BS ISO 16425:2024

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

National foreword

This British Standard is the UK implementation of ISO 16425:2024. It supersedes BS ISO 16425:2013, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/80, Maritime navigation and radiocommunication equipment and systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 15622 5

ICS 47.020.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

International Standard

ISO 16425

Second edition
2024-01

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

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

Reference number
ISO 16425:2024(en)

© ISO 2024

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

Contents

Page

Foreword ... **vi**
Introduction ... **viii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Abbreviated terms ... **6**
5 Network system architecture ... **7**
5.1 Scope of networks system architecture ... 7
5.2 Controlled network requirements ... 9
5.3 Network system design ... 9
5.3.1 General ... 9
5.3.2 Network system separation ... 10
5.3.3 Network division ... 10
5.3.4 Traffic division ... 10
5.3.5 Redundancy ... 11
5.3.6 Cyber security ... 11
5.4 Roles and management ... 11
5.4.1 General ... 11
5.4.2 Ship owner ... 11
5.4.3 System integrator ... 11
5.4.4 Ship operator ... 11
5.4.5 Manufacturer ... 12
5.4.6 After-sales-service provider ... 12
6 Organized necessary function ... **12**
6.1 General ... 12
6.2 Necessary information ... 12
7 Operation plan design ... **13**
7.1 General ... 13
7.2 Objectives for managing shipboard network operations ... 13
7.3 Items to manage ... 15
7.3.1 Items to manage devices and cables to be installed ... 15
7.3.2 Items to monitor and details ... 15
7.3.3 Details of maintenance ... 15
7.3.4 Back-ups and log management ... 15
7.3.5 Operation of reports ... 15
7.3.6 Service management ... 16
8 Understanding the equipment to be installed ... **16**
8.1 Understanding the equipment ... 16
8.1.1 General ... 16
8.1.2 Inventory lists ... 16
8.2 Requirements for the 16425-Network device and 16425-equipment installed in the shipboard network ... 16
8.2.1 General cyber security requirements for 16425-Network devices and 16425-equipment ... 16
8.2.2 Network interface for 16425-Network equipment and 16425-Network device ... 17
8.2.3 Requirements for 16425-Network nodes ... 17
8.2.4 Requirements for 16425-Network devices ... 18
8.3 Protocol and traffic ... 23
8.3.1 General ... 23
8.3.2 Protocol ... 23
8.3.3 Traffic ... 23
8.3.4 IP address ... 23

© ISO 2024 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

8.3.5 MAC address 23
8.4 Cable 23
8.4.1 General 23
8.4.2 Cable specification 23
8.4.3 Cable earth method 23

9 Network design 24
9.1 General 24
9.2 Concept of shipboard network system 24
9.2.1 General arrangement 24
9.2.2 Channel 24
9.2.3 Permanent ink 24
9.2.4 Code 25
9.2.5 Extender connector 25
9.2.6 Telecommunications outlet 25
9.3 Design standard 25
9.3.1 Category of cables and codes 25
9.3.2 Plug connection method 25
9.3.3 Specifications for naming cable 25
9.3.4 Model number of cable, code, plug, jack and crimping tools to be used 25
9.4 Physical design 25
9.4.1 Selection of 16425-Network equipment 25
9.4.2 Cabling 27
9.4.3 Separation of collision domain 28
9.4.4 Setting of interfaces 28
9.4.5 Installation 28
9.5 Logical design 28
9.5.1 General 28
9.5.2 Isolation of network 28
9.5.3 Broadcast domain 29
9.6 Reliability design 29
9.6.1 General 29
9.6.2 Redundancy 29
9.6.3 Monitoring of shipboard networks 29
9.6.4 Load design 30
9.7 Wireless network design 30
9.7.1 General 30
9.7.2 Frequency requirement 30
9.7.3 Frequency interference 30
9.7.4 Load design 31
9.7.5 Installation design 31
9.7.6 Wireless network security design 31
9.7.7 Power supply and voltage 31
9.7.8 Pre-survey 31
9.7.9 Security design 32
9.8 Documentation 32
9.8.1 Network design document 32
9.8.2 List of equipment (device inventory) 32
9.8.3 Schematic diagram 32
9.8.4 Logical topology diagram 33
9.8.5 List of virtual networks 33
9.8.6 List of interfaces between (virtual) networks 33
9.9 Risk assessment (design phase) 33

10 16425-Network device and cable installation 33
10.1 General 33
10.2 Installation procedure 34
10.2.1 16425-Network device 34
10.2.2 Network cable 34
10.2.3 Cable end termination 36

© ISO 2024 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

10.3 Installation confirmation ... 37
10.3.1 Conductivity confirmation ... 37
10.3.2 Wire map confirmation ... 37
10.3.3 Length confirmation ... 37
10.3.4 Insertion loss test ... 37
10.3.5 Near end crosstalk loss ... 37
10.3.6 Power meter checking ... 38
10.3.7 Cable ID ... 38
10.3.8 End termination ... 38
10.4 16425-Wireless-Gateway installation procedures ... 38
10.4.1 Environmental resistance ... 38

11 Network cable installation and wireless installation test and inspection ... 38
11.1 Cable installation ... 38
11.2 16425-Wireless Gateway installation confirmation ... 44

