



BSI Standards Publication

Maritime navigation and radiocommunication equipment and systems — Digital interfaces

Part 460: Multiple talkers and multiple listeners —
Ethernet interconnection — Safety and security

National foreword

This British Standard is the UK implementation of IEC 61162-460:2024. It supersedes BS EN IEC 61162-460:2018+A1:2020, which is withdrawn.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 20603 6

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 31 July 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



IEC 61162-460

Edition 3.0 2024-04

INTERNATIONAL STANDARD



**Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection –
Safety and security**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 47.020.70

ISBN 978-2-8322-8275-5

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 High-level requirements.....	16
4.1 Overview.....	16
4.2 Description	16
4.3 General requirements	16
4.3.1 Equipment and system requirements	16
4.3.2 Physical composition requirements	17
4.3.3 Logical composition requirements	17
4.4 Physical component requirements.....	17
4.4.1 450-Node.....	17
4.4.2 460-Node.....	18
4.4.3 460-Switch	18
4.4.4 460-Forwarder	18
4.4.5 460-Gateway and 460-Wireless gateway	19
4.5 Logical component requirements.....	19
4.5.1 Network monitoring function	19
4.5.2 System management function	19
4.6 System documentation requirements	19
4.7 Secure area requirements.....	20
5 Network traffic management requirements.....	20
5.1 460-Node requirements.....	20
5.2 460-Switch requirements.....	20
5.2.1 Resource allocation	20
5.2.2 Loop prevention.....	21
5.3 460-Forwarder requirements	21
5.3.1 Traffic separation.....	21
5.3.2 Resource allocation	22
5.3.3 Traffic prioritization.....	22
5.4 System design requirements	23
5.4.1 Documentation	23
5.4.2 Traffic.....	23
5.4.3 Connections between secure and non-secure areas	23
6 Security requirements.....	24
6.1 Security scenarios	24
6.1.1 Threat scenarios.....	24
6.1.2 Internal threats	24
6.1.3 External threats	24
6.2 Internal security requirements.....	25
6.2.1 General	25
6.2.2 Denial of service protection	25
6.2.3 REDS security	25
6.2.4 Access control.....	26
6.2.5 Executable and non-executable file security	28

6.2.6	Recording of device management activities	29
6.3	External security requirements	30
6.3.1	Overview	30
6.3.2	Firewalls	30
6.3.3	Direct communication	31
6.3.4	Node requirements for direct communication	32
6.3.5	460-Gateway	33
6.3.6	460-Wireless gateway	34
6.4	Additional security issues	35
6.5	Onboard software maintenance	36
6.5.1	General	36
6.5.2	Roll back to previous safe configuration	36
6.5.3	Software maintenance in maintenance mode	37
6.5.4	Semi-automatic software maintenance by the crew onboard the vessel	37
6.5.5	Remote software maintenance	38
6.6	Secure software lifecycle management	39
7	Redundancy requirements	39
7.1	General requirements	39
7.1.1	General	39
7.1.2	Interface redundancy	39
7.1.3	Device redundancy	40
7.2	460-Node requirements	40
7.3	460-Switch requirements	40
7.4	460-Forwarder requirements	40
7.5	460-Gateway and 460-Wireless gateway requirements	40
7.6	Network monitoring function requirements	41
7.7	System design requirements	41
8	Network monitoring requirements	41
8.1	Network status monitoring	41
8.1.1	460-Network	41
8.1.2	460-Node	41
8.1.3	460-Switch	41
8.1.4	460-Forwarder	42
8.2	Network monitoring function	42
8.2.1	General	42
8.2.2	Network load monitoring function	43
8.2.3	Redundancy monitoring function	44
8.2.4	Network topology monitoring function	45
8.2.5	Syslog recording function	47
8.2.6	Redundancy of network monitoring function	48
8.2.7	Alert management	48
9	Controlled network requirements	49
10	Methods of testing and required test results	50
10.1	Subject of tests	50
10.2	Test site	50
10.3	General requirements	51
10.4	450-Node	51
10.5	460-Node	51

10.5.1	Network traffic management	51
10.5.2	Security	52
10.5.3	Redundancy	55
10.5.4	Monitoring	55
10.6	460-Switch	55
10.6.1	Resource allocation	55
10.6.2	Loop prevention	56
10.6.3	Security	56
10.6.4	Monitoring	59
10.7	460-Forwarder	60
10.7.1	Traffic separation	60
10.7.2	Resource allocation	60
10.7.3	Traffic prioritisation	61
10.7.4	Security	61
10.7.5	Monitoring	62
10.8	460-Gateway	63
10.8.1	Denial of service behaviour	63
10.8.2	Access control to configuration setup	63
10.8.3	Communication security	63
10.8.4	Firewall	64
10.8.5	Application services	65
10.8.6	Interoperable access to file storage of DMZ	65
10.8.7	Additional security	66
10.9	460-Wireless gateway	66
10.9.1	General	66
10.9.2	Security	66
10.10	Controlled network	66
10.11	Network monitoring function	67
10.11.1	General	67
10.11.2	Network load monitoring function	67
10.11.3	Redundancy monitoring function	68
10.11.4	Network topology monitoring function	68
10.11.5	Syslog recording function	69
10.11.6	Alert management	69
10.12	System level	70
10.12.1	General	70
10.12.2	System management function	71
10.12.3	System design	71
10.12.4	Network monitoring function	73
10.12.5	Network load monitoring function	73
10.12.6	Redundancy monitoring function	73
10.12.7	Network topology monitoring function	73
Annex A (informative) Communication scenarios between an IEC 61162-460 network and uncontrolled networks		74
A.1	General	74
A.2	Routine off-ship	74
A.3	Routine on-ship	75
A.4	460-Gateway usage for direct connection with equipment	75
Annex B (informative) Summary of redundancy protocols in IEC 62439 (all parts)		76

