



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 EN IEC 61162-460:2018+A1:2020. It is identical to IEC 61162-460:2018, incorporating amendment 1:2020. It supersedes BS EN IEC 61162-460:2018, which will be withdrawn on 24 February 2023.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by **A1** **A1**.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 03274 1

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 August 2018.

Amendments/corrigenda issued since publication

Date	Text affected
30 April 2020	Implementation of IEC amendment 1:2020 with CENELEC endorsement A1:2020

English Version

Maritime navigation and radiocommunication equipment and
systems - Digital interfaces - Part 460: Multiple talkers and
multiple listeners - Ethernet interconnection - Safety and security
(IEC 61162-460:2018)

Matériels et systèmes de navigation et de
radiocommunication maritimes - Interfaces numériques -
Partie 460: Émetteurs multiples et récepteurs multiples -
Interconnexion Ethernet - Sécurité et sécurité
(IEC 61162-460:2018)

Navigations- und Funkkommunikationsgeräte und -systeme
für die Seeschifffahrt - Digitale Schnittstellen - Teil 460:
Mehrere Datensender und mehrere Datenempfänger -
Ethernet-Verbund - Funktionale und Informationssicherheit
(IEC 61162-460:2018)

This European Standard was approved by CENELEC on 2018-06-08. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 80/879/FDIS, future edition 2 of IEC 61162-460, prepared by IEC/TC 80 "Maritime navigation and radiocommunication equipment and systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61162-460:2018.

The following dates are fixed:

- latest date by which the document has to be (dop) 2019-03-08
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2021-06-08
standards conflicting with the
document have to be withdrawn

This document supersedes EN 61162-460:2015.

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

Endorsement notice

The text of the International Standard IEC 61162-460:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60812	NOTE	Harmonized as EN 60812.
IEC 61162 Series	NOTE	Harmonized as EN 61162 Series.
IEC 61162-1	NOTE	Harmonized as EN 61162-1.
IEC 61162-2	NOTE	Harmonized as EN 61162-2.
IEC 62388	NOTE	Harmonized as EN 62388.
IEC 62439 Series	NOTE	Harmonized as EN 62439 Series.
IEC 62439-1	NOTE	Harmonized as EN 62439-1.
IEC 62439-2	NOTE	Harmonized as EN 62439-2.
IEC 62439-3	NOTE	Harmonized as EN 62439-3.
IEC 62439-4	NOTE	Harmonized as EN 62439-4.
IEC 62439-5	NOTE	Harmonized as EN 62439-5.
IEC 62439-6	NOTE	Harmonized as EN 62439-6.
IEC 62940	NOTE	Harmonized as EN 62940.
ISO 9241-12	NOTE	Harmonized as EN ISO 9241-12 ¹ .

¹ Superseded by EN ISO 9241-112 (ISO 9241-112) and EN ISO 9241-125 (ISO 9241-125).

Foreword to amendment A1

The text of document 80/943/FDIS, future IEC 61162-460/A1, prepared by IEC/TC 80 "Maritime navigation and radiocommunication equipment and systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61162-460:2018/A1:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-11-24
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-02-24

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

Endorsement notice

The text of the International Standard IEC 61162-460:2018/A1:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61924-2:2012	NOTE	Harmonized as EN 61924-2:2013 (not modified)
IEC 62288:2014	NOTE	Harmonized as EN 62288:2014 (not modified)

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60945	-	Maritime navigation and radiocommunication equipment and systems - General requirements - Methods of testing and required test results	EN 60945	-
IEC 61162-460	2018	Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security	EN IEC 61162-460	2018
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	EN IEC 62923-1	-
IEC 62923-2	-	Maritime navigation and radiocommunication equipment and systems - Bridge alert management - Part 2: Alert and cluster identifiers and other additional features	EN IEC 62923-2	-
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 - Bridges and Bridged Networks	-	-

CONTENTS

FOREWORD	6
Introduction to the Amendment	8
1 Scope	9
2 Normative references	9
3 Terms and definitions	10
4 High-level requirements	16
4.1 Overview	16
4.2 Description	16
4.3 General requirements	17
4.3.1 Equipment and system requirements	17
4.3.2 Physical composition requirements	17
4.3.3 Logical composition requirements	17
4.4 Physical component requirements	18
4.4.1 450-Node	18
4.4.2 460-Node	18
4.4.3 460-Switch	18
4.4.4 460-Forwarder	19
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	19
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	21
5.3.3 Traffic prioritization	22
5.4 System design requirements	22
5.4.1 Documentation	22
5.4.2 Traffic	23
5.4.3 Connections between secure and non-secure areas	23
6 Security requirements	23
6.1 Security scenarios	23
6.1.1 Threat scenarios	23
6.1.2 Internal threats	23
6.1.3 External threats	24
6.2 Internal security requirements	24
6.2.1 General	24
6.2.2 Denial of service protection	24
6.2.3 REDS security	25
6.2.4 Access control	25