12 Network operation ... 45
12.1 General ... 45
12.2 Identify vulnerabilities ... 45
12.2.1 Operation policy and procedure ... 45
12.2.2 Inventory and assessment ... 45
12.3 Develop protection and detection measures ... 46
12.3.1 Policy and procedure ... 46
12.3.2 Access control ... 46
12.4 Response and recovery ... 46
12.4.1 Contingency plan ... 46
12.4.2 Response to shipboard network incidents ... 46
12.4.3 Recovery from shipboard network incidents ... 46
12.5 Maintenance ... 47
12.5.1 Maintenance policy and procedure ... 47
12.5.2 Maintenance document and report ... 47

13 Network cyber security ... 47
13.1 Network cyber security requirements ... 47
13.1.1 General ... 47
13.1.2 Cyber security management system ... 47
13.1.3 Operation plan design ... 48
13.1.4 16425-Network equipment access security ... 49
13.1.5 Wireless network access authentication method ... 50
13.1.6 Network design ... 51

Annex A (informative) **Implementing the content provided in this document ... 56**

Annex B (informative) **16425-Network nodes and network monitoring specifications ... 77**

Annex C (informative) **16425-Network implementation example ... 81**

Bibliography ... 83

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 16425:2013), which has been technically revised.

The main changes compared are as follows:

— the title of this document has been changed from “guidelines” to “specification”;

— all Clauses have been revised in line with the shipboard network design procedure;

— designs for Wi-Fi networks, networks equipped with a shipboard data server that conform to ISO 19847 and ISO 19848, and requirements for cybersecurity for shipboard networks have been added;

— in Clause 5, the scope of this document has been included in the network system architecture;

— in Clause 6, information necessary for network design has been provided;

— in Clause 7, the requirements for the operation plan design of the shipboard network have been added;

— in Clause 8, information on shipboard network devices has been added;

— in Clause 9, the network design methods for the physical design of cable and connector for shipboard network equipment and for the logical design of network separation and communication between networks with cyber security have been updated;

— in Clause 10, the equipment, grounding and termination of cables and network equipment have been clarified;

— in Clause 11, network testing and inspection objectives, conditions, methods and criteria have been added;

— in Clause 12, information necessary for network operation has been provided;

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

— in Clause 13, cyber security requirements for networks have been added;

— in Annex A examples of input/output information required for network design have been added;

— in Annex B, examples of monitoring and managing the shipboard network and the nodes connected to the network have been added;

— in Annex C, an example of secure-network implementation compliant with this document has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

Introduction

This document gives specifications relating to communication network-system architecture, data requirements, administration, operation, commissioning, inspection and testing for shipboard equipment and systems.

This document also takes into account differences between shipboard communication networks and networks that are used outside of ships, and stipulates requirements and specifications relating to matters unique to shipboard use.

Until the publication of this document, there has been a lack of comprehensive specifications for connecting devices that are provided by many different manufacturers to a network via a generic means. This gap has impeded the wider use of shipboard networks.

This document aims to improve the convenience for all involved parties, including manufacturers, engineering firms, shipbuilders, and shipping companies.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

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

1 Scope

This document provides installation specifications for ship communication networks, so as to improve communication between shipboard equipment and within shipboard systems that are independent from navigational equipment networks and engine-control networks. This document can also be applied to operational technology (OT) networks that use software and hardware to control and monitor devices and infrastructure such as navigational equipment networks and machinery control networks in ship.

The ship communication networks covered in this document are intended for information sharing and are not directly related to safety of navigation.

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

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

This document uses the standard communication network Internet protocol.

This document applies to shipboard wired networks for IP communication, using Fast Ethernet and Gigabit Ethernet as specified in IEEE 802.3 and to shipboard wireless networks for IP communication, using the unlicensed 2,4 GHz and 5 GHz bands as specified in IEEE 802.11.

NOTE Other wireless technologies based on non-IP communication such as IEEE 802.15.1, IEEE 802.15.4 or wireless communication methods using 920 MHz band are not covered in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 24060:2021, *Ships and marine technology — Ship software logging system for operational technology*

ISO/IEC 11801-1, *Information technology — Generic cabling for customer premises — Part 1: General requirements*

ISO/IEC 14763-3, *Information technology — Implementation and operation of customer premises cabling — Part 3: Testing of optical fibre cabling*

ISO/IEC 20000 (all parts), *Information technology — Service management*

IEC 60092-504:2016, *Electrical installations in ships— Part 504: Automation, control and instrumentation*

IEC 60945, *Maritime navigation and radiocommunication equipment and systems - General requirements - Methods of testing and required test results*

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

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

IEC 61162-460:2018/AMD1:2020, *Maritime navigation and radio communication equipment and systems — Digital interfaces — Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and security*

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

IEEE 802.11, *Ethernet (Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications)*

ANSI/TIA-568.0:2020, *Generic Telecommunications Cabling for Customer Premises*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
16425-Network
controlled network consisting of devices that meet the requirements of the *16425-Network node* (3.4)

3.2
16425-Network device
hubs (3.21), layer 2 switches, layer 3 switches, routers and other devices that connect and relay between networks

3.3
16425-Network equipment
shipboard equipment for processing, sending and receiving data

3.4
16425-Network node
16425-Network equipment (3.3) and *16425-Network device* (3.2)

3.5
AES
advanced encryption standard
symmetric key cryptosystem

3.6
application level gateway
network infrastructure device that connects 16425-Networks with other networks and which satisfies the safety and security requirements as specified in this document

3.7
business local area network
business LAN
network that crewmembers use for ship operation duties

3.8
broadcast domain
domain on a computer network where broadcasted frames (broadcasts) are received

3.9
collision domain
domain in a computer network where simultaneous transmission cause collisions or congestion

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

3.10
controlled network
network that has been designed to operate such that authorities are satisfied by documented evidence that the network does not pose any security risks to any connected network nodes

Note 1 to entry: For example, any network compliant to IEC 61162-450 or this document that is approved by classification society, flag state or recognized organization (RO) is considered as a controlled network.