Annex C (informative) Guidance for testing	77
C.1 Methods of test	77
C.2 Observation	77
C.3 Inspection of documented evidence	77
C.4 Measurement	77
C.5 Analytical evaluation	78
Annex D (informative) Some examples to use this document	79
Annex E (normative) IEC 61162 interfaces for the network monitoring function	83
Annex F (informative) Distribution of functions around 460-Network	84
Annex G (normative) USB class codes	86
Annex H (informative) Cross reference between IACS UR E26/E27 and IEC 61162-460	87
Bibliography	90
Figure 1 – Functional overview of IEC 61162-460 applications	16
Figure 2 – 460-Network with 460-Gateway	30
Figure 3 – Example of redundancy	39
Figure 4 – Example of network status recording information	43
Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks	74
Figure D.1 – 460-Forwarder used between two networks	79
Figure D.2 – 460-Forwarder used between two networks	79
Figure D.3 – 460-Gateway used for e-Navigation services	80
Figure D.4 – 460-Gateway used for remote maintenance	80
Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices	81
Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices	82
Figure E.1 – Network monitoring function logical interfaces	83
Table 1 – Traffic prioritization with CoS and DSCP	22
Table 2 – Summary of alert of network monitoring	48
Table B.1 – Redundancy protocols and recovery times	76
Table E.1 – Sentences received by the network monitoring function	83
Table E.2 – Sentences transmitted by the network monitoring function	83
Table F.1 – Distribution of functions around 460-Network	84
Table F.2 – Equipment standards referencing IEC 61162-460	85
Table G.1 – USB class codes	86
Table H.1 – Cross reference between IACS UR E26/E27 and IEC 61162-460	87

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**MARITIME NAVIGATION AND RADIOCOMMUNICATION
EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –****Part 460: Multiple talkers and multiple listeners –
Ethernet interconnection – Safety and security**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC 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, IEC 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 <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61162-460 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems. It is an International Standard.

This third edition cancels and replaces the second edition published in 2018 and Amendment 1:2020. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) term application server in the 460-Gateway has been changed to application service and application services have been clarified;
- b) based on field experience the alert limit of the network monitoring load has been changed from 80 % to 90 %;

- c) default time for escalation of a warning to an alarm has been changed from max 60 seconds to max 5 minutes as allowed by IMO BAM rules and escalation from caution to warning has been removed from the use of direct access;
- d) recorded event size in network monitoring function has been changed from 1 000 bytes to 1 472 bytes (i.e. size of an ethernet datagram in the network);
- e) requirements have been incorporated for cyber resilience given by the International Association of Classification Societies (IACS) in their documents UR E26 and UR E27. A new Annex H has been added giving a cross reference between the IACS documents and this document.

The text of this International Standard is based on the following documents:

Draft	Report on voting
80/1103/FDIS	80/1112/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

This International Standard is to be used in conjunction with IEC 61162-450:2023.

A list of all parts in the IEC 61162 series, published under the general title *Maritime navigation and radiocommunication equipment and systems – Digital interfaces*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

1 Scope

This part of IEC 61162 is an add-on to IEC 61162-450 where higher safety and security standards are needed, for example due to higher exposure to external threats or to improve network integrity. This document provides requirements and test methods for equipment to be used in an IEC 61162-460 compliant network as well as requirements for the network itself and requirements for interconnection from the network to other networks. This document also contains requirements for a redundant IEC 61162-460 compliant network.

This document does not introduce new application level protocol requirements to those that are defined in IEC 61162-450.

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.

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

IEC 61162-450:2023, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*

IEC 62923-1, *Maritime navigation and radiocommunication equipment and systems – Bridge alert management – Part 1: Operational and performance requirements, methods of testing and required test results*

IEC 62923-2, *Maritime navigation and radiocommunication equipment and systems – Bridge alert management – Part 2: Alert and cluster identifiers and other additional features*

IEEE 802.1D-2004, *IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges*

IEEE 802.1Q, *IEEE Standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks*

ISOC RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)*
Available at <https://tools.ietf.org/html/rfc792>

ISOC RFC 1112, *Host Extensions for IP Multicasting*
Available at <https://www.ietf.org/rfc/rfc1112.txt>

ISOC RFC 1157, *A Simple Network Management Protocol (SNMP)*
Available at <https://tools.ietf.org/html/rfc1157>

ISOC RFC 2021, *Remote Network Monitoring Management Information Base Version 2*
Available at <https://tools.ietf.org/html/rfc2021>

ISOC RFC 2236, *Internet Group Management Protocol, Version 2*
Available at <https://tools.ietf.org/html/rfc2236>

ISOC RFC 2819, *Remote Network Monitoring Management Information Base*
Available at <https://tools.ietf.org/html/rfc2819>

ISOC RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
Available at <https://www.ietf.org/rfc/rfc3411.txt>

ISOC RFC 3577, *Introduction to the Remote Monitoring RMON family of MIB modules*
Available at <https://tools.ietf.org/html/rfc3577>

ISOC RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*
Available at <https://tools.ietf.org/html/rfc4604>

ISOC RFC 5424, *The Syslog Protocol*
Available at <https://tools.ietf.org/html/rfc5424>

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:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1

450-Node

device compliant with IEC 61162-450 and which satisfies additional requirements specified in this document

Note 1 to entry: This also includes nodes only implementing the ONF function block.

3.2

460-Forwarder

network infrastructure device that can exchange data streams between a 460-Network and other controlled networks including other 460-Networks

3.3

460-Gateway

network infrastructure device that connects to 460-Networks and to uncontrolled networks or controlled networks and which satisfies the safety and security requirements as specified in this document

3.4

460-Network

network which consists of only 460-Nodes, 460-Switches, 460-Forwarder, 460-Gateway and 460-Wireless gateway as well as 450-Nodes

3.5

460-Node

device compliant with the requirement of a 450-Node and which satisfies the safety and security requirements as specified in this document

3.6

460-Switch

network infrastructure device used to interconnect nodes on a 460-Network and which satisfies the safety and security requirements as specified in this document

3.7

460-Wireless gateway

network infrastructure device that connects a 460-Network and wireless networks and which satisfies the safety and security requirements as specified in this document

3.8

advanced encryption standard

AES

symmetric-key block cipher algorithm which is based on a substitution-permutation network (SPN) and does not use the data encryption standard (DES) Feistel network

Note 1 to entry: This note applies to the French language only.