6.3	External security requirements	26
6.3.1	Overview	26
6.3.2	Firewalls	27
6.3.3	Direct communication	27
6.3.4	460-Node	27
6.3.5	460-Gateway	28
6.3.6	460-Wireless gateway	29
6.4	Additional security issues	29
7	Redundancy requirements	30
7.1	General requirements	30
7.1.1	General	30
7.1.2	Interface redundancy	30
7.1.3	Device redundancy	31
7.2	460-Node requirements	31
7.3	460-Switch requirements	31
7.4	460-Forwarder requirements	31
7.5	460-Gateway and 460-Wireless gateway requirements	31
7.6	Network monitoring function requirements	31
7.7	System design requirements	31
8	Network monitoring requirements	32
8.1	Network status monitoring	32
8.1.1	460-Network	32
8.1.2	460-Node	32
8.1.3	460-Switch	32
8.1.4	460-Forwarder	32
8.2	Network monitoring function	33
8.2.1	General	33
8.2.2	Network load monitoring function	34
8.2.3	Redundancy monitoring function	34
8.2.4	Network topology monitoring function	35
8.2.5	Syslog recording function	36
8.2.6	Redundancy of network monitoring function	36
8.2.7	Alert management	36
9	Controlled network requirements	38
10	Methods of testing and required test results	38
10.1	Subject of tests	38
10.2	Test site	38
10.3	General requirements	39
10.4	450-Node	39
10.5	460-Node	40
10.5.1	Network traffic management	40
10.5.2	Security	40
10.5.3	Redundancy	42
10.5.4	Monitoring	42
10.6	460-Switch	42
10.6.1	Resource allocation	42
10.6.2	Loop prevention	43
10.6.3	Security	43

10.6.4	Monitoring	44
10.7	460-Forwarder	45
10.7.1	Traffic separation.....	45
10.7.2	Resource allocation	45
10.7.3	Traffic prioritisation.....	46
10.7.4	Security	46
10.7.5	Monitoring	47
10.8	460-Gateway	48
10.8.1	Denial of service behaviour.....	48
10.8.2	Access control to configuration setup.....	48
10.8.3	Communication security.....	48
10.8.4	Firewall.....	49
10.8.5	Application server	50
10.8.6	Interoperable access to file storage of DMZ.....	50
10.8.7	Additional security	50
10.9	460-Wireless gateway.....	51
10.9.1	General	51
10.9.2	Security	51
10.10	Controlled network.....	51
10.11	Network monitoring function.....	51
10.11.1	General	51
10.11.2	Network load monitoring function.....	52
10.11.3	Redundancy monitoring function.....	52
10.11.4	Network topology monitoring function	53
10.11.5	Syslog recording function	53
10.11.6	Alert management	53
10.12	System level	55
10.12.1	General	55
10.12.2	System management function	55
10.12.3	System design	56
10.12.4	Network monitoring function	57
10.12.5	Network load monitoring function.....	57
10.12.6	Redundancy monitoring function.....	57
10.12.7	Network topology monitoring function	58
Annex A (informative) Communication scenarios between an IEC 61162-460 network and uncontrolled networks		59
A.1	General.....	59
A.2	Routine off-ship	59
A.3	Routine on-ship.....	60
A.4	460-Gateway usage for direct connection with equipment	60
Annex B (informative) Summary of redundancy protocols in IEC 62439 (all parts).....		61
Annex C (informative) Guidance for testing.....		62
C.1	Methods of test	62
C.2	Observation	62
C.3	Inspection of documented evidence	62
C.4	Measurement.....	62
C.5	Analytical evaluation	63
Annex D (informative) Some examples to use this document		64
Annex E (normative) IEC 61162 interfaces for the network monitoring function.....		68

