IEC 61162-460

Edition 3.0 2024-04
COMMENTED VERSION

INTERNATIONAL STANDARD

colour inside

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



IEC 61162-460:2024-04 CMV(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC 61162-460

Edition 3.0 2024-04
COMMENTED VERSION

INTERNATIONAL STANDARD

colour inside

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 978-2-8322-8715-6

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 6
~~Introduction to the Amendment~~ .....
1 Scope 10
2 Normative references 10
3 Terms and definitions 11
4 High-level requirements 18
4.1 Overview 18
4.2 Description 18
4.3 General requirements 19
4.3.1 Equipment and system requirements 19
4.3.2 Physical composition requirements 20
4.3.3 Logical composition requirements 20
4.4 Physical component requirements 20
4.4.1 450-Node 20
4.4.2 460-Node 20
4.4.3 460-Switch 21
4.4.4 460-Forwarder 21
4.4.5 460-Gateway and 460-Wireless gateway 21
4.5 Logical component requirements 21
4.5.1 Network monitoring function 21
4.5.2 System management function 22
4.6 System documentation requirements 22
4.7 Secure area requirements 22
5 Network traffic management requirements 23
5.1 460-Node requirements 23
5.2 460-Switch requirements 23
5.2.1 Resource allocation 23
5.2.2 Loop prevention 24
5.3 460-Forwarder requirements 24
5.3.1 Traffic separation 24
5.3.2 Resource allocation 24
5.3.3 Traffic prioritization 25
5.4 System design requirements 26
5.4.1 Documentation 26
5.4.2 Traffic 26
5.4.3 Connections between secure and non-secure areas 26
6 Security requirements 26
6.1 Security scenarios 26
6.1.1 Threat scenarios 26
6.1.2 Internal threats 27
6.1.3 External threats 27
6.2 Internal security requirements 27
6.2.1 General 27
6.2.2 Denial of service protection 28
6.2.3 REDS security 28
6.2.4 Access control 30

6.2.5 Executable and non-executable file security 31
6.2.6 Recording of device management activities 32
6.3 External security requirements 33
6.3.1 Overview 33
6.3.2 Firewalls 34
6.3.3 Direct communication 34
6.3.4 ~~460-Node~~ Node requirements for direct communication n 36
6.3.5 460-Gateway 37
6.3.6 460-Wireless gateway 39
6.4 Additional security issues 39
6.5 Onboard software maintenance 40
6.5.1 General 40
6.5.2 Roll back to previous safe configuration 41
6.5.3 Software maintenance in maintenance mode 41
6.5.4 Semi-automatic software maintenance by the crew onboard the vessel 41
6.5.5 Remote software maintenance 42
6.6 Secure software lifecycle management 43
7 Redundancy requirements 43
7.1 General requirements 43
7.1.1 General 43
7.1.2 Interface redundancy 44
7.1.3 Device redundancy 44
7.2 460-Node requirements 44
7.3 460-Switch requirements 45
7.4 460-Forwarder requirements 45
7.5 460-Gateway and 460-Wireless gateway requirements 45
7.6 Network monitoring function requirements 45
7.7 System design requirements 45
8 Network monitoring requirements 45
8.1 Network status monitoring 45
8.1.1 460-Network 45
8.1.2 460-Node 45
8.1.3 460-Switch 46
8.1.4 460-Forwarder 46
8.2 Network monitoring function 47
8.2.1 General 47
8.2.2 Network load monitoring function 48
8.2.3 Redundancy monitoring function 49
8.2.4 Network topology monitoring function 49
8.2.5 Syslog recording function 52
8.2.6 Redundancy of network monitoring function 53
8.2.7 Alert management 53
9 Controlled network requirements 54
10 Methods of testing and required test results 55
10.1 Subject of tests 55
10.2 Test site 55
10.3 General requirements 56
10.4 450-Node 56