3.9

alarm

high-priority alert, condition requiring immediate attention and action by the bridge team, to maintain the safe navigation and safe operation of the ship

[SOURCE: IEC 62923-1]

3.10

backdoor

installed program allowing access to a computer by providing a method of bypassing normal authentication

3.11

controlled network

any network that has been designed to operate such that authorities are satisfied by documented evidence that the network minimises the security risks to any connected network nodes

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

3.12

controlled shutdown

defined way to switch off equipment under normal operating conditions

Note 1 to entry: For example, via the power button to initiate orderly shutdown without data loss or corruption using Advanced Control Power Interface (ACPI).

3.13

category B alert

alert where no additional information for decision support is necessary besides the information which can be presented at the central alert management HMI

[SOURCE: IEC 62923-1]

3.14**caution**

lowest-priority alert, awareness of a condition which does not warrant an alarm or warning condition but still requires attention out of the ordinary consideration of the situation or of given information

[SOURCE: IEC 62923-1]

3.15**demilitarized zone****DMZ**

physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually Internet

Note 1 to entry: This note applies to the French language only.

3.16**denial of service****DoS**

attempt to prevent legitimate users from accessing a machine or network resource

Note 1 to entry: This note applies to the French language only.

3.17**flow**

combination of the following information: source and destination MAC address, source and destination IP address, protocol, source and destination port number

3.18**external data source****EDS**

network or non-network data source, including, but not limited to REDS, excluding 460-Network for which the equipment belongs

3.19**failure mode and effects analysis****FMEA**

method as specified in IEC 60812 for the analysis of a system to identify the potential failure modes, their causes and effects on system performance

3.20**failure mode, effects and criticality analysis****FMECA**

analytic method as specified in IEC 60812 that includes a means of ranking the severity of the failure modes

Note 1 to entry: FMECA extends FMEA by including a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences.

3.21**firewall**

logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules

[SOURCE: IACS UR E27]

3.22**internet control message protocol****ICMP**

protocol according to ISOC RFC 792

Note 1 to entry: This note applies to the French language only.

3.23

internet group management protocol

IGMP

protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and ISOC RFC 4604 (version 3)

Note 1 to entry: This note applies to the French language only.

3.24

least privilege

security concept in which a user is given the minimum levels of access or permissions needed to perform their work

3.25

loss rate

amount of lost data by the receiving device of a flow as lost packets per total amount of packets, measured at the input port of a device

Note 1 to entry: The loss rate is expressed in percent.

3.26

malware

malicious code

software used or created to compromise computer operation

3.27

maximum network load

cumulative maximum amount of all traffic from all network nodes and network infrastructure components of a single 460-Network

Note 1 to entry: The maximum network load is measured in bytes per second (B/s).

3.28

maximum transmission rate

maximum number of bytes per second that can be transmitted by a network node or network infrastructure equipment

3.29

multi-factor authentication

authentication using two or more distinct factors to achieve authentication

Note 1 to entry: Factors are: 1) something you know (e.g., password/personal identification number); 2) something you have (e.g., cryptographic identification device, token); and 3) something you are (e.g., biometric).

3.30

multiple spanning tree protocol

MSTP

protocol, according to IEEE 802.1Q, which is an extension of RSTP for VLANs

Note 1 to entry: This note applies to the French language only.

3.31

neighbour MAC address

MAC (media access control) address of connected 450-Node or 460-Node as seen by 460 Switch and as reported by SNMP (simple network management protocol)

3.32**network infrastructure component**

device that connects at least two nodes in a 460-Network and two different networks, such as 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

3.33**nominal network capacity**

network capacity as a byte rate which is based on the configuration

Note 1 to entry: The capacity is the lowest capacity of any switch in the network to route all traffic.

Note 2 to entry: This is used for specifying capabilities of equipment.

3.34**other network function****ONF**

function block that interfaces to the network as specified in IEC 61162-450

Note 1 to entry: The ONF represents a function that is allowed to share the infrastructure of an IEC 61162-450 network but does not use the protocols defined in IEC 61162-450.

Note 2 to entry: This note applies to the French language only.

3.35**privilege**

authority to perform functions on a computer system

3.36**rapid spanning tree protocol****RSTP**

protocol according to IEEE 802.1D for calculating and configuring the active topology of a network

Note 1 to entry: This note applies to the French language only.

3.37**removable external data source****REDS**

user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth¹ devices

Note 1 to entry: This note applies to the French language only.

3.38**remote network monitoring****RMON**

standard monitoring specification as described in ISOC RFC 3577

Note 1 to entry: This note applies to the French language only.

3.39**ring topology**

topology where each node is connected in series to two other nodes

¹ Bluetooth is the trademark of a product supplied by Bluetooth Special Interest Group. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

3.40

roll-back

restore the system to a previous known state

3.41

RSA

public-key cryptosystem as described in IEEE 1363

3.42

safety

protection of networks from unintentional threats such as system malfunctioning, misconfiguration and misoperation

3.43

secure area

area with defined physical perimeters and barriers, with physical entry controls or access point protection or access point supervision

Note 1 to entry: A ship's navigation bridge with closed consoles and access supervision by the master or officer of the watch is an example of a secure area.

3.44

security

protection of networks from intentional threats such as virus, worm, denial-of-service attacks, illicit access, etc.

3.45

security strength

number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system

EXAMPLE 80 bits, 112 bits, 128 bits, 192 bits, 256 bits.

Note 1 to entry: Security strength of a 3072-bit RSA key is 128 bits.

3.46

simple network management protocol

SNMP

protocol according to ISOC RFC 3411 used to provide management information

Note 1 to entry: This note applies to the French language only.

