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)

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.

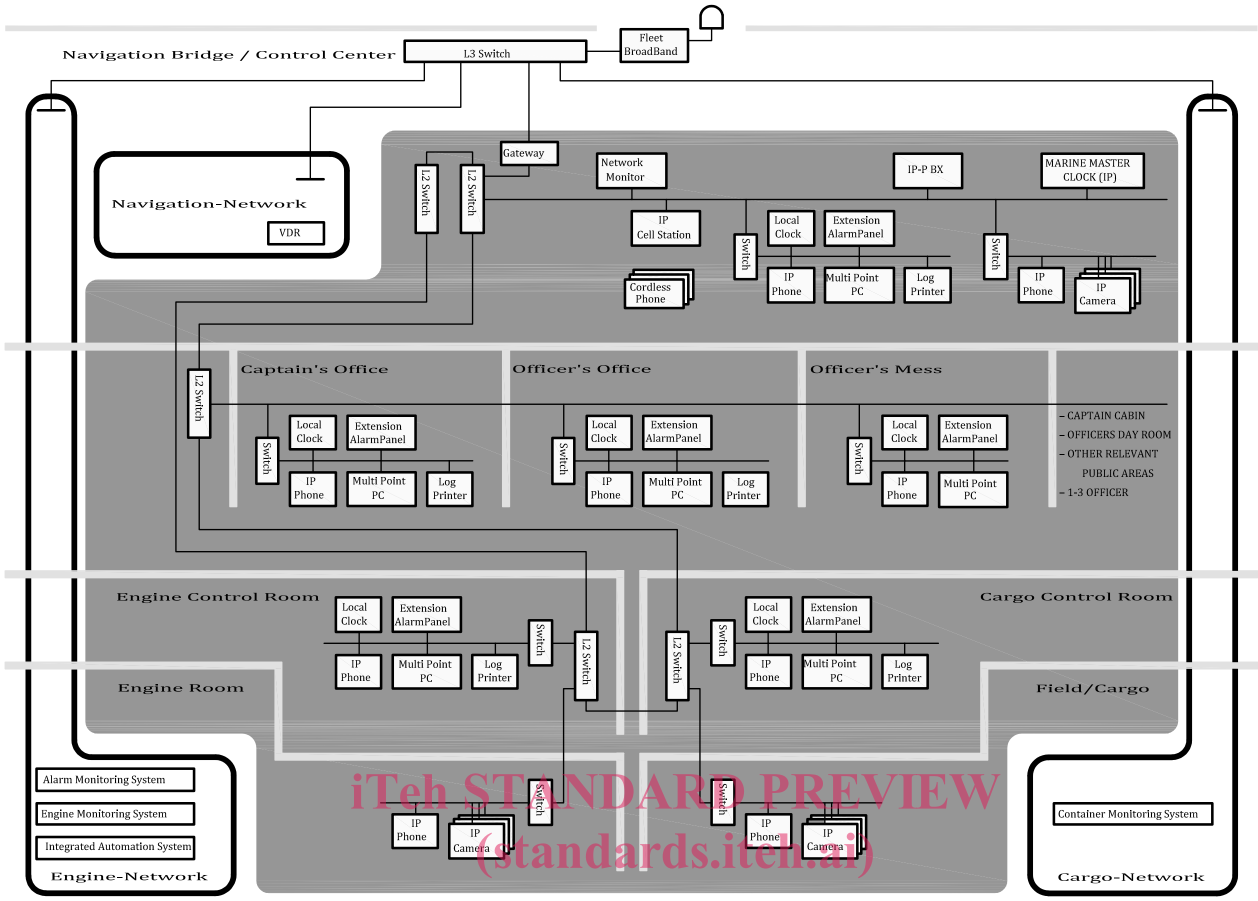

Figure 1 — Sample network architecture scope (Reference)

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 REVOLU-TION	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* >