

INTERNATIONAL STANDARD



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 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 Central Office
3, rue de Varembe
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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 61162-460

Edition 2.0 2018-05
REDLINE VERSION

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 978-2-8322-5686-2

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	15
4.1 Overview	15
4.2 Description	15
4.3 General requirements	16
4.3.1 Equipment and system requirements	16
4.3.2 Physical composition requirements	16
4.3.3 Logical composition requirements	17
4.4 Physical component requirements	17
4.4.1 450-Node	17
4.4.2 460-Node	17
4.4.3 460-Switch	18
4.4.4 460-Forwarder	18
4.4.5 460-Gateway and 460-Wireless gateway	18
4.5 Logical component requirements	18
4.5.1 Network monitoring function	18
4.5.2 System management function	19
4.6 System documentation requirements	19
4.7 Secure area requirements	19
5 Network traffic management requirements	19
5.1 460-Node requirements	19
5.2 460-Switch requirements	20
5.2.1 Resource allocation	20
5.2.2 Loop prevention	20
5.3 460-Forwarder requirements	21
5.3.1 Traffic separation	21
5.3.2 Resource allocation	21
5.3.3 Traffic prioritization	21
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	23
6.2 Internal security requirements	24
6.2.1 General	24
6.2.2 Denial of service protection	24
6.2.3 REDS security	24
6.2.4 Access control	25
6.3 External security requirements	26

6.3.1	Overview	26
6.3.2	Firewalls	26
6.3.3	Direct communication	27
	~~Communication security~~	
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	29
7.1	General requirements	29
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
	~~460-Gateway and 460-Wireless gateway~~	
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	37
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	43
10.6.1	Resource allocation	43
10.6.2	Loop prevention	43

10.6.3	Security	44
10.6.4	Monitoring	45
10.7	460-Forwarder	45
10.7.1	Traffic separation.....	45
10.7.2	Resource allocation	46
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.....	49
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
~~Monitoring~~		
10.9	460-Wireless gateway.....	51
10.9.1	General	51
10.9.2	Security	51
~~Monitoring~~		
10.10	Controlled network.....	52
10.11	Network monitoring function.....	52
10.11.1	General	52
10.11.2	Network load monitoring function.....	53
10.11.3	Redundancy monitoring function.....	53
10.11.4	Network topology monitoring function	53
10.11.5	Syslog recording function	54
10.11.6	Alert management	54
10.12	System level	55
10.12.1	General	55
10.12.2	System management function.....	56
10.12.3	System design	56
10.12.4	Network monitoring function	58
10.12.5	Network load monitoring function.....	58
10.12.6	Redundancy monitoring function.....	58
10.12.7	Network topology monitoring function	59
Annex A (informative) Communication scenarios between an IEC 61162-460 network and uncontrolled networks		60
A.1	General.....	60
A.2	Routine off-ship	60
A.3	Routine on-ship.....	61
A.4	460-Gateway usage for direct connection with equipment	61
Annex B (informative) Summary of redundancy protocols in IEC 62439 (all parts).....		62
~~B.1 Summary of redundancy protocols~~		
~~B.2 RSTP recovery time~~		
Annex C (informative) Guidance for testing		64
C.1	Methods of test	64
C.2	Observation	64

C.3	Inspection of documented evidence	64
C.4	Measurement	64
C.5	Analytical evaluation	65
Annex D (informative)	Some examples to use this document	66
Annex E (normative)	IEC 61162 interfaces for the network monitoring function	70
Annex F (informative)	Distribution of functions around 460-Network	71
Bibliography		73
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 ~~61162-450~~ 61162-460 network and shore networks	60
Figure D.1	– 460-Forwarder used between two networks	66
Figure D.2	– 460-Forwarder used between two networks	66
Figure D.3	– 460-Gateway used for e-Navigation services	67
Figure D.4	– 460-Gateway used for remote maintenance	67
Figure D.5	– 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices	68
Figure D.6	– 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices	69
Figure E.1	– Network monitoring function logical interfaces	70
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	62
Table E.1	– Sentences received by the network monitoring function	70
Table E.2	– Sentences transmitted by the network monitoring function	70
Table F.1	– Distribution of functions around 460-Network	71
Table F.2	– Equipment standards referencing IEC 61162-460	72

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.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

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 standard extends the informative guidance given in Annex D of IEC 61162-450:2011.~~
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:~~2011~~ 2018, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*

IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results*

IEC 62288:2014, *Maritime navigation and radiocommunication equipment and systems – Presentation of navigation-related information on shipborne navigational displays – General requirements, methods of testing and required test results*

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

IEEE 802.1Q-~~2005~~, *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 ~~UDP/TCP~~ 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



Documents

Document Sharing Hub

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.

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.

3.39
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.