3.47

SNMP-Trap

method to collect events and statistical information from SNMP enabled equipment such as switches, according to ISOC RFC 1157, ISOC RFC 2021 and ISOC RFC 2819

3.48

shipborne network

data network infrastructure on board a ship to exchange data between equipment on board

Note 1 to entry: This may or may not be connected to shore by satellites or other means.

3.49

sniffing

monitoring and analysis of the network traffic

3.50

stream

combination of all flows from a device that use same protocol

3.51**syslog**

protocol according to ISOC RFC 5424, which is used for an external logging in IEC 61162-450

3.52**system integrator**

person or organisation responsible for the functionality of the integrated 460-network

3.53**threat**

potential cause of an incident in computer security that may result in harm to the system

3.54**transport layer security****TLS**

widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. The TLS protocol is described in the following RFCs; RFC2246 v1.0, RFC4346 v1.1, RFC5346 v1.2, and RFC8446 v1.3

3.55**traffic**

combination of all streams from a device

3.56**uncontrolled network**

any data network that is not a controlled network

Note 1 to entry: In this document this is also known as untrusted network.

3.57**virtual local area network****VLAN**

network according to IEEE 802.1Q consisting of interconnected networks with bridges

Note 1 to entry: This note applies to the French language only.

3.58**virtual private network****VPN****VPN tunnel**

extension of a private network through encapsulated, encrypted, and authenticated links across shared or public networks

Note 1 to entry: This note applies to the French language only.

3.59**warning**

condition requiring immediate attention but no immediate action by the bridge team

Note 1 to entry: Warnings are presented for precautionary reasons to make the bridge team aware of changed conditions which are not immediately hazardous, but may become so, if no action is taken.

[SOURCE: IEC 62923-1]

3.60**wireless access point****wireless AP**

device that connects wireless devices to wired devices through various wireless technologies such as Wi-Fi, Bluetooth

Note 1 to entry: This note applies to the French language only.

4 High-level requirements

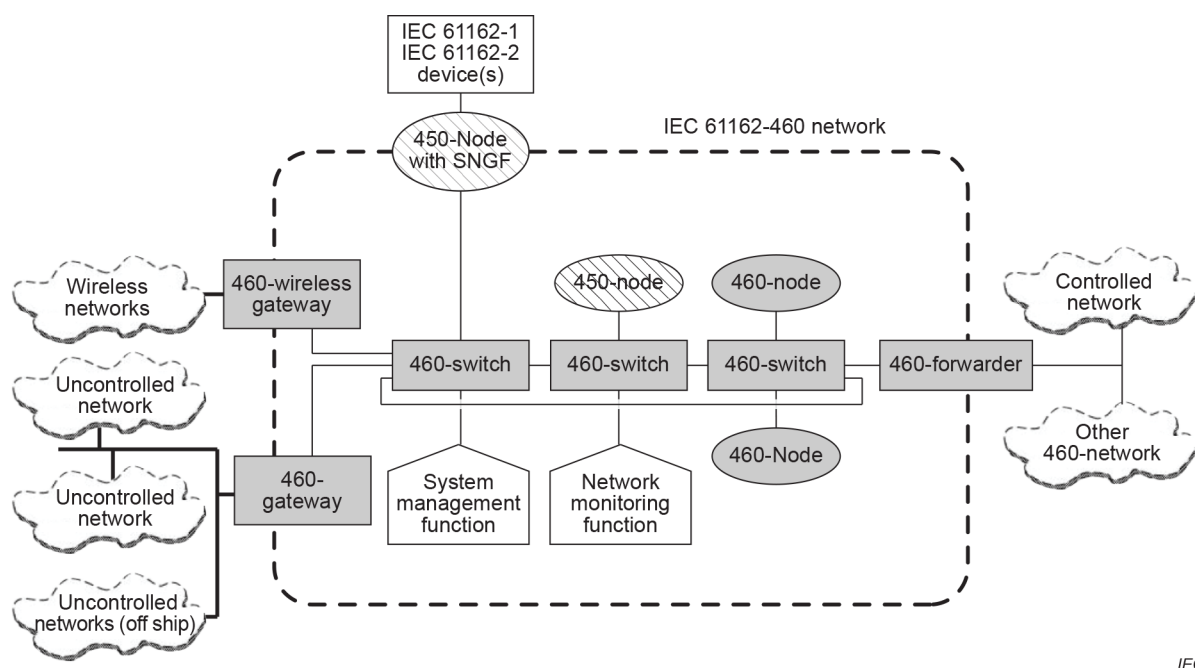
4.1 Overview

This document is based on IEC 61162-450, which is indispensable for this document. This document specifies more stringent requirements for equipment, system design and operation.

Compliance with this document will provide additional protection from threats both from external connections to a network and connections within a network. When a network is solely physically enclosed in a secure area, such as the bridge of a ship where access can be controlled, the larger threat will be from the external connections. Requirements applicable to secure areas are given in 4.7.

4.2 Description

Figure 1 shows a 460-Network as described in this document. The grey symbols represent equipment specified in this document. The pentagons represent logical software functions specified in this document. The hatched symbols represent IEC 61162-450 compliant equipment that is permitted to be included into a 460-Network.



IEC

Figure 1 – Functional overview of IEC 61162-460 applications

Some examples of the use of a 460-Gateway are given in Annex A, and some examples of the use of this document are given in Annex D.

4.3 General requirements

4.3.1 Equipment and system requirements

(See 10.3)

The requirements of 4.3 apply to all equipment and systems intended to be compliant with any part of this document. Subclauses 4.4, 4.5, 4.6 and 4.7 summarize requirements for one type of capability that may be implemented alone, without requiring compliance with other parts of this document.

All equipment forming the 460-Network shall satisfy the general requirements for navigation and radiocommunication equipment as specified in IEC 60945.