Annex F (informative) Distribution of functions around 460-Network.....	69
Bibliography.....	71
Figure 1 – Functional overview of IEC 61162-460 requirement applications	16
Figure 2 – 460-Network with 460-Gateway.....	26
Figure 3 –Example of redundancy.....	30
Figure 4 – Example of network status recording information	34
Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks	59
Figure D.1 – 460-Forwarder used between two networks	64
Figure D.2 – 460-Forwarder used between two networks	64
Figure D.3 – 460-Gateway used for e-Navigation services	65
Figure D.4 – 460-Gateway used for remote maintenance	65
Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices	66
Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices	67
Figure E.1 – Network monitoring function logical interfaces	68
Table 1 – Traffic prioritization with CoS and DSCP	22
Table 2 – Summary of alert of network monitoring	37
Table B.1 – Redundancy protocols and recovery times	61
Table E.1 – Sentences received by the network monitoring function	68
Table E.2 – Sentences transmitted by the network monitoring function	68
Table F.1 – Distribution of functions around 460-Network	69
Table F.2 – Equipment standards referencing IEC 61162-460	70

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

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

This second edition of IEC 61162-460 cancels and replaces the first edition published in 2015. This edition constitutes a technical revision.

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

- a) 460-Switches and 460-Forwarders are required to implement IGMP snooping;
- b) connection between secure and non-secure areas requires a 460-Forwarder as an isolation element;

- c) SFI collision detection added as function of network monitoring;
- d) 460-Gateway and 460-Wireless gateway are no longer required to report to the network monitoring;
- e) all alerts from network monitoring have standardized alert identifiers.

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

FDIS	Report on voting
80/879/FDIS	80/884/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

This International Standard is to be used in conjunction with IEC 61162-450:2018.

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 "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.

Introduction to the Amendment

This amendment provides greater clarity to the external security requirements in 6.3, updates the alert management in 8.2.7 and associated tests in 10.11.6 to comply with bridge alert management and provides an improved test of firewalls in 10.8.4.

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 61162-450:2018, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*

 Text deleted 

 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*

INTERNET SOCIETY (ISOC). RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)* [online]. Edited by J. Postel. September 1981 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc792>

INTERNET SOCIETY (ISOC). RFC 1112, *Host Extensions for IP Multicasting* [online]. Edited by S. Deering. August 1989 [viewed 2018-01-08]. Available at <https://www.ietf.org/rfc/rfc1112.txt>

INTERNET SOCIETY (ISOC). RFC 1157, *A Simple Network Management Protocol (SNMP)* [online]. Edited by J. Case et al. May 1990 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc1157>

INTERNET SOCIETY (ISOC). RFC 2021, *Remote Network Monitoring Management Information Base* [online]. Edited by S. Waldbusser. January 1997 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2021>

INTERNET SOCIETY (ISOC). RFC 2236, *Internet Group Management Protocol, Version 2* [online]. Edited by W. Fenner. November 1997 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2236>

INTERNET SOCIETY (ISOC). RFC 2819, *Remote Network Monitoring Management Information Base* [online]. Edited by S. Waldbusser. May 2000 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2819>

INTERNET SOCIETY (ISOC). RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* [online]. Edited by D. Harrington. December 2002 [viewed 2018-01-08]. Available at <https://www.ietf.org/rfc/rfc3411.txt>

INTERNET SOCIETY (ISOC). RFC 3577, *Introduction to the RMON family of MIB modules* [online]. Edited by S. Waldbusser. August 2003 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc3577>

INTERNET SOCIETY (ISOC). RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast* [online]. Edited by H. Holbrook et al. August 2006 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc4604>

INTERNET SOCIETY (ISOC). RFC 5424, *The Syslog Protocol* [online]. Edited by R. Gerhards. March 2009 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc5424>

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61162-450 and the following apply.

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://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 safely exchange data streams between a 460-Network and other controlled networks including other 460-Networks

3.3

460-Gateway

network infrastructure device that connects 460-Networks and uncontrolled 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

highest priority of an alert, announcing a situation or condition requiring immediate attention, decision and, if necessary, action by the bridge team, to maintain the safe navigation of the ship

3.10

application level gateway

network infrastructure device that connects 460-Networks with other networks and which satisfies the safety and security requirements as specified in this document

3.11

backdoor

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

3.12

controlled network

any 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 IEC 61162-450 compliant network that is approved by classification society, flag state or recognized organization (RO).

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

3.14

caution

lowest priority of an alert

Note 1 to entry: "Caution" raises a bridge team's 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.

3.15

demilitarized zone

DMZ

physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and un-trusted 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

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

3.19

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.