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

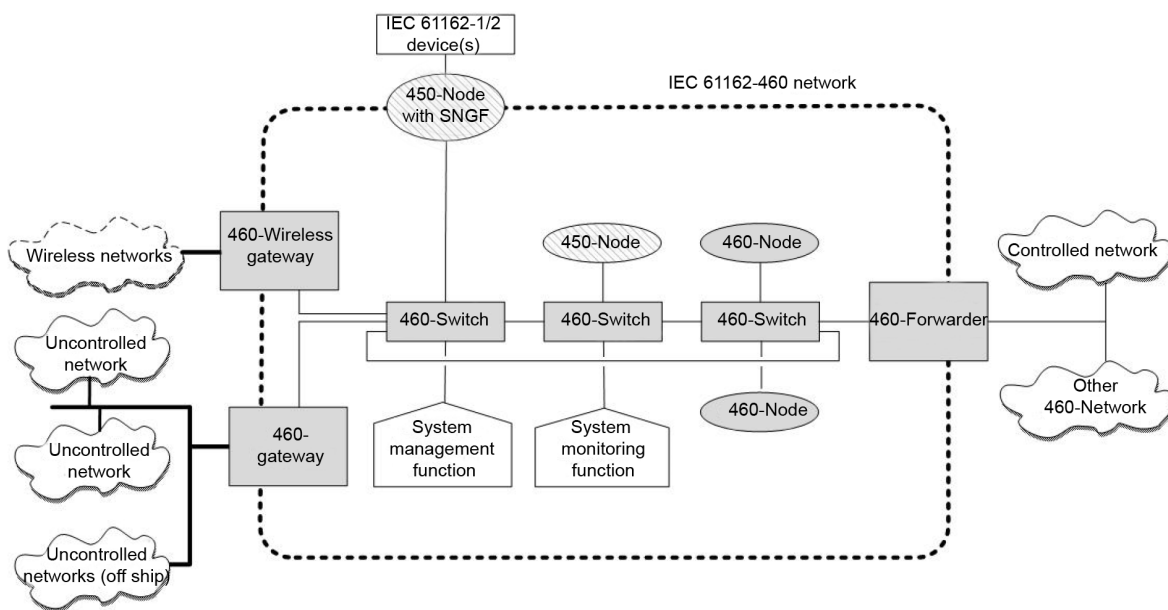
4.1 Overview

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.



EC

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 61162-450:2014 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 ~~are located at~~ **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: ~~2011~~ **2018**, 4.3.3.2;
- data output bandwidth documented by the manufacturer as described in 6.2.2.1;
- implemented ONF services ~~if provided~~ specified by the manufacturer, including the necessary protocol parameters, ~~for instance for~~ **at least** IP address and ~~UDP/TCP~~ 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 ~~UDP/TCP~~ 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 ~~may~~ 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, ~~for instance for at least~~ IP address and ~~UDP/TCP~~ 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. ~~The following functions~~ Security requirements as specified in 6.2, 6.3 and 6.4 shall be implemented ~~in a 460-Gateway and 460-Wireless gateway.~~

- ~~• security requirement as specified in 6.2, 6.3 and 6.4;~~
- ~~• network monitoring as specified in 8.1.5.~~

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;
- ~~functionality to~~ save and ~~to~~ restore configuration information either automatically or manually from 460-Switches, 460-Forwarders, 460-Gateways and 460-Wireless gateways;
- ~~functionality to~~ change the infrastructure configuration –

NOTE 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 ~~structure~~ **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)

The 460-Switch and 460-Forwarder may support ~~relaxed~~ **disabling** MAC address ~~related~~ **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 ~~image~~ **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 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 % for 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, ~~VLAN protocol version IEEE 802.1Q:2005 shall be supported~~, 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:

- 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 ~~TCP or UDP~~ port number or range of port numbers;
- means to allocate network bandwidth resource for each registered stream;
- all incoming and outgoing traffic shall be registered;
- all traffic not registered shall be ~~prohibited~~ blocked;
- 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;
- the total amount of traffic per interface to a 450-Node and 460-Node shall be limited to the network design value of that interface. The network design value shall be selectable between 0 % to 50 % of the physical capacity of the ~~switch~~ port;
- if VLAN is provided, a means to configure virtual networks (VLAN) per interface shall be provided;
- if VLAN is provided, VLAN protocol ~~version~~ IEEE 802.1Q:2005 shall be supported;
- means to filter multicast traffic by IGMP snooping as required by IEC 61162-450:2018;
- 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 provide a capability to enable RSTP in all 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 ~~version~~ IEEE 802.1Q ~~2005~~ shall be supported.
- means to filter multicast traffic IGMP snooping as required by IEC 61162-450:2018;
- 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 ~~switch~~ forwarder;
- the 460-Forwarder shall be configurable for a maximum traffic flow;
- a means shall be provided 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 ~~TCP or UDP~~ port number;
- 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 ~~are required~~ means shall be provided for traffic prioritisation at a 460-Forwarder:

- a) means to handle dropping of lower priority traffic based on priority;
 - ~~• if the amount of traffic to be transferred in 30 s is higher than 50 % of the set maximum then traffic prioritisation shall be used to drop lower priority traffic until the traffic is below 50 % of the set maximum;~~
 - ~~• the highest priority traffic shall continue lossless until the amount of traffic to be transferred in 30 s is higher than 100 % of the set maximum after which also a part of highest priority traffic shall be dropped;~~
 - ~~• the use of dropping shall be reported by syslog for each period of 30 s during which the dropping has been used.~~
 - 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)

Documents shall be provided which include the following information:

- 460-Network traffic flow analysis and network topology information;
- 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.