NOTE IEC 60945 includes the requirement that equipment be so designed that maintenance of software can be readily carried out on board ship, for example to support periodic update of firmware of network infrastructure equipment to improve encryption algorithms and security features.

All network nodes, network infrastructure components and cables shall satisfy the requirements in Clauses 4 and 5 of IEC 61162-450:2023 as far as applicable.

Manufacturers of network nodes and network infrastructure components shall provide a list of all MAC addresses being used in a 460-Network.

The list can be a label or list or equivalent.

Annex F includes an overview of distribution of various functionalities around physical equipment.

Equipment or network connection points which may be disconnected manually or automatically in order to isolate the 460 Network from other networks or network segments shall be clearly marked, see 4.6.

4.3.2 Physical composition requirements

(See 10.12.3.1)

A 460-Network shall only be composed of the following physical network nodes or network infrastructure components:

- 450-Node, i.e., network nodes compliant with IEC 61162-450 and which fulfil the requirements in 4.4.1;
- 460-Node, network nodes compliant with IEC 61162-450 and which fulfil the additional requirements in 4.4.2;
- network infrastructure components compliant with the requirements for a 460-Switch or 460-Forwarder in 4.4.3 and 4.4.4;
- network infrastructure components compliant with the requirements of a 460-Gateway or 460-Wireless gateway in 4.4.5.

4.3.3 Logical composition requirements

(See 10.12.3.1)

A 460-Network shall also include the following logical system function components, which cover all nodes in a 460-Network:

- network monitoring function, which can be a SF (system function block, see IEC 61162-450) or an ONF (other network function block, see IEC 61162-450) compliant with the requirements in 4.5.1;
- system management function, which can be a SF or an ONF compliant with the requirements in 4.5.2.

4.4 Physical component requirements

4.4.1 450-Node

(See 10.4)

Network nodes that fulfil the requirements of IEC 61162-450 shall also fulfil the following requirements in order to be used in a 460-Network:

- no connection to external networks or REDS;
- syslog implemented as defined IEC 61162-450:2023, 4.3.3.2;
- data output bandwidth documented by the manufacturer as described in 6.2.2.1;
- implemented ONF services specified by the manufacturer, including the necessary protocol parameters, at least IP address and port number;

4.4.2 460-Node

The following functions shall be implemented in a 460-Node:

- network traffic management as specified in 5.1;
- security requirement as specified in 6.2.1, 6.2.2.1 and 6.2.4.1;
- redundancy as specified in 7.2;
- network monitoring as specified in 8.1.2.

If any of the following functions are supported by a 460-Node, they shall be implemented as specified in the following:

- connection with external controlled networks:
 - all valid data packets with correct IP address and port number received from an external controlled network via direct connection through 460-Gateway or 460-Wireless gateway (see 6.3.5.1 and 6.3.6) shall be processed and checked by application level software in the 460-Node; or

NOTE This can be used to create gateways to other network protocols such as MODBUS or OPC.

- if a connection with the controlled network is used to forward unmodified datagrams between the 460-Network and controlled networks or other 460-Networks, then this forwarding shall be handled by a 460-Forwarder;
- support for REDS as specified in 6.2.3;
- direct connection with uncontrolled networks as specified in 6.3.4;
- VLAN compatibility as specified in 5.1;
- implemented ONF services specified by the manufacturer including the necessary protocol parameters, at least IP address and port number;
- ephemeral ports may be used.

4.4.3 460-Switch

The following functions shall be implemented in network infrastructure components which connect equipment within a 460-Network:

- network traffic management as specified in 5.2;
- security requirement as specified in 6.2.1, 6.2.2.2, 6.2.4 and 6.4;
- network monitoring as specified in 8.1.3;
- support for REDS as specified in 6.2.3.

4.4.4 460-Forwarder

The following functions shall be implemented in a 460-Forwarder:

- network traffic management as specified in 5.3;
- security requirements as specified in 6.2.1, 6.2.2.2, 6.2.4 and 6.4;
- network monitoring as specified in 8.1.4;
- support for REDS as specified in 6.2.3;

- VLAN functionality to combine two physical networks (controlled networks and other 460-Networks) into a logical network, if provided, as specified in 5.3.

4.4.5 460-Gateway and 460-Wireless gateway

Connections to uncontrolled networks shall be protected by a gateway fulfilling the requirements for a 460-Gateway as specified in 6.3.5 or a 460-Wireless gateway as specified in 6.3.6. Security requirements as specified in 6.2, 6.2.5 and 6.4 shall be implemented.

4.5 Logical component requirements

4.5.1 Network monitoring function

The network monitoring function shall perform the following functions:

- network load as specified in 8.2.2;
- network redundancy as specified in 8.2.3;
- network topology as specified in 8.2.4.1;
- system function ID SFI collision detection as specified in 8.2.4.2.

4.5.2 System management function

(See 10.12.2)

The system management function is not intended for normal operation and, in accordance with IMO Resolution A.694(17), clause 3.2, should not be readily accessible. Equally, the system management function does not impose a requirement for carriage of additional workstations.

The system management function shall perform the following functions either automatically or manually:

- maintain all network infrastructure configuration information and be able to restore this to the equipment when requested – the management function shall maintain a history of at least the previous configuration;
- save and restore configuration information from 460-Switches, 460-Forwarders, 460-Gateways and 460-Wireless gateways;
- change the infrastructure configuration – this function is necessary to allow exchange of equipment with new MAC addresses as, for example, 460-Switches, which only allow a known MAC to be connected to a specific port.

The save and restore configuration information of the system management function shall be redundantly available using device redundancy and/or interface redundancy.

4.6 System documentation requirements

(See 10.12.3.1)

Where the information required is deemed confidential the manufacture may take measures to control access to such information.

A system integrator of a 460-Network shall provide documentation of the network topology and its functions and devices. This includes:

- short description of each device within the 460-Network including brief functional description and technical features;
- block diagram(s) indicating the physical and logical connections between the equipment in the 460 network and their interactions with connected networks and devices;

- equipment or network connection points which may be disconnected manually or automatically in order to isolate the 460 Network from other networks or network segments.