3.11
Crew local area network
Crew LAN
network that crewmembers use for personal matters or in their spare time

3.12
extender connector
non-powered connections, including telecommunication outlets

3.13
data base system
systems equipped on the internet working or shore to manage data efficiently

3.14
DIAMETER
authentication, authorisation, and accounting protocol for computer networks

3.15
DMZ
demilitarized zone
physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and un-trusted network, usually the Internet

3.16
firewall
system installed at network nodes to ensure security by controlling unwanted traffic among different network segments and to and from the internet and other external sources

3.17
gateway
communication device that connects computer networks to networks with differing protocols

3.18
hub
concentrator that is centrally located in a network comprising a star physical topology

3.19
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

3.20
IP
internet protocol
network layer communications protocol in the Internet protocol suite for relaying datagrams across network boundaries

3.21
IT network
information network not related to onboard control system

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

3.22
layer 2 switch
hub (3.18) that can direct traffic on an *open systems interconnection reference model* (3.28) layer 2 (data link layer)

3.23
layer 3 switch
hub (3.18) that can direct traffic on an *open systems interconnection reference model* (3.28) layer 3 (network layer)

3.24
log rotation
automated process used in system administration in which log files are compressed, moved (archived), renamed or deleted once they are too old or too big

3.25
MAC address
media access control address
identifier used to identify network interfaces

3.26
MD5
message digest algorithm 5
hash function producing a 128-bit hash value

3.27
MIB
management information base
type of database for managing devices in a network

3.28
OSI reference model
open systems interconnection reference model
model that divides the communication functions for computers into layers

Note 1 to entry: See ISO/IEC 7498 for further details.

3.29
operation technology network
OT network
exclusive network of control and operational technology for optimal operation of products, equipment, and systems on board

3.30
proxy
component acting as an intermediary between two equipment on the network

3.31
port trunk
method of raising transmission speed by governing two or more physical cables

3.32
RADIUS
remote authentication dial-in user service
networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

3.33
REDS
removable external data source
user removable non-network data source, including, but not limited to, compact discs, memory sticks and devices compliant with IEEE 802.15.1

3.34
SNMP
simple network management protocol
communication rules that define methods for communicating information in order to monitor and control network devices within a network

3.35
shore network
non-shipboard networks, including internet working

3.36
SSID
service set identifier
name which identifies an access point in a wireless network

3.37
SHA
secure hash algorithm
cryptographic hash function

3.38
STP
spanning tree protocol
method of control in a loop topology network for preventing data from entering endless loops

3.39
SYN flood attacks
attack that abuses transmission control protocol (TCP) connections and overloads the system to prevent it from operating

3.40
TAG VLAN
tag virtual local area network
function that adds an ID called a VLAN tag to Ethernet frames to identify the *VLAN* (3.44) to which the frames forwarded across the switch belong

3.41
trouble report
statement reporting the nature of a malfunction to the system integrator, shipowner, or management company, in the event of a malfunction within shipboard equipment or networks

3.42
uncontrolled network
data network that is not compliant with IEC 61162-450, IEC 61162-460, this document, or a controlled network

3.43
UTM
unified threat management
collective control over several different security systems, such as firewall and website filtering, by consolidating them into a single hardware

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

3.44
VLAN
virtual local area network
method for configuring a local area network virtually, regardless of the physical network configuration

4 Abbreviated terms

AMS	alarm monitoring system
ASCII	American Standard Code for Information Interchange
BR	bridge
BWMS	ballast water management system
C/R	control room
CCR	cargo control room
CD	compact disc
CSMA/CD	carrier sense multiple access/collision detection
DVD	digital versatile disc
ECR	engine control room
E/R	engine room
FBB	fleet broad band
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IP	internet protocol
IT	information technology
LAN	local area network
MAC	Media Access Control
MD5	message digest algorithm 5
MIB	management information base
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
OID	Object Identifier

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

OSPF	Open Shortest Path First
OT	operational technology
QoS	quality of service
RIP	Routing Information Protocol
RM	room
RSTP	Rapid Spanning Tree Protocol
SHA	secure hash algorithm
STP	shield twisted pair
TCP	transmission control protocol
UDP	user diagram protocol
UTC	Universal time coordinated
UTP	unshield twisted pair
UTM	unified threat management
VDR	voyage data recorder
VDU	visual display unit
VLAN	virtual local area network
VPN	virtual private network
W/H	wheelhouse
WPA	Wi-fi protected access

5 Network system architecture

5.1 Scope of networks 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 (or control) the ship's navigational equipment, however it is permitted to monitor navigational equipment.