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 ~~460~~-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 or change of the configuration file by mistake (mis-operation);
- 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 wireless 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 an important file 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 6.3.

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 protocol 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 node under 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.

6.2.3 REDS security

(See 10.5.2.3)

6.2.3.1 Physical protection

The number of connection points (USB ports, disc drives, etc.) shall be limited to the absolute minimum required for the operation of the system and its lifetime maintenance and support. All other points shall be physically blocked from easy access by a user without a tool or key.

6.2.3.2 Operational protection

Connection points shall limit their operation to permitting connection only to data sources.

For USB based devices, only USB device class 08h (USB mass storage) is acceptable for REDS. For other devices, the manufacturer shall provide information about the technology used and how the connection point fulfils the requirement to limit connection to only data sources.

USB connection points used for keyboards, printers, etc. shall be blocked from easy access by a user for example by means of a tool or key or password protection (disable/enable) in the device set-up.

6.2.3.3 Executable program file verification

All automatic execution at a 460-Node from REDS including USB auto-run shall be prohibited.

Manual execution of any type of files from REDS shall only be possible after passing authentication for accessing the executable content of the REDS. Manual execution shall be possible only for the files which are verified before execution, using digital signature or special keys.

NOTE 1 A digital signature method is based on a private/public key pair. Typically, a hash function is used, for example the SHA-2 family (use of MD5 and SHA-1 are now discouraged, see ISO/IEC 10118-3).

NOTE 2 Special keys ~~may~~ can be values calculated from the delivered data using a specified function and compared against a known and expected value, both the function and the value being specified by the trusted source or sender.

6.2.3.4 Non-executable data verification

All non-executable data in REDS shall be verified before it is used in equipment.

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.

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 includes 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;
- 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", "random and meaningless passwords should be used";

- passwords shall use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and special characters.

6.2.4.2 Network access control

(See 10.6.3.4, 10.7.4.4)

Network access control is intended to permit or to deny access to 460-Network resources. A 460-Switch or 460-Forwarder shall deny the access of unauthorised equipment and unauthorised traffic by network access control.

Each connected 450-Node and 460-Node to a 460-Network, if installed outside of a secure area, shall be authorised by its MAC address and physically connected to a port at a 460-Switch or 460-Forwarder. If a connected node is intended to be installed in a secure area means shall be provided to enable or disable the authorisation by MAC address.

All bypassing and originating traffic at a 460-Switch and 460-Forwarder shall be authorised by IP address, protocol number and ~~UDP/TCP~~ port number.

NOTE Typically, network access control functions are provided by the equipment manufacturer under the name of Access Control List (ACL).

6.3 External security requirements

6.3.1 Overview

All traffic from uncontrolled networks is passed or processed through the 460-Gateway or 460-Wireless gateway. Figure 2 shows an example of a 460-Network with a 460-Gateway. As shown in Figure 2, a 460-Gateway consists of firewalls and DMZ with various servers. The DMZ is located between the internal 460-Network and the uncontrolled network. Two firewalls are implemented, one for the uncontrolled network and the other for the 460-Network. These firewalls are classified as external and internal.

The 460-Gateway components may be implemented in one device or in different devices.

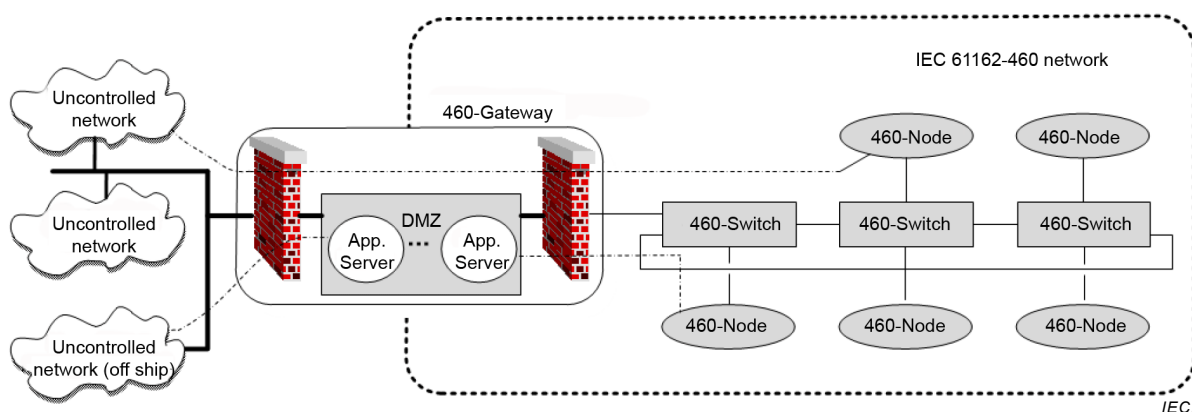


Figure 2 – 460-Network with 460-Gateway

6.3.2 Firewalls

6.3.2.1 External firewall

An external firewall blocks all traffic unless it is registered and destined only to equipment in the DMZ. This means that, in principle, all direct communication to a 460-Network is not allowed.

6.3.2.2 Internal firewall

An internal firewall blocks all traffic unless it is destined to equipment in a 460-Network and it originates from equipment in the DMZ. All traffic passing through the internal firewall is registered in advance.