3.20

internet control message protocol

ICMP

protocol according to ISOC RFC 792

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

3.21

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.

3.22

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.

3.23

malware

malicious code

software used or created to disrupt computer operation

3.24

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).

3.25

maximum transmission rate

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

3.26

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.

3.27

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)

3.28

network infrastructure component

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

3.29

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.

3.30

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.

3.31
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.

3.32
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.

3.33
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.

3.34
ring topology

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

3.35
RSA

public-key cryptosystem as described in IEEE 1363

3.36
safety

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

3.37
secure area

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

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

3.38
security

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

3.39
simple network management protocol
SNMP

protocol according to ISOC RFC 3411 used to convey management information

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

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

SNMP-Trap

method to collect events and statistical information from switches, according to ISOC RFC 1157, ISOC RFC 2021 and ISOC RFC 2819

3.41

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.

3.42

sniffing

monitoring and analysis of the network traffic

3.43

stream

combination of all flows from a device that use same protocol

3.44

syslog

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

3.45

system integrator

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

3.46

threat

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

3.47

traffic

combination of all streams from a device

3.48

uncontrolled network

data network that is not an IEC 61162-450 compliant network, an IEC 61162-460 compliant network or a controlled network

EXAMPLE Wireless networks.

3.49

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.

3.50

virtual private network

VPN

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.

3.51

warning

announcement of a situation or condition requiring attention but no immediate attention or 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 forward-looking decision is made or action is taken.

3.52

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

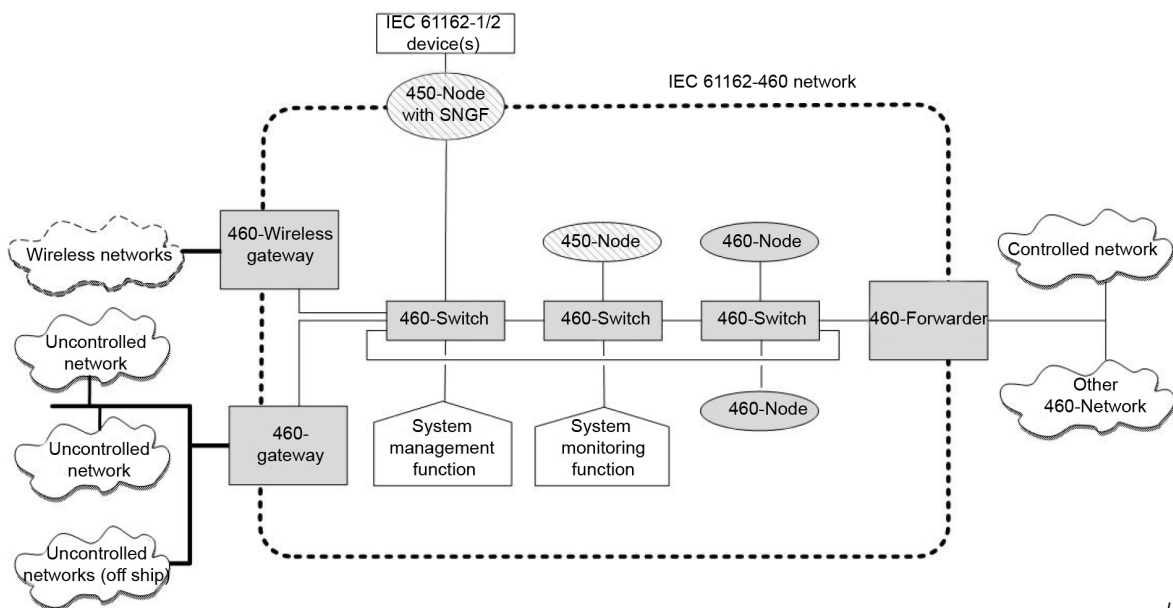
4.1 Overview

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 network implementing the requirements of this document on different parts and components of the network. 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 requirement 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 to 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 61162-450:2018.

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.

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;
- application level gateways 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 61162-450:2018, 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;
- ephemeral ports, if used, indicated by the manufacturer.

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 if used indicated by the manufacturer.

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;
- VLAN compatibility, if provided, as specified in 5.2.1.

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;
- 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, 6.3 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;
- SFI collision detection as specified in 8.2.4.2.

4.5.2 System management function

(See 10.12.2)

The system management function shall perform the following functions:

- 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 either automatically or manually 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 system management function shall be redundantly available.

4.6 System documentation requirements

(See 10.12.3.1)

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

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)