A system integrator of a 460-Network shall provide documentation showing that the 460-network includes only equipment listed in 4.3.2.

See also 5.4.

4.7 Secure area requirements

(See 10.12.3.1)

The 460-Switch and 460-Forwarder may support disabling MAC address authorisation requirements in secure areas as described in 6.2.4.2.

The documentation for the 460-Switch and 460-Forwarder shall include the description of the secure area and the description of the features which can be relaxed when installed in the secure area.

5 Network traffic management requirements

5.1 460-Node requirements

(See 10.5.1)

The 460-Node shall comply with the following to satisfy network traffic management requirements:

- all traffic shall be specified as one of the IEC 61162-450 compliant data types, for example IEC 61162-1 sentence transmission, binary file traffic or ONF;

NOTE 1 Chart update is an example of ONF.

- the maximum operational data output for a device shall be declared by the manufacturer in bytes per second averaged over a specified period of time;

NOTE 2 The specified period of time depends on the characteristics of the data output and is chosen to be appropriate for network traffic management purposes.

- device behaviour shall be specified by the manufacturer when its maximum input data rate is exceeded. The input data rate shall be expressed in bytes per second as available in the network line including all protocol-specific overheads;
- only data specified by the relevant standards or by the manufacturer for the node shall be processed by the node;
- devices shall continue normal operation with an input loss rate of packets up to 0,1 % per second over a time period of 10 min.

NOTE 3 Normal operation includes the ability to survive even when something is lost in interfaces. Normal reaction to such losses is either to continue as if nothing has been lost (i.e. there has been sufficient information available to continue without any effect) or to generate an indication and/or alert based on the loss.

If VLAN is provided, all VLAN traffic shall be included in the maximum transmission rate.

NOTE 4 For example, VLAN is used to create a separate segment.

5.2 460-Switch requirements

5.2.1 Resource allocation

(See 10.6.1)

The following are required for resource allocation:

- a) means to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and port number or range of port numbers. The source may be from any source or range of sources or group of sources, etc. The destination may be to any destination or range of destinations or group of destinations, etc.;
- b) a stream or network flow only to be permitted to interfaces with configured MAC or IP-addresses for specified protocols and ports where network bandwidth limits are applied (see bullet e)). All other traffic shall be blocked;

NOTE This approach is sometimes described as deny all, permit by exception.

- c) means to allocate network bandwidth resource for each stream or network flow;
- d) the amount of bandwidth allocated at a 460-Switch shall be more than the sum of all normal traffic volumes of each traffic class allocated to the network connected to the switch;
- e) the total amount of traffic per interface to a 450-Node or 460-Node shall be limited to the appropriate bandwidth as a proportion of the switch's or connected node's overall capacity so that the capacity of the switch or node is not exceeded by the traffic allocated to all ports;
- f) if VLAN is provided, a means to configure virtual networks (VLAN) per interface shall be provided;
- g) if VLAN is provided, VLAN protocol IEEE 802.1Q shall be supported;
- h) means to filter multicast traffic by IGMP snooping as required by IEC 61162-450;
- i) means to send IGMP membership queries to other 460-Switches, 460-Forwarders, 460-Nodes and 450-Nodes.

5.2.2 Loop prevention

(See 10.6.2)

The switch shall provide a loop prevention mechanism, for example, RSTP, MSTP. Network topology and switch configuration shall support its convergence within 5 s.

NOTE When there is a loop in a network, the traffic is never terminated. This increases the network traffic significantly. This problem becomes severe when multicasting traffic is multiplied by a switch. A network loop can be caused by network misconfiguration. Also, it is caused when there are multiple paths to the destination by the network topology (i.e. mesh network topology) or network redundancy.

The following are the RSTP requirements, if provided:

- RSTP protocol version IEEE 802.1D-2004 shall be supported;
- a 460-Switch shall support RSTP on each of its interfaces.

5.3 460-Forwarder requirements

5.3.1 Traffic separation

(See 10.7.1)

The following are required for traffic separation:

- means to configure transmitting all or a subset of the traffic;
- means to configure for a maximum traffic flow;
- if VLAN provided, a means to configure virtual networks (VLAN) per each interface;
- if VLAN provided, VLAN protocol IEEE 802.1Q shall be supported.
- means to filter multicast traffic IGMP snooping as required by IEC 61162-450;

- means to send IGMP membership queries to other 460-Switches, 460-Forwarders, 460-Nodes and 450-Nodes.

5.3.2 Resource allocation

(See 10.7.2)

The following are required for resource allocation:

- the 460-Forwarder shall have a capacity more than the summation of all traffic volumes of each traffic class allocated to the network connected to the forwarder;
- the 460-Forwarder shall be configurable for a maximum traffic flow;
- firewall functionality shall be provided as means to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and port number. The source may be from any source or range of sources or group of sources, etc. The destination may be to any destination or range of destinations or group of destinations, etc. All connections between networks shall be registered (i.e. all network traffic that does not match a set firewall rule shall be blocked by the firewall);
- a means shall be provided to allocate network resource for all registered streams;
- a means shall be provided to allocate resource for each virtual network if provided.

5.3.3 Traffic prioritization

(See 10.7.3)

All or part of the traffic may be prioritized to control transfer of traffic from one 460-Network to controlled networks. By default all traffic shall have a value of zero for the default priority. The prioritization may be provided by either IP DSCP (Differentiated Service Code Point) or CoS (Class of Service) in VLAN if provided. There are eight priorities where zero (=000) is the lowest and seven (=111) is the highest.

The priority of each packet is provided based on the traffic type. The priority information is given in the precedence of IP DSCP field or CoS field. Table 1 is an example of the relationship between traffic types and traffic prioritization specified in IP DSCP and CoS in VLAN.