6.3.3 Direct communication

(See 10.8.3)

When direct communication is required to equipment in a 460-Network, permission from an administrator or supervisor is required together with monitoring during the entire communication period (see 6.3.5 and Annex A).

~~6.3.3~~ Communication security

A direct connection between uncontrolled networks and a 460-Network is only enabled from a 460-Gateway or from a 460-Wireless gateway. The direct connection is protected from activation remotely via an external network. Once the direct connection is established, a 460-Node can use this connection for communication with an uncontrolled network, for details see 6.3.4.

All **direct** connections between uncontrolled networks and a 460-Network shall use VPN through a 460-Gateway or 460-Wireless gateway. All data exchanged with an uncontrolled network shall be encrypted to protect from security attacks. **VPN can be used by the 460-Gateway or 460-Wireless gateway to connect 460-Networks over uncontrolled networks.** A 460-Gateway or a 460-Wireless gateway may also allow a 460-Node to communicate through VPN directly to another destination. In this case a 460-Gateway or a 460-Wireless gateway shall establish the VPN connection and the 460-Gateway or the 460-Wireless gateway shall provide the network functions for the connections within the internal 460-Network.

NOTE Encryption protects against unauthorized reading, signature/authentication protects against unauthorized modification and identifies the sender. Combination of both is possible.

The secure encryption algorithm shall use either asymmetric or symmetric algorithms with the following key length:

- an asymmetric encryption algorithm shall provide at least 2 048-bit key length (256 B) with encryption strength at least as strong as RSA;
- a symmetric encryption algorithm shall provide at least 256-bit key length (32 B) with an encryption strength at least as strong as AES.

The key shall be delivered using a chain of trust, or if private keys are involved, exchanged in a secure manual way or using a combination of manual (e.g. by phone call) and message (e.g. by secured/encrypted email transfer).

6.3.4 460-Node

(See 10.5.2.5)

A 460-Node can exchange information with other equipment directly from uncontrolled networks only through a 460-Gateway bypassing the DMZ if it is required. When direct connection is provided, the following requirements shall be satisfied:

- by manufacturing default, direct connection from an uncontrolled network shall be set to "not allowed";
- the direct connection to a 460-Node from an uncontrolled network shall only be activated by an operator from a 460-Node. ~~It shall be protected from activation remotely via an external network;~~ precondition is that a direct connection between uncontrolled network

and the 460-Network itself is already enabled from the 460-Gateway or from the 460-Wireless gateway.

- a 460-Node shall have a permanent indication when direct connection with an uncontrolled network is activated;

NOTE Examples of indication are mechanical position, lamp, display, etc.

- a caution "Connected to uncontrolled network" shall be generated ~~after a pre-defined time period~~, and the interface as described in 8.2.7 shall be used when a direct connection is activated;
- the caution may be replaced with a warning after ~~another~~ a pre-defined time period;
- all connections between uncontrolled networks and a 460-Node shall satisfy ~~external~~ communication security requirements (6.3.3).

6.3.5 460-Gateway

6.3.5.1 Firewall

(See 10.8.4)

The following are requirements for a 460-Gateway:

- by manufacturing default, direct connection from an uncontrolled network shall be set to "not allowed";
- internal and external firewalls shall be provided that are configured with the combination of source/destination IP address, protocol and port number;
- all connections between uncontrolled networks and a 460-Network shall be registered;
- all connections from uncontrolled networks to a 460-Network shall satisfy external communication security requirements (see 6.3.3);
- a 460-Gateway shall either indicate activated direct connection between 460-Networks and uncontrolled networks or generate a caution "Connected to uncontrolled network"; if provided, the caution shall use an interface as described in 8.2.7;

NOTE ~~Indication may be based on mechanical position, lamp, display, etc.~~

- a 460-Gateway shall provide a list of all activated direct connections between 460-Networks and uncontrolled networks; this list shall be recorded by the gateway or an external device including changes over the past 12 months; means to view the list shall be provided; at least the following information, if available, shall be recorded for each activated direct connection: source IP address, destination IP address, starting time and end time of the connection, protocol, and ~~TCP~~ port number;
- the direct connection with a 460-Node from an uncontrolled network shall only be activated by an operation on the installation site or the 460-Network side of the firewall; it shall not be possible to be activated from uncontrolled networks; means shall be provided to ensure that the operation can only be performed with permission from an administrator or supervisor;
- all direct connection shall be terminated automatically after a pre-defined time period no longer than 4 h unless there is user intervention to extend the time;
- all traffic for direct connection shall not be forwarded automatically after a pre-defined time ~~period of not exceeding~~ 10 min of no traffic on the connection.

6.3.5.2 Application server

(See 10.8.5)

An application server allows a common data access to be seen by the uncontrolled networks and the 460-Network.

If provided, the application server shall provide an application level authentication mechanism, such as password to client, from uncontrolled networks.

The following are requirements for any server that is located at the DMZ in a 460-Gateway:

- no routing of packets is allowed;
- shall comply with 460-Node requirements;
- means shall be provided to protect from malware as appropriate to the computer platform.