Figure 1 shows a diagram of the network architecture scope in this document. The typical implementation of the contents provided in this document is specified in Annex C. As shipboard networks extend to all important locations onboard ships, the application range of designing, installing, verifying and operating the 16425-network shall not be limited to navigation equipment networks or engine-control networks. If documents prescribe application ranges, these ranges shall be prioritized.

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

— Navigation Bridge/Control Centre;

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

— Business LAN;

— Crew LAN;

— Server system LAN;

— Engine LAN;

— Field/cargo controller LAN.

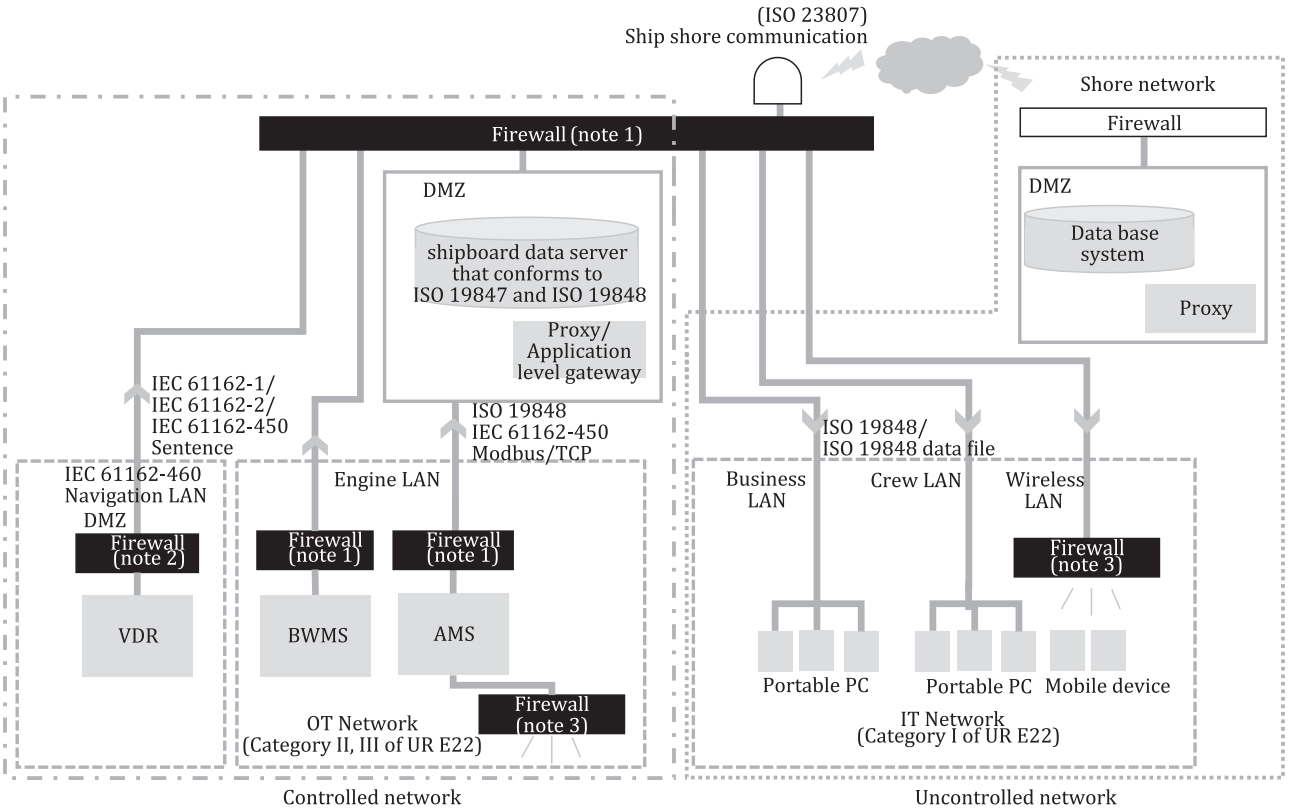
The engine control network and filed/cargo controller network are compliant with this document.

The server system network is configured in the DMZ of an IEC 61162-460 compliant network or an ISO 16425 compliant network.

The Navigation bridge/control centre shall be a network compliant with IEC 61162-450 or IEC 61162-460 that connects to a network compliant with ISO 16425 via a 460-Gateway or 460-forwarder.

Networks compliant with IEC 61162-460 or ISO 16425 are controlled networks. For requirements on controlled networks, see 5.2.

The business LAN and crew LAN are uncontrolled networks.



NOTE 1 The firewall is part of the 460-Gateway or 16425-Gateway. The 16425-Gateway can consist of layer 3 switch, UTM etc.

NOTE 2 The firewall complies with the requirements of the 460-Gateway. The 460-Gateway can consist of layer 3 switch, UTM etc.

NOTE 3 The firewall complies with the 460-Wireless gateway or 16425-Wireless gateway.

Figure 1 — Scope of the network architecture

The functional requirements to use the firewall depend on the capabilities of the network to which it is connected (see Figure 1).

