	NMEA/XML	Broadcast	Unidirectional	Constant		None
Remark: Asterisk (*) signifies that the destination is not specified.											

A.4 Network administration

A.4.1 Design of network monitoring devices

A.4.1.1 Hardware for network monitoring device

Computers to be used should be 24 h of continuous operation guaranteed.

Computers and displays should be compliant with IEC 60945 as they will be installed on the bridge for monitoring purposes.

Ethernet interface in the computers should be 10 Mbps, 100 Mbps and 1 Gbps compatible.

Storage devices with appropriate capacity should be installed for recording SNMP communication data, logs, network traffic data etc.

A.4.1.2 Operating system for network monitoring devices

In consideration for monitoring software, Windows or LINUX should be used for the operating system.

A.4.1.3 Monitoring software for network monitoring devices

Monitoring software for network monitoring devices should be SNMP (V2c compliant) and PING response monitor compliant. Software with functions to display network diagram and to automatically display the operational status of switches and communication status between switches by SNMP communication data, should be selected.

SNMP trap communication data should be saved in the storage devices for 30 days.

A.4.1.4 Log management software for network monitoring devices

In case a log management server is to be installed, the software should be equipped with functions to import syslog communication data and display and save the imported data.

The communication data of syslog should be saved in the storage devices for 30 days.

A.4.1.5 Abnormality notification design for network monitoring device

Signals for the following abnormalities and status changes should be transmitted from network devices and network terminals and notified to the user by sound or display on the screen.

a) Notification by display on the screen only:

   1) When the link is disconnected and power is out for network devices or network terminals

   2) When the link is connected and power is on for network devices or network terminals

b) Notification by both sound and display on the screen:

   1) Packet loops

   2) When the communication traffic data (broadcast, multicast, unicast) exceeds the threshold

   3) Other abnormalities in defined network devices and network terminals.

A.4.1.6 Traffic display function for network monitoring system

Network traffic transitions (between a network device and network terminal, between network devices) should be displayed as trend graphs. The traffic data acquired from devices by SNMP should be recorded

in the storage devices for 30 days (the recording frequency should be determined based on the data size and the capacity of storage devices).

A.4.1.7 Failure recovery support design for network monitoring devices

Save a list containing information including device name, MAC address, IP address and location of network terminals and display the list on the screen.

Save a list containing information including device name, IP address (if any) and location of network devices and display the list on the screen.

Recovery procedures for the following failures are installed, and display the procedures as necessary.

a) Network device stoppage;

b) Network device restart;

c) Packet loops.

A.4.2 Network administration

A.4.2.1 Administrative items and methods for equipment

See Table A.6 below for the administrative items and methods for the communication network systems.

Table A.6 — Administrative items and methods for equipment

No.	Device name	Administrative item	Method
1	Sensor Box IP-PBX IP Phone Master Clock (IP) Local Clock (IP) IP Camera Data Logger Data Logger EXT Alarm Engine Telegraph Engine Remote Controller Generator Controller Ballast Controller VDR Rea Time Monitor (PC)	IP address	ICMP
2	HUB1: L3 Switch HUB2: L2 Switch HUB3: L2 Switch	IP address MIB information (SNMP) Trap information (SNMP)	SNMP

A.4.2.2 Network administration requirements

No piece of equipment should have the SNMP manager function installed. Instead, such equipment should have SNMP agent or ICMP protocol installed, and should respond to requests from monitoring devices that have SNMP manager functions.

A.4.2.2.1 Administration by ICMP

Only ICMP should be installed, and SNMP manager responds to periodical ICMP.

A.4.2.2.2 Administration by SNMP

Information should be transmitted to SNMP manager in accordance with MIB information and trap setting using SNMP agent.

A.4.2.2.3 SNMP design

SNMP community name, password etc. should be determined.

Names and passwords that are commonly used (i.e. public) should not be used. Arbitrary names and passwords with more than eight letters that contain both letters and numbers should be used.

A.4.2.3 Miscellaneous

a) In case camera images or audio data are transmitted, network design should be examined by traffic statistical analysis using LAN analyser (i.e. by stream or by packet such as images, sound, data etc.) due to factors such as priority control and the high traffic associated with such transmission.

b) UPS status should be monitored by SNMP as administrative requirements for start up and shutdown of power related and network systems:

   — UPS operation status.

   — Battery deterioration status.

   — Output current.

   — It should be configured so that operation and monitoring even logs may be recorded and checked.

   — When starting the network system, the PC and related equipment automatically start up with their Wake on LAN function when UPS power is turned on. Accordingly, the PC and related equipment should be configured to automatically shut down when UPS power is turned off. However, it is not required that embedded equipment and low information platform be equipped with Wake on LAN as DC24V is used for that equipment and platforms. As for power monitor operation log should be recorded by UPS so that the system can be recovered quickly when experiencing abnormalities.