6.3.5.3 Interoperable access to file storage of DMZ

(See 10.8.6)

Means may be provided to download/upload files between the DMZ and uncontrolled networks or a 460-Network in order to access the file storage within the DMZ. If access to the file storage within the DMZ is provided, then it shall implement a protocol such as SMB networking protocol (for example Samba²) or SFTP (Secure Shell (SSH) File Transfer Protocol). **If SMB networking protocol is implemented, version 1 shall not be used due to security vulnerabilities.**

6.3.6 460-Wireless gateway

(See 10.9.2)

The following are requirements for a 460-Wireless gateway:

- wireless access point (AP) functions shall not be allowed, i.e. a wireless gateway shall be operated only as a client;
- traffic forwarding from the wireless network to 460-Network shall not be allowed;
- a corresponding SF or ONF as defined in IEC 61162-450 shall be provided; a wireless gateway shall meet all the requirements of a 460-Gateway; all data exchanged through a wireless interface shall meet the encryption requirement of 6.3.3;
- wireless connection shall be established only to registered Wireless AP(s) with authentication.

6.4 Additional security issues

(See 10.6.3.5, 10.7.4.5, 10.8.7)

The following management functions are required for a 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway:

- the configuration shall be retained following a switch off or power failure and the equipment shall return to the normal operation upon restoration of power;
- when changes are made to the configuration, the previous configuration shall be stored **by the system management function**; means shall be provided to revert to the previous configuration **from the system management function (see 4.5.2)**;
- installation instruction shall advise that physical access to 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway shall be restricted.

7 Redundancy requirements

7.1 General requirements

(See 10.12.3.10)

² Samba is the trademark of a product supplied by Samba Organization (www.samba.org). 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.

7.1.1 General

A single component failure (cable, 460-Switch, 460-Forwarder, 460-Gateway or 460-Wireless gateway) shall not affect the functionality of the critical nodes in 460-Network.

Documentation of system configuration shall identify which nodes are critical.

NOTE 1 Three kinds of failures are defined in IEC 62439-1: transient failure, component failure, systematic failure (see Annex B).

When a problem occurs in a 460-Network (detected by network monitoring), the recovery time from a failure event to the activation of a redundant method shall be no longer than 5 s.

NOTE 2 For systems that require shorter recovery time than 5 s, refer to ISO 16425.

The redundancy shall be provided by either interface redundancy (see 7.1.2) or device redundancy (see 7.1.3). Figure 3 shows an example for network configuration with the redundancy specified in this document.

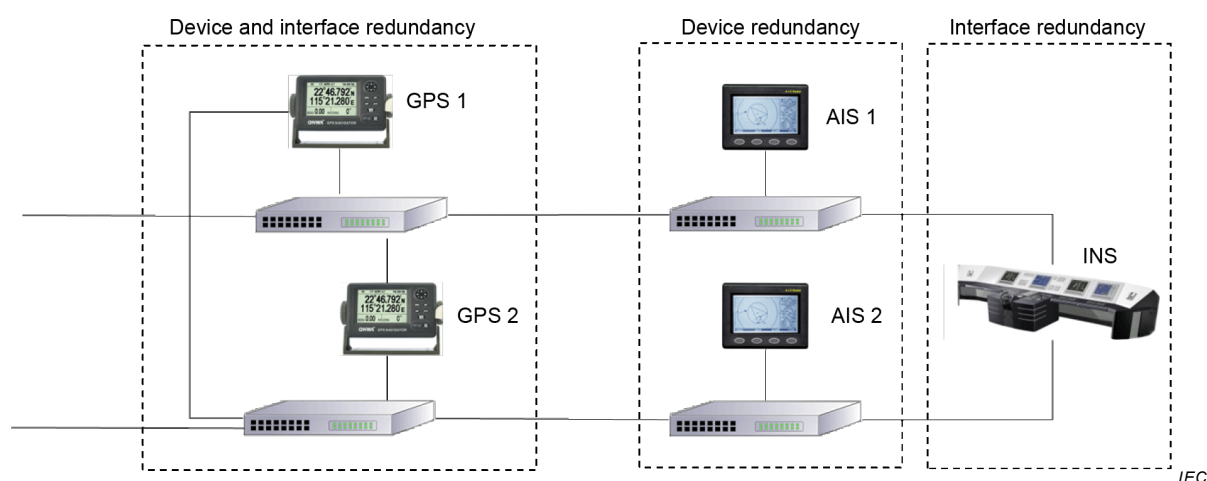


Figure 3 –Example of redundancy

7.1.2 Interface redundancy

Interface redundancy means that there is more than one IEC 61162-450 interface at the device and interfaces are connected to at least two different 460-Switches.

The equipment shall implement interface redundancy by either of the methods below.

- Data stream redundancy

The equipment with the data stream redundancy shall transmit and receive the same data from two interfaces. When equipment receives duplicated messages, the duplicated message shall be processed at the network layer or above the transport layer.

NOTE 1 Processing can lead to use or no use of a message by the receiving equipment.

- Link based redundancy

The equipment with the link based redundancy shall transmit and receive data only on the first interface, while the second interface is in standby. If the first interface fails, the second interface shall take over within 5 s. The two interfaces can be configured with two separate IP addresses or one common IP address

NOTE 2 This technique is known as switch fault tolerance, backup bonding or dual homing. The interface switching is managed by the operating system. The application layer regards both interfaces as a single

interface and does not need to process duplicated messages. This enables the use of redundancy protocols such as CARP (common address redundancy protocol).