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

5.2 Controlled network requirements

A controlled network is one that has been designed to operate in such a way that it does not pose any security risks to any of its connected network nodes. This shall, as a minimum, satisfy the following requirements:

— it shall not be possible to connect devices to the network that can be used to insert non-authorized traffic into the network, neither by direct access to the physical infrastructure nor through wireless interfaces;

— network nodes shall not grant a user direct access to operating systems or functions that can be used to insert non-authorized traffic into the network, unless this user is authorized to perform these operations;

— it shall not be possible to transfer data from a non-authorized removable external data source (REDS) or a REDS with un-authorized contents to any node or device in the network.

Most controlled networks also include provisions for hindering non-authorized reading of data in the network, hindering changes in network topology, etc. However, such provisions are not required for the controlled networks that are connected to the 16425-Network.

The system integrator shall provide documented evidence that these requirements are met.

5.3 Network system design

5.3.1 General

The design of this network system shall give due consideration to matters such 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 an understanding 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 precalculated when the network media are under maximum load.

When networks are designed, the processes described in Figure 2 shall be followed. In every process, there is information to be input and outcomes to be output, both of which are different from one process to another. Different processes have different conductors to play roles. For the roles of conductors, see 5.4. An example of input and output information required for network design is shown in Annex A.

The squares at the top of the processes listed in Figure 2 represent the information required for the process, and the squares at the bottom of the process represent the deliverables of the process.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

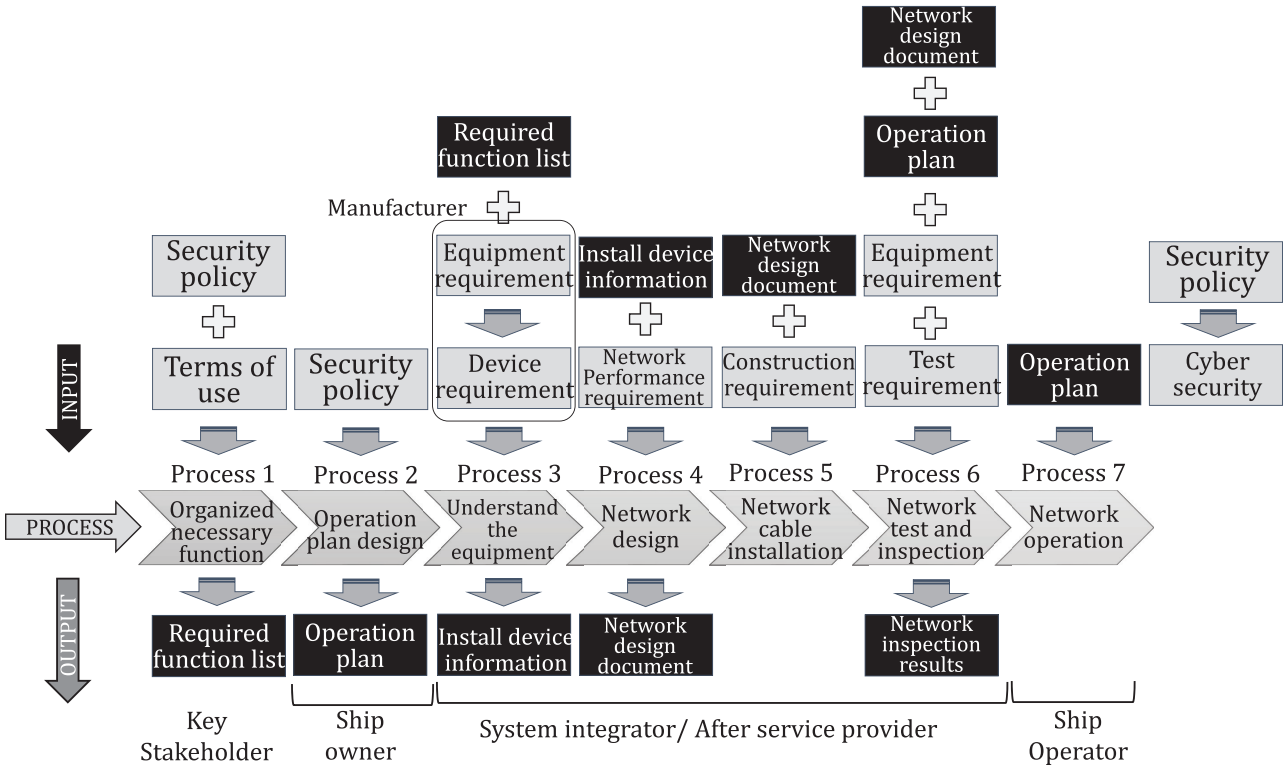


Figure 2 — Shipboard network design processes

5.3.2 Network system separation

The network system shall be separated from other networks by the 16425-Gateway, 460-Gateway or layer 3 switch so that it is not adversely affected by failures on other networks. The routing and filtering rules should be configured appropriately on the 16425-Gateway, 460-Gateway or layer 3 switch for traffic and security. For more advanced security, a firewall for the upper layer can be used.

5.3.3 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. 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.

5.3.4 Traffic division

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.

This logical network shall use a virtual local area network (VLAN) architecture, which forms the network from a virtual group that does not depend on the type of physical connections.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

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.

5.3.5 Redundancy

The connections within the network system shall use a redundant architecture that guarantees that information is transmitted without failure. A loop architecture should be used for connections between sub-networks, employing architecture such as a Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) 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.