Table 1 – Traffic prioritization with CoS and DSCP

CoS Value	DSCP value	Traffic type based on IEC 61162-450
000	000000	Data provided by ONF except network control and management traffic
001	001000	PROP, USR1 to USR8
010	010000	MISC, simple binary image
011	011000	VDRD, TIME
100	100000	RCOM, retransmittable binary image
101	101000	TGTD, SATD, NAVD
110	110000	Reserved
111	111000	Network control and management traffic

The following means shall be provided for traffic prioritisation at a 460-Forwarder:

- a) means to handle dropping of lower priority traffic based on priority;
- b) means to handle dropping if the amount of traffic to be transferred per each physical port is higher than 50 % of physical capacity of the line or is over the set maximum input data rate capacity of the 460-Node or 450-Node. The traffic prioritisation shall be used to drop the

lower priority traffic until the traffic is below 50 % of physical capacity of the line or is below the set maximum input data rate capacity of the 460-Node or 450-Node;

NOTE 1 An example of means to handle dropping is a setup method in which amount of traffic of different priorities can be assigned.

- c) means to continue lossless traffic in each priority until the amount of traffic to be transferred is higher than 100 % of the set maximum as set for the priority in the switch;
- d) means to report the use of dropping by syslog for each period of 30 s during which the dropping has been used or by responding to SNMP-Trap method (i.e. by requesting RMON alerts) about the use of dropping (see 8.2.2).

NOTE 2 For example, network monitoring function using SNMP-Trap method queries to 460-Forwarder about the use of dropping.

5.4 System design requirements

5.4.1 Documentation

(See 10.12.3.2)

For a system intended to be compliant with this standard, documents shall be provided which include information from the following list. For an individual equipment the manufacturer's documentation shall provide appropriate information:

- where applicable, backup and recovery procedures including controls to ensure integrity and confidentiality of externalized data. Where certain parts are not applicable, this shall be clearly stated in the documentation;
- where applicable, physical layout of the network infrastructure components, nodes and network access points;
- where applicable, description of the features of each network segment in the system;
- where applicable, 460-Network traffic flow analysis and network topology information including connected networks, MAC addresses and IP address ranges or other appropriate identifiers;
- documents that specify the total amount of network traffic of every switch and between switches, forwarders and gateways and the average load of all traffic for the 460-Network;
- the maximum traffic flow transferred from one 460-Network to another 460-Network at each 460-Forwarder;
- the prioritization of each traffic type at each 460-Forwarder.

NOTE Information can be collected from the network monitoring function, see 8.2.4.

See also 4.6.

5.4.2 Traffic

(See 10.12.3.3)

System design for 460-Networks shall comply with the following requirements:

- the maximum designed network load shall not exceed the nominal network capacity;
- the average load of all traffic in a 460-Network shall not exceed 95 % of nominal network capacity planned over a period of 1 s and shall not exceed 80 % of nominal network capacity planned over a period of 10 s.

5.4.3 Connections between secure and non-secure areas

(See 10.12.3.9)

The connection between a 460-Network installed in a secure area and a 460-Network installed in a non-secure area shall be established by using a 460-Forwarder (see Figure 1).

6 Security requirements

6.1 Security scenarios

6.1.1 Threat scenarios

As shown in the example of network topology illustrated in Figure 1, 460-Networks are threatened internally by 450-Nodes and externally from uncontrolled networks such as other shipborne equipment or off-ship equipment. Therefore, 460-Networks are required to be protected not only from internal threats but also from external threats.

6.1.2 Internal threats

The following are scenarios that can occur in networks:

- malware replication from other equipment in a 460-Network such as a notebook that is infected by the malware;
- infection from corrupted mass storage devices (e.g. USB flash drive) or removable media drives (CD/DVD) being used within the 460-Network, for example in connection with (authorised or unauthorised) maintenance and support;
- installation of a backdoor in one of the equipment to get system privilege through it; other equipment is then attacked;
- deletion of the system file(s) or change of the configuration file(s) by mistake (misoperation);
- illicit access that prohibits the normal operation of equipment;
- false data generation that prohibits the normal operation of equipment;
- security threats in controlled networks which are easily propagated into 460-Networks;
- security threats in other 460-Networks which are easily propagated into 460-Networks;
- interruption of network service due to the heavy volume of broadcasting traffic and of ICMP and IGMP packets.

Requirements for security against internal threats are described in 6.2.

6.1.3 External threats

The following are scenarios that are caused from external networks:

- threats from unsecure networks;
- infection of a piece of equipment in the 460-Network by a malware in other shipborne networks;
- remote log-in to equipment in a 460-Network by a user in a shipborne network, which deletes important files or changes the configuration by mistake (misoperation);
- installation of a backdoor by shipborne equipment to use it as an attack agent; direct attack to equipment through the network infrastructure such as switch or router;
- scanning attack – attacker finds a port for attack by scanning the ports first. If found, it scans the service with the port. For example, when port number 80 is open for the web service, the attacker collects the information of web server type and version;
- in-direct attack to the 460-Network via uncontrolled networks such as another shipborne network;
- data sniffing and modification attack during the communication with external equipment and systems – When equipment in a 460-Network communicates with off-ship network systems,

the attack extracts and modifies data by sniffing. For example, the navigational route information may be exposed to and be modified by pirates and terrorists;

- incoming excessive data traffic to 460-Networks and protocol features attack including SYN flooding attack.

Requirements for security against external threats are described in 6.2.5.

6.2 Internal security requirements

6.2.1 General

(See 10.5.2.1, 10.6.3.1, 10.7.4.1)

A 460-Node, 460-Switch and 460-Forwarder shall not use a wireless LAN interface and wireless access point (AP) functions.

All VLAN tunnelling protocols used between 460-Networks and uncontrolled networks shall be disabled in a 460-Node, 460-Switch and 460-Forwarder.

6.2.2 Denial of service protection

6.2.2.1 460-Node

(See 10.5.2.2)

The maximum operational input and output bandwidth for a device shall be declared by the manufacturer averaged over a specified time period.