NOTE 3 The implementation of interface redundancy depends on the local area network (LAN) topology.

7.1.3 Device redundancy

Device redundancy means that at least two devices with the same function are activated at the same time.

Equipment with device redundancy shall have a unique device identifier, i.e. TAG block and SFI, and shall be connected to a different 460-Switch. For additional safety, device redundancy can be used with interface redundancy.

7.2 460-Node requirements

(See 10.5.3)

Each 460-Node defined as critical shall provide at least interface redundancy or device redundancy.

NOTE The manufacturer of the 460-Node defines the equipment as critical or not critical.

Documentation shall be provided describing the redundancy capability.

7.3 460-Switch requirements

(See 10.5.3)

If a 460-Switch is failing or a cable between 460-Switches is disconnected, the main network traffic resulting from other 460-Switches in the 460-Network shall be rerouted to the 460-Node defined as critical either by a ring, a backup interface, or any comparable architecture.

7.4 460-Forwarder requirements

If redundancy is provided, the redundancy requirements of a 460-Switch shall be applied.

7.5 460-Gateway and 460-Wireless gateway requirements

If redundancy is provided, the redundancy requirements of the 460-Switch shall be applied.

7.6 Network monitoring function requirements

Network monitoring functions shall be redundantly available (see 8.2.6).

7.7 System design requirements

(See 10.12.3.10)

The system documentation shall include FMEA or FMECA for its redundancy capability.

The system integrator of a 460-Network shall provide sufficient documentation showing that the 460-Network including all connected equipment fulfils the single component failure requirement: a failure in a cable, a 460-Switch, 460-Forwarder, 460-Gateway or 460-Wireless gateway shall not affect the functionality of the critical nodes in a 460-Network. The documentation shall identify the critical nodes.

8 Network monitoring requirements

8.1 Network status monitoring

8.1.1 460-Network

The configuration of the 460-Network and the traffic flows shall be reported and monitored as described in 8.1.2 to 8.1.4.

8.1.2 460-Node

(See 10.5.4)

The required configuration information for monitoring at a 460-Node is:

- the number of interfaces;
- the list of traffic flows and its designed maximum traffic rate;
- the change of the flows – add, delete or modify;
- the list of flows assigned to each interface.

The information shall be provided by syslog (see IEC 61162-450) periodically each 30 min at a 460-Node. Also, the information shall be logged whenever changes in the configuration occur such as addition or deletion of flows at nodes. The configuration information shall not be reported more often than once per minute.

8.1.3 460-Switch

(See 10.6.4)

The required configuration information for monitoring at a 460-Switch is:

- the interface information;
- the list of neighbour MAC address per interface;
- the change of neighbour MAC address.

The information shall be reported by a 460-Switch when it receives a SNMP query request message (see 8.2.3 and 8.2.4). Also, ~~the information shall be logged~~ whenever changes in the configuration occur, such as changes of a neighbour MAC address, ~~the changes shall be reported using SNMP-Traps and/or syslog~~. The configuration information ~~using syslog~~ shall not be reported more often than once per minute.

The required traffic flow information for monitoring at a 460-Switch is the interface input and output link utilization in percent (average over 5 min).

The information shall be reported by a 460-Switch when it receives a SNMP query request message (see 8.2.2). Also, ~~the information shall be logged~~ whenever significant changes (traffic is more than ~~10 % difference with the previous information~~ predefined limit in 0 % to 100 % scale of network capacity) have been made, ~~the changes shall be reported using SNMP-Traps and/or syslog~~. The traffic flow information ~~using syslog~~ shall not be reported more often than once every 3 s.

NOTE The SNMP responses sent by the 460-Switch to the network monitoring do not directly cause any alert but act as a statistical base for the network monitoring function to raise the alerts.

8.1.4 460-Forwarder

(See 10.7.5)

The 460-Forwarder shall provide the configuration information which is required for the switch (see 8.1.3) ~~periodically each 30 min using~~ when it receives a SNMP query request message

(see 8.2.3 and 8.2.4). If VLAN is provided, current VLAN configuration information shall be provided. Also, ~~the information shall be reported~~ whenever changes have been made, ~~the changes shall be reported using SNMP-Traps and/or syslog~~. The configuration information using syslog shall not be reported more often than once per minute.

The 460-Forwarder shall provide the traffic flow information which is required for the switch (see 8.1.3) together with the number of valid input and output packets per interface (average over 5 min). ~~The information shall be provided periodically every 30 s. Also, the information shall be reported whenever significant changes (more than 10 % difference with the previous information in 0 % to 100 % scale of network capacity) have been made. The traffic flow information shall not be reported more often than once every 3 s.~~

The information shall be reported by a 460-Forwarder in the same way as for a 460-Switch (see 8.1.3).