5.3.6 Cyber security

Shipboard equipment shall be protected from threats from the shipboard networks with which they are connected and the outside network with which the shipboard networks are connected.

5.4 Roles and management

5.4.1 General

Roles apply at various stages of the shipboard network design processes identified in Figure 2. In addition, each role has general requirements that apply to the installation of ship communication networks within shipboard equipment and systems that are specified in this document.

5.4.2 Ship owner

Ship owners shall define functions and specifications for shipboard networks, and policies for designing such functions and specifications. For defining functions, see Clause 6; for designing networks, see Clause 9; and for operating networks, see Clause 12.

5.4.3 System integrator

Based upon the functions, specifications and policies for designing and operating shipboard networks defined by ship owners, system integrators shall choose devices that meet the requirements set forth in Clause 8 to be installed on shipboard networks. In accordance with Clause 9, system integrators shall design shipboard networks and provide ship owners and ship managers with deliverables.

From time to time, system integrators conduct tests for building shipboard networks. In this case, system integrators shall install shipboard network devices and cables in accordance with Clause 10. Thereafter, system integrators shall test and inspect shipboard networks, as prescribed in Clause 11, and submit the results to ship owners and ship managers.

5.4.4 Ship operator

Ship operators shall appropriately run shipboard networks in accordance with policies created by ship owners for running shipboard networks in Clause 12. When there are changes in shipboard network topologies and/or designs resulting from changes in business operations and/or services used, ship operators shall comply with the policies required by ship owners for designing and running necessary functions and shipboard networks. When installing shipboard devices and/or shipboard networks to be used, ship operators shall use products that meet the requirements described in Clause 8. When cables and other equipment are added because networks are expanded or for other reasons, ship operators shall draw designs in accordance with the network design protocols specified in Clause 9 and install 16425-Network devices and wiring in accordance with the Network device and cable installation protocols specified in Clause 10. When needed, ship operators shall conduct tests and inspections on shipboard networks, and keep documents on shipboard network designs, as specified in Clause 11.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

5.4.5 Manufacturer

Manufacturers provide devices used with shipboard networks, 16425-Network devices and 16425-Network equipment. The devices used for shipboard networks, 16425-Network devices and 16425-Network equipment that manufacturers provide shall comply with the requirements set forth in Clause 8. When requests are made by ship owners, ship operators and/or system integrators to provide protocols and/or traffic, manufacturers shall comply with such requests.

NOTE When information is provided, confidential agreements are signed in some cases between/among ship owners, ship operators, system integrators and manufacturers.

5.4.6 After-sales-service provider

When making changes of shipboard network topologies and/or renewing devices that are used with shipboard networks and/or 16425-Network devices at the request of ship owners or ship operators, after-sales-service providers shall comply to meet functions and specifications defined by ship owners and policies for designing and operating shipboard networks defined by ship owners. Shipboard devices and 16425-Network devices used shall be products meeting the requirements set forth in Clause 8.

When cables and other equipment are added because networks are expanded or for other reasons, ship operators shall draw designs in accordance with Clause 9 and install 16425-Network devices and wiring in accordance with Clause 10. When needed, ship operators shall conduct tests and inspections on shipboard networks, as prescribed in Clause 11. After-sales-service providers shall, then, submit reports to ship owners or ship operators regarding changes made, dates on which the changes are made and test results, and have them reflected on documents on designing shipboard networks.

6 Organized necessary function

6.1 General

Ship owners shall clarify the purposes of building shipboard networks, and define what information is required to accomplish these purposes.

6.2 Necessary information

Ship owners shall submit information on the following items to system integrators.

a) services used on shipboard networks;

b) parties using such services;

c) down time to be tolerated in such services (targeted operation rates);

d) applications required to enjoy such services;

e) information (data) required to enjoy such services;

f) new risks;

g) parties (equipment) that have necessary information;

h) locations of such parties (equipment);

i) plans for expansions after ships are deployed in service;

j) clarification of cybersecurity management systems and policies;

k) operation plan design;

l) security policy.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

Security policies are not applied exclusively on board but should be applied to all relevant organizations, including ships.

7 Operation plan design

7.1 General

System integrators shall design plans for operating shipboard networks in accordance with organized necessary functions defined by ship owners (see Clause 6). Designing plans for operating shipboard networks is important to safely continue to operate shipboard networks.

In operation plan design management, the specific items and contents to be monitored, maintenance details, backup and log management methods, and reporting operations should be based on the ISO/IEC 20000 series.

For items to manage, see 7.3.

7.2 Objectives for managing shipboard network operations

System integrators shall submit operation plans to ship owners when they are designed. By managing shipboard network operations, the objectives described in Table 1 and a) to f) below can be achieved.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

Table 1 — Objectives for managing shipboard network operation

Shipboard network operations	Advantages	Functions					
		Configuration management	Fault management	Performance management	Cost management	Security management	Operation support
Efficient operations	Appropriate use of shipboard network resources	Yes		Yes			
	Easy use of shipboard network states	Yes	Yes	Yes	Yes		Yes
Easy operations	Temporarily separate faults from machinery			Yes			
	Minimize function losses when there are failures	Yes	Yes	Yes			
	Quickly see how much failures spread		Yes				
	Easily add shipboard networks/ make configuration changes in integrated fashions	Yes					Yes
	Easily see shipboard network operations (performances)			Yes			
Safe operations	Fully accomplish system security					Yes	
Fault countermeasures	Easily separate failures in early stages (at node levels)		Yes				
Preventive maintenance	Easily conduct repair/ replacement work	Yes	Yes				