Means shall be provided to ensure normal operation of the functionality not dependent on the incoming traffic of the node under excessive incoming traffic received at its Ethernet port.

Means shall be provided to ensure normal operation of the node following a period of excessive incoming traffic received at its Ethernet port.

6.2.2.2 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

(See 10.6.3.2, 10.7.4.2, 10.8.1)

Protection from DoS attacks using ICMP and IGMP protocols shall be provided. Additional DoS prevention methods may be provided.

NOTE Resource allocation requirements for 460-Switch, see 5.2.1, assist network nodes in DoS protection.

6.2.3 REDS security

(See 10.5.2.3)

6.2.3.1 General

Protection for REDS shall be provided by physical and/or operational means.

The operator's manual shall include guidance that procedures and processes should be established to ensure that REDS have been checked for malware prior to being connected in an equipment of the 460-Network.

6.2.3.2 Physical protection

The number of connection points for REDS (for example keyboard/mice ports, printer ports, USB ports, Secure Digital (SD)-cards, disc drives, (hot swappable) drive bays, etc.) shall be

limited to the minimum required for the operation of the system and its lifetime maintenance and support. An exception is USB ports providing only the functionality of charging. All other points shall either:

- be physically blocked from easy access by a user without a tool or key, for example, by port blocker, or;
- be subject to an instruction in the manufacturer's installation manual that the equipment shall only be installed in a closed console or cabinet requiring additional tools or keys to open; the manufacturer's installation manual shall include a notice of cyber security risk if not installed as described by the manufacturer.

Attention should be given to wireless interfaces where physical protection provides security in normal operation in order to ensure that the interface is indeed protected against access by personnel with physical access to the equipment. For example, this might be achieved by fitting a terminator to an antenna interface used only during commissioning and maintenance, that is internal to the equipment or requires a tool or key to remove.

6.2.3.3 Operational protection

Interfaces for removable devices (for example storage, keyboards, printers, etc.) as required for operation and lifecycle maintenance shall be minimized and restricted by one or more of the alternatives listed below:

- logical blocking (i.e. software or firmware or operating system) of the interface. For example, blocking of all connection points for REDS (in particular USB and SD ports) and allow unblocking only in administrator or maintenance mode;
- preventing device drivers from installing; this means that the device drivers can only be installed in maintenance mode;
- cryptographic authentication with a security strength of at least 128 bits prior to use of any content or functionality from USB devices;
- restriction of the interface to specific USB device classes (see Annex G);
- restriction of the interface to a specific hardware identifier (i.e. same model of equipment);
- restriction of the interface to specific instance identifiers (i.e. individual equipment).

For any removable device which cannot practically be restricted using the options detailed above, the manufacturer shall provide information about how the interface has been limited to its intended functionality and protected against misuse.

NOTE For example, non-network wireless interfaces such as certain types of Bluetooth devices can use a password or key to authenticate the removable device with the equipment it connects to and use encryption to provide confidentiality and integrity for data transferred wirelessly.

Physical port blockers can be used as an appropriate measure to avoid any unauthorized devices being plugged into the system. This will ensure that an additional security mechanism is installed to protect operations (see 6.2.3.2).

6.2.3.4 Executable program file verification

See 6.2.5.2.

6.2.3.5 Non-executable data verification

See 6.2.5.3.

6.2.4 Access control

6.2.4.1 Device access control

(See 10.5.2.4, 10.6.3.3, 10.7.4.3, 10.8.2)

Access to make changes in the configuration of 460-Node, 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway equipment shall be subject to user authentication.

Any user, program or process allowed to access the device shall only have the minimum privilege necessary to perform its function.

NOTE 1 For example, the user level required to run applications or processes on the equipment is not assigned admin privileges, but only the minimum privileges required for the operation of the applications or processes.

NOTE 2 In some cases, a process has to initially run with elevated privileges before losing those privileges. For example, on some operating systems, to bind to a privileged port a process has to run with elevated privileges then it can immediately switch to running as an unprivileged user. In some cases, the function of a process means that it is necessary for the process to run with elevated privileges.

If, based on the manufacturer's documentation, the equipment provides different levels of authorization, the manufacturer's documentation shall include guidance on how to implement the principle of least privilege for the lifecycle of the equipment. This will typically require the equipment to provide the capability to withdraw permission from entities such as users or processes that are then no longer able to access the equipment or subsets of its functionality. Manufacturer's documentation shall describe pre-emptive procedures of the manufacturer that prevents employees from accumulating excessive permissions over time.

User authentication shall be provided with log-in information. The following is required for the device access control process:

- a user authentication mechanism shall be provided before changing the device settings. Some examples of authentication include passwords and key cards;
- if a password is required at login, it shall be provided with at least 8 characters. Longer passwords and other authentication tokens like RSA keys, etc. may be supported where possible;
- if asymmetric cryptography is used, for example in smart cards, the security strength of the cipher shall be at least 112 bits;
- the operator's manual shall include guidance such as "passwords should not contain the user name or parts of the user's full name, such as his first name, company name, product name, etc", "dictionary words should not be used", "repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd') should not be used", "random and meaningless passwords should be used";
- additional password restrictions may be enforced at the manufacturer's discretion, including length, character complexity, periodic changes and excluded word lists.

NOTE 3 NIST SP 800-63B recommends a password length of at least 8 characters and no specific requirements on complexity (mix of letters, symbols, and figures) because highly complex memorized secrets introduce a new potential vulnerability, for example password written on paper.

6.2.4.2 Network access control

(See 10.6.3.4, 10.7.4.4)

In normal operation unused network connection points to the 460-Network shall be protected by one or more of the alternatives listed below:

- be logically blocked (i.e. software or firmware or operating system) of the interface; or;
- be physically blocked from easy access by a user without a tool or key; or
- be subject to an instruction in the manufacturer's installation manual that the equipment shall only be installed in a closed console or cabinet requiring additional tools or keys to open; the manufacturer's installation manual shall include a notice of cyber security risk if not installed as described by the manufacturer.