10.5 460-Node 56
10.5.1 Network traffic management 56
10.5.2 Security 57
10.5.3 Redundancy 61
10.5.4 Monitoring 61
10.6 460-Switch 61
10.6.1 Resource allocation 61
10.6.2 Loop prevention 62
10.6.3 Security 62
10.6.4 Monitoring 66
10.7 460-Forwarder 66
10.7.1 Traffic separation 66
10.7.2 Resource allocation 67
10.7.3 Traffic prioritisation 67
10.7.4 Security 67
10.7.5 Monitoring 69
10.8 460-Gateway 69
10.8.1 Denial of service behaviour 69
10.8.2 Access control to configuration setup 69
10.8.3 Communication security 70
10.8.4 Firewall 70
10.8.5 Application ~~server~~ services 72
10.8.6 Interoperable access to file storage of DMZ 72
10.8.7 Additional security 72
10.9 460-Wireless gateway 73
10.9.1 General 73
10.9.2 Security 73
10.10 Controlled network 73
10.11 Network monitoring function 74
10.11.1 General 74
10.11.2 Network load monitoring function 74
10.11.3 Redundancy monitoring function 74
10.11.4 Network topology monitoring function 75
10.11.5 Syslog recording function 75
10.11.6 Alert management 76
10.12 System level 77
10.12.1 General 77
10.12.2 System management function 78
10.12.3 System design 78
10.12.4 Network monitoring function 80
10.12.5 Network load monitoring function 80
10.12.6 Redundancy monitoring function 80
10.12.7 Network topology monitoring function 80
Annex A (informative) Communication scenarios between an IEC 61162-460 network and uncontrolled networks 81
A.1 General 81
A.2 Routine off-ship 81
A.3 Routine on-ship 82
A.4 460-Gateway usage for direct connection with equipment 82

Annex B (informative) Summary of redundancy protocols in IEC 62439 (all parts) 83
Annex C (informative) Guidance for testing 84
C.1 Methods of test.....84
C.2 Observation.....84
C.3 Inspection of documented evidence.....84
C.4 Measurement 84
C.5 Analytical evaluation.....85
Annex D (informative) Some examples to use this document 86
Annex E (normative) IEC 61162 interfaces for the network monitoring function.....90
Annex F (informative) Distribution of functions around 460-Network.....91
Annex G (normative) USB class codes.....93
Annex H (informative) Cross reference between IACS UR E26/E27 and IEC 61162-460.....94
Bibliography.....97
List of comments.....99

Figure 1 – Functional overview of IEC 61162-460 ~~requirement~~ applications.....19
Figure 2 – 460-Network with 460-Gateway 34
Figure 3 – Example of redundancy.....44
Figure 4 – Example of network status recording information 48
Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks 81
Figure D.1 – 460-Forwarder used between two networks.....86
Figure D.2 – 460-Forwarder used between two networks.....86
Figure D.3 – 460-Gateway used for e-Navigation services 87
Figure D.4 – 460-Gateway used for remote maintenance.....87
Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices 88
Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices 89
Figure E.1 – Network monitoring function logical interfaces 90

Table 1 – Traffic prioritization with CoS and DSCP.....25
Table 2 – Summary of alert of network monitoring 53
Table B.1 – Redundancy protocols and recovery times.....83
Table E.1 – Sentences received by the network monitoring function.....90
Table E.2 – Sentences transmitted by the network monitoring function.....90
Table F.1 – Distribution of functions around 460-Network 91
Table F.2 – Equipment standards referencing IEC 61162-460.....92
Table G.1 – USB class codes 93
Table H.1 – Cross reference between IACS UR E26/E27 and IEC 61162-460 94

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.

This commented version (CMV) of the official standard IEC 61162-460:2024 edition 3.0 allows the user to identify the changes made to the previous IEC 61162-460:2018+AMD1:2020 CSV edition 2.1. Furthermore, comments from IEC TC 80 experts are provided to explain the reasons of the most relevant changes, or to clarify any part of the content.

A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text. Experts' comments are identified by a blue-background number. Mouse over a number to display a pop-up note with the comment.

This publication contains the CMV and the official standard. The full list of comments is available at the end of the CMV.

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 61162-450:2024.

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.

The contents of the corrigendum 1 (2024-08) have been included in this copy.

~~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~~2024 **1**, *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*

~~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].~~ *Version 2*
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 Remote Monitoring 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 following terms and definitions ~~given in IEC 61162-450 and the following~~ 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 ~~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 to 460-Networks and to uncontrolled networks or controlled **2** 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~~

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**

~~**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~~ **4**

3.10
backdoor
installed program allowing ~~remote~~ **5** 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 ~~does not pose any~~ 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] **6**

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.~~

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**

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 ~~disrupt~~ 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 Bluetooth[1] 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

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 ~~observation~~ supervision

Note 1 to entry: A ship's navigation bridge with closed consoles and access ~~observation~~ 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.

---

[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.

3.46
simple network management protocol
SNMP
protocol according to ISOC RFC 3411 used to ~~convey~~ 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 7 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 ~~an IEC 61162-450 compliant network, an IEC 61162-460 compliant network or~~ a controlled network

~~EXAMPLE Wireless networks.~~

Note 1 to entry: In this document this is also known as untrusted network. 8

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 9
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
~~announcement of a situation or~~ condition requiring immediate 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.

[SOURCE: IEC 62923-1] 3

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 ~~network implementing the requirements of~~ 460-Network as described in 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.