~~8.1.5 460-Gateway and 460-Wireless gateway~~

~~(See 10.8.8, 10.9.3)~~

~~The 460-Gateway shall provide configuration information using syslog (see 8.1.2) and/or SNMP (see 8.1.3) periodically each 30 min. Also, the information shall be reported whenever changes have been made. The configuration information shall not be reported more often than once per minute.~~

~~Additionally, the 460-Gateway shall provide traffic flow information using syslog and/or SNMP (see 8.1.3) periodically every 30 s. Also, the information shall be reported whenever significant changes (more than 10 % difference with the previous information in 0 % to 100 % scale of network capacity) have been made. The traffic flow information shall not be reported more often than every 3 s.~~

8.2 Network monitoring function

8.2.1 General

(See 10.11.1)

The network monitoring function assists in maintaining the network operation by monitoring the network load, redundancy and topology, detecting violations and generating alerts. The function of network monitoring shall be available at least in ~~a one 460-Node or in one 460-Switch~~ which is a part of a 460-Network.

If the EUT does not provide the network monitoring function, the installation documentation shall specify that the EUT can only be connected to a network in which another equipment provides the network monitoring function.

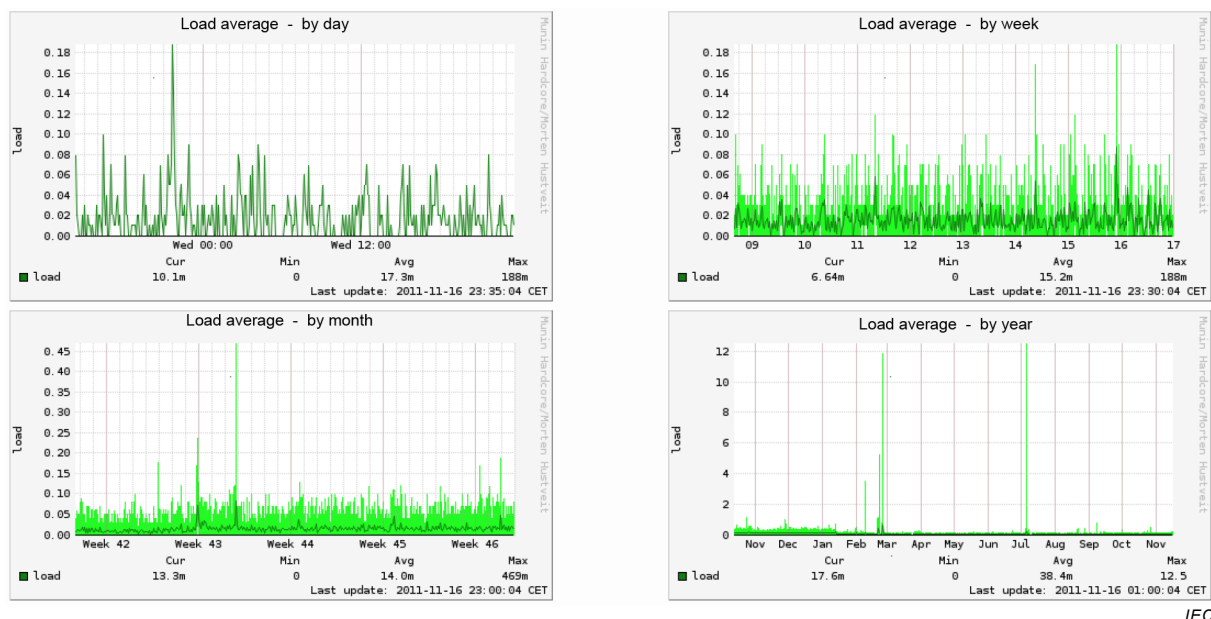
The network monitoring function shall provide ~~either a local~~ the functionality of the alert management and shall provide human machine interface (HMI) ~~or an interface for~~ to access the alerts management function (see 8.2.7).

If a local HMI is provided and the system is intended for installation on the bridge, the interface for alerts (see 8.2.7) shall be provided. Compatibility for bridge installation shall be declared by the manufacturer.

The network monitoring function shall keep a recording which is available on demand. The recording shall be capable of storing events for at least the last 3 months or last 10 000 events, whichever is smaller. At least the following events shall be stored in the recording:

- a) any alert from the network monitoring function;
- b) any event or reports from 460-Switches or 460-Forwarders using SNMP and/or syslog (see 8.2.2, 8.2.3 and 8.2.4).

The recordings shall be capable of being displayed in a format suitable for viewing by users. An example is given in Figure 4.



IEC

Figure 4 – Example of network status recording information

8.2.2 Network load monitoring function

(See 10.11.2)

The system documentation shall include an analysis for every switch and between switches, forwarders and gateways of the maximum network load based on the manufacturer's declarations of total maximum traffic rates for all flows the system generates to the 460-Network.

The network monitoring function shall ~~request SNMP responses~~ use at least one of the alternatives below to collect the information from the 460-Switches and 460-Forwarders as specified in 8.1.3 and 8.1.4:

- periodically every 30 s using SNMP query;
- using a combination of SNMP-Trap method (i.e. by requesting RMON statistics) and periodic SNMP query every 15 min;
- using syslog method with reports not more often than once per minute.

The network load monitoring function shall generate the following alerts.

- Caution: Network traffic capacity may be exceeded – when the observed network load has exceeded the 80 % limit of physical capacity of any port in a 460-Switch or a 460-Forwarder for a period of 30 s more often than 3 times within a period of 10 min;
- Warning: Network traffic capacity exceeded – when the observed network load has exceeded the 80 % limit of physical capacity of any port in a 460-Switch or a 460-Forwarder for a period of 30 s more often than 10 times within a period of 10 min.