   — Output power frequency should be fixed at 60 Hz regardless of whether the input power frequency is switched to 50 Hz from 60 Hz, or the other way around.

A.5 Installation

In accordance with the communication network systems traffic calculation sheet, shipboard network should have 3 HUBs compatible with optical cables that can support transmission at rates of 100 Mbps or above as the main HUB.

A.5.1 Guidelines for network installation

The HUB should be stored in a lockable box located on bridge, General and ECR respectively.

Refer to Table A.7 Equipment Management items for details on the equipment.

Refer to Table A.8 Cable Management items for details on the cables.

Table A.7 — Equipment Management items

Items		Description								
Equipment ID Number		HUB3								
Equipment type		L2								
Installation location		General								
Panel ID No		HUB3								
Power/Backup Power		UPS Backup								
IP Address		172.20.1.252/24								
STP type		RSTP								
Port Information										
	Connection shape	Speed	Compliant	Wave length	Transmission loss	VLAN ID	STP	Trunk	Cable ID	Node
1										
2	RJ45	100/Full	100Base-T			20			W-DT-45	
3	RJ45	100/Full	100Base-T			20			W-DT-46	
4										
5	RJ45	100/Full	100Base-T			20			W-DT-47	
6	RJ45	100/Full	100Base-T			20			W-DT-48	
7	RJ45	10/Half	10Base-T			20			W-DT-49	
8										
9	RJ45	100/Full	100Base-T			40			W-DT-50	
10	RJ45	100/Full	100Base-T			40			W-DT-51	
11										
12	RJ45	100/Full	100Base-T			20			W-DT-52	
13	RJ45	100/Full	100Base-T			20			W-DT-53	
14	RJ45	100/Full	100Base-T			20			W-DT-54	
15										
16	RJ45	100/Full	100Base-T			30			W-DT-55	
17	RJ45	100/Full	100Base-T			30			W-DT-56	
18	RJ45	100/Full	100Base-T			30			W-DT-57	
19	RJ45	100/Full	100Base-T			30			W-DT-58	
20	RJ45	100/Full	100Base-T			30			W-DT-59	
21	RJ45	100/Full	100Base-T			30			W-DT-60	
22										
23										
24										

Table A.7 — *(Continued)*

Port Information										
	Connection shape	Speed	Compliant	Wave length	Transmission loss	VLAN ID	STP	Trunk	Cable ID	Node
25	SC	1000/Full		850nm	3 dB/km	Tag(10/20 /30)	RSTP		W-DT-1	
26	SC	1000/Full		850nm	3 dB/km	Tag(10/20 /30)	RSTP		W-DT-3	
IGMP Information			None							
Config File/ver			SNO1234.cfg ver 1.01							
OS Version										
Login User/password			Manager/friend							
Routing			Static							
IP Filter			none							
Port Information										
	Connection shape	Speed	Compliant	Wave length	Transmission loss	VLAN ID	STP	Trunk	Cable ID	Node
VLAN Information										
ID	10	20	30	40						
Name	BRIDGE	ENG	IPTEL	GEN						
IP	172.20.1.253	172.20. 2.253	172.20.3. 253	172.20.4.253						

Table A.8 — Cable Management items

No.	Cable ID	Type	Metal Cyeable			Optical Cable							Maker	Length m	Date Installed	Results of conductivity test	Wire map	Transmission loss	Near end cross-talk loss
			Specifications	Single/ Twist	straight/ cross	Connector shape	Mode	Core diameter µm	Cladding diameter µm	Material	Wave length nm	Optical loss dB/km							
1	W-DT-1	Optical				SC	Multi mode	50	125	Quartz	850	3	FEIC	180					
2	W-DT-2	Optical				SC	Multi mode	50	125	Quartz	850	3	FEIC	160					
3	W-DT-3	Optical				SC	Multi mode	50	125	Quartz	850	3	FEIC	30					
4	W-DT-4	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	10					
5	W-DT-5	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	35					
6	W-DT-6	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	35					
7	W-DT-7	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	27					
8	W-DT-8	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	12					
9	W-DT-9	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	20					

Table A.8 — *(Continued)*

No.	Cable ID	Type	Metal Cable			Optical Cable							Maker	Length m	date installed	Results of conductivity test	Wire map	Transmission loss	Near end cross-talk loss
			Specifications	Single/ Twist	straight/ cross	Connector shape	Mode	Core diameter	Cladding diameter	Material	Wave length	Optical loss							
10	W-DT-10	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	20					
11	W-DT-11	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	40					
12	W-DT-12	Metal	Shield Twisted Pair Cable	Twist	straight								FEIC	3					
13	W-DT-13	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	24					
14	W-DT-14	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	30					
15	W-DT-15	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	34					
16	W-DT-16	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	30					
17	W-DT-17	Metal	Shield Twisted Pair Cable	Single	straight								FEIC	20					