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

The following is an elaborated list of the outcomes in Table 1.

a) Configuration management

Information on shipboard network routes (logical and physical paths), node connections and configurations and operation control are maintained and managed, and operating states are monitored and transmitted.

b) Failure management

By determining and reporting failures that can occur at nodes in shipboard networks, diagnosing the failures, making operation checks and reporting results and taking actions planned in accordance with the failures, it is easier to separate failed areas at early stages, project how much of the failure will spread, and take precautionary and maintenance actions.

c) Performance management

By statistically tallying and appropriately evaluating shipboard network operations, such as traffic and response time, it is possible to efficiently use network resources and draw appropriate plans for expansion work.

d) Cost management

By managing data traffic, it is possible to appropriately manage costs regardless of whether communication is performed under the pay-as-you-go system or at fixed rates.

e) Security management

Security is supported for communications between nodes connected with shipboard networks.

f) Operation support

Different from configuration and failure management, operation support enables networks to be operated and managed smoothly at application levels.

7.3 Items to manage

7.3.1 Items to manage devices and cables to be installed

Devices, cables and codes to be installed shall be managed on lists. Lists shall contain dates when they were created and updated, and information on different versions.

7.3.2 Items to monitor and details

To operate shipboard networks, the state of shipboard network resources for 16425-Network devices and resources for shipboard equipment shall be monitored.

7.3.3 Details of maintenance

Rules shall be established for applying patches, approving and performing upgrading work, controlling access, making setting changes and carrying out machinery maintenance.

7.3.4 Back-ups and log management

Rules shall be established for data and logs, in terms of back-ups, replacement, media storage, rotation, monitoring and compressing.

7.3.5 Operation of reports

Rules shall be established for regular and trouble reports.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

7.3.6 Service management

Rules shall be established for managing incidents in accordance with the ISO/IEC 20000 series.

8 Understanding the equipment to be installed

8.1 Understanding the equipment

8.1.1 General

Equipment to be installed on shipboard networks shall meet the requirements specified in 8.2. System integrators shall document the protocol and traffic information shown in 8.3 and the information required for the design of the shipboard network shown in 9.8, regarding the equipment installed on the shipboard networks.

This document shall be kept as an inventory list and updated during the construction and operation of the ship. Hardware and software information should be updated to ensure that new vulnerabilities and dependencies are not introduced and are handled appropriately to reduce the risk.

8.1.2 Inventory lists

In order to understand the information of the connected equipment, it is necessary to summarize the information related to communication, such as the protocol and data format of the equipment, required cable type, required data and transmitted data, installation location, understanding of the status monitoring function of the equipment, importance of the application, requirements for redundancy, and communication volume. It is also necessary to understand the location of the device and what kind of network topology is required for the device, as well as to summarize prohibited items (items that cannot be handled by security policies or devices) and restrictions rather than necessary functions.

Information on these hardware and software versions shall be maintained in inventory lists (see 12.2.2.1).

8.2 Requirements for the 16425-Network device and 16425-equipment installed in the shipboard network

8.2.1 General cyber security requirements for 16425-Network devices and 16425-equipment

8.2.1.1 REDS security

For removable external data source security, refer to IEC 61162-460:2018/AMD1:2020, 6.2.3.

8.2.1.2 Access control

If the equipment has the capability for software maintenance by crew or service personnel, the equipment shall have a mechanism to identify and authorize users to restrict operation and use of resources. Appropriate authorization shall be assigned to the user and only operations and use of resources consistent with the authorization shall be permitted.

The device shall have at least two authorizations to restrict its operation: general user and administrator with maintenance mode. The identification of the user is carried out by means of an identification and password, through an account, or by means of a physical key authorization. In the case of multi-factor authentication, a combination of these is used, or otherwise. It shall be possible to restrict the operation of the system by using tools that are restricted to service personnel.

8.2.1.3 User authentication

If user identification is by means of an identification and password, a) to e) shall be met.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

If password-based user authentication is used, a) to e) shall also be met, except that additional password restrictions may be enforced by the manufacturer, such as password length, character complexity, excluded word lists, etc.

a) Passwords shall be case-sensitive.

b) Administrator passwords shall be at least 10 characters long and contain a combination of at least three (3) of the following: numbers, uppercase and lowercase letters, and special characters.

c) Passwords for ordinary users shall be at least eight (8) characters in length and shall be a combination of at least two types of alphanumeric and special characters: numbers, uppercase and lowercase letters and special characters.

d) The password shall be a random and meaningless password, not a word found in a dictionary.

e) Passwords shall be strictly stored and managed so that they are hidden from unauthorised persons.

8.2.2 Network interface for 16425-Network equipment and 16425-Network device

8.2.2.1 General

Requirements are defined for devices which are equipped with shipboard networks and shipboard network devices.

8.2.2.2 Interface

The 16425-Network shall use the local area network specified in IEEE 802.3 that is most frequently used for computer networks, and a wireless network specified in IEEE 802.11.