8.2.3 Redundancy monitoring function

(See 10.11.3)

The system documentation shall include a list of data sources which are redundantly available either by interface redundancy (see 7.1.2) or device redundancy (see 7.1.3). For interface redundancy, the list shall contain the MAC address, interface number and interface name.

in a 460-Switch. For device redundancy, the list shall contain the MAC address of each redundantly available device.

The network monitoring function shall ~~request SNMP responses~~ use at least one of the alternatives below to collect the information from the 460-Switches and 460-Forwarders as specified in 8.1.3 and 8.1.4:

- a) periodically every 30 s using SNMP query;
- b) using a combination of SNMP-Trap method (i.e. by requesting RMON change notifications) and periodic SNMP query every 15 min;
- c) using syslog method with reports not more often than once per minute.

The list shall include the following information:

- name of data source: maximum 8 character string;
- two or more MAC addresses, interface number and interface available alternatives for each redundant network address from which this data is available.

When less than two MAC addresses, or one MAC address with less than two interfaces available for the source of data, have been lost for a period of 2 min, the network redundancy monitoring function shall generate the following alert:

Caution: Network redundancy lost for xxxx.

Where xxxx is the name of the data source.

8.2.4 Network topology monitoring function

(See 10.11.4)

8.2.4.1 Topology monitoring

System documentation shall include the list of accepted devices for a 460-Network with their MAC addresses. For accepted devices in a secure area, the list may include "not applicable" instead of the MAC address if the device has been selected for disabling the authorisation (see 6.2.4.2).

Maintaining the network topology requires network topology monitoring and generating alerts based on detected additional devices not available in the list of accepted devices. The network monitoring function shall ~~request network configuration~~ use at least one of the alternatives below to collect information from the 460-Switches and 460-Forwarders as specified in 8.1.3 ~~using SNMP periodically every 30 min~~ and 8.1.4:

- a) periodically every 30 min using SNMP query;
- b) using a combination of SNMP-Trap method (i.e. by requesting RMON change notifications) and periodic SNMP query every 2 h;
- c) using syslog method with reports not more often than once per minute.

When a MAC address which is not included in the list of accepted devices has been found from the SNMP requests, the network topology monitoring function shall generate the following alert.

Caution: New device is detected in the network.

8.2.4.2 SFI collision monitoring

At the construction of a 460-Network of a ship, the assignment of SFI (system function ID) may be clearly defined. However, as the equipment of the ship is amended, replaced, repaired and serviced, the assignment of SFIs may not be as clear.

Maintaining uniqueness of SFIs requires SFI collision monitoring and generating alerts based on detected collision between multiple instances of equal SFIs. The SFI collision monitoring is based on SRP-sentences sent by 450-Nodes and 460-Nodes (see IEC 61162-450). The SFI collision monitoring assists service organizations to maintain the uniqueness of SFIs as well as inform the users if something is wrong in the setup configuration of their system in use.

The following rules apply to SFI collision monitoring:

- SFI collision monitoring shall maintain an SFI Table based on all fields available in the received SRP sentences. A new combination of fields of SRP-sentence shall cause a new entry to the SFI Table;
- SFI collision monitoring shall provide a possibility to view the content of the SFI Table. The view shall indicate at least SFI collisions and redundantly available SFIs. The view may be available internally in the equipment in which the SFI collision monitoring is implemented or may be available in other equipment for which the SFI collision monitoring provides the required information;
- SFI collision monitoring shall provide reset of the SFI Table at boot up of SFI collision monitoring and on demand by the user;
- based on the SFI Table, non-colliding SFI can be identified. Equal MAC address combined with different SFI or equal IP address combined with different SFI do not cause collision of SFI;
- based on the SFI Table, redundantly available SFIs can be identified from differences in the "Instance number of redundant alternative" fields of SRP sentences. Redundantly available SFIs do not cause collision of SFIs;
- based on the SFI Table, a collision is detected when all conditions below are met:
 - an equal SFI is available from multiple SRP sentences;
 - "Instance number of redundant alternative" field of at least one of the SRP sentences contains null or two SRP sentences contains equal values; and
 - there are either differences in the "MAC address" field or differences in the "IP address" field of SRP sentences.

When an SFI collision is detected, the SFI collision monitoring function shall generate the following alert.

Caution: SFI cxxxx collision in the network.

Where cxxxx is the identifier string of the SFI.

8.2.5 Syslog recording function

(See 10.11.5)

The network monitoring function shall act as receiver and recorder of the syslog messages.

The network monitoring function shall provide recording and viewing of the syslog information which the 450-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways have provided.

The minimum capacity of the recording shall be ~~100 000~~ 20 000 messages. The recorded syslog messages shall be available for at least the last ~~30~~ 90 days.

8.2.6 Redundancy of network monitoring function

(See 10.12.7.3)

The network monitoring function shall be redundantly available.

8.2.7 Alert management

8.2.7.1 Alerts and indication

(See 10.11.6.1)

Alerts and indications shall comply with the presentation requirements specified in IEC 62288.

Table 2 is a summary of all alerts defined in this