8.2.2.3 Connected equipment

The devices to be connected to the 16425-Network shall be 16425-Network devices that shall share information onboard the vessel.

8.2.3 Requirements for 16425-Network nodes

8.2.3.1 General

The nodes connected to the ship network are classified according to the degree of impact on the ship in the event of a failure. Classifications are called system categories (see Table 2), and the requirements for the 16425-Network node vary by system category.

Table 2 — System categories

Category	Failure effects	Typical system functionality
I	Those systems, failure of which does not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	Monitoring function for informational/ administrative tasks
II	Those systems, failure of which can eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	— Alarm and monitoring functions — Control functions which are necessary to maintain the ship in its normal operational and habitable conditions
III	Those systems, failure of which can immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	— Control functions for maintaining the vessel's propulsion and steering — Vessel safety functions

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024

8.2.3.2 16425-Network nodes (Category I, Category II and Category III)

8.2.3.2.1 16425-Network nodes function requirements

Category II/III equipment installed in the 16425-Network shall meet the requirements a) to g).

a) Category II/III equipment installed in the 16425-Network shall be capable of providing one of the management functions set forth in B.1.2.1.

b) Category II/III equipment installed in the 16425-Network shall be able to control the use of mobile codes.

   When normal operations cannot be maintained, the equipment shall be able to either limit the use of the latest known values or fixed values, as described in manufacturers' instruction manuals.

c) Category II/III equipment installed in the 16425-Network shall provide the function to limit the use of automatic release resources so as not to exhaust CPUs, memory, storage and other resources.

d) Category II/III equipment installed in the 16425-Network shall provide the function to collect definition information that affects system operations and back up saved information without impacting normal operations.

e) Category II/III equipment installed in the 16425-Network shall provide the function to resume a known protected state in case such a state is lost due to breakdowns and other accidents.

f) Category II/III equipment installed in the 16425-Network shall not lose essential services or functions even if there are audit process failures.

g) Category II/III equipment installed in the 16425-Network shall take actions to prevent falsification of checksums or other tools when communication is made between 16425-Network equipment.

8.2.3.2.2 16425-Network nodes management information

16425-Network nodes shall provide information in response to requests from the network monitoring function.

See 8.2.4.6 for the network monitoring function.

8.2.3.2.3 16425-Network nodes functional safety general

16425-network nodes should comply with functional safety standards (e.g. the IEC 61508 series).

Cyber security function should not adversely affect the essential functions or functional safety of ISO 16425-network nodes. If there is a conflict between the functional safety function and the cyber security function, the functional safety function shall be performed prior to the cyber security function and shall provide evidence of 16425-Network nodes.

8.2.4 Requirements for 16425-Network devices

8.2.4.1 General

Devices intended to be connected with the 16425-Network shall meet the requirements specified in 8.2.4.2 to 8.2.4.5.

8.2.4.2 Device constituting communication network system

8.2.4.2.1 Device access control

Changes in network switch, network 16425-Gateway and 16425-Wireless Gateway configurations require authentication from users.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16425:2024

For more information on device access control, see 13.1.4.

8.2.4.2.2 Traffic prioritization

The 16425-Gateway and 16425-Wireless Gateway may prioritize some or all of the traffic from the 16425-Network to the other controlled and uncontrolled networks.

8.2.4.2.3 16425-Network device function requirements

The 16425-Network device function shall be able to define network flows with combinations of interfaces, MAC addresses and IP addresses, protocol numbers and TCP or UDP port numbers.

All unregistered network flows are prohibited.

If VLANs are provided, it should be possible to configure VLANs on a per-interface basis and to support the VLAN protocol version specified in IEEE 802.1Q:2018 (TAG VLAN).

Loop prevention functions such as RSTP and MSTP shall be provided.

NOTE Loops can be produced by misconfigurations. They can also be generated when there are multiple passes due to network topologies or network redundancies.

The 16425-Network device function supports at least the RSTP protocol version of IEEE 802.1s-2002.

Layer 2 switch, layer 3 switch and firewall shall provide the function to make RSTP effective on all interfaces.

8.2.4.3 16425-Gateway/16425-Wireless Gateway

8.2.4.3.1 Requirements

The 16425-Gateway and 16425-Wireless gateway shall meet the following requirements or the requirements for the 460-Gateway set forth in IEC 61162-460:2018, AMD1:2020, 6.3.5.

The following requirements in a) to f) apply to IP communication on controlled and uncontrolled networks.

a) For connections from uncontrolled networks, “not allowed” shall be set as the default.

b) Inward and outward firewalls shall be provided, consisting of source and destination IP addresses, protocols and port numbers.

c) Lists shall be provided of conditions for all direct connections between controlled networks and uncontrolled networks.

d) Lists shall be recorded in the 16425-Gateway and 16425-Wireless gateway or external devices, which shall include changes made in the last 12 months.

e) A list of lists shall be available.

f) Information on source and destination IP addresses, connection start and termination time and TCP port numbers shall be recorded whenever direct connections are made.

8.2.4.3.2 Management functions

8.2.4.3.2.1 General

Network nodes shall provide information in response to requests from network monitoring function.

The 16425-Gateway and 16425-Wireless gateway shall have the following functions:

a) Maintain the configuration information (Config) of all network infrastructure and be able to restore it when requested.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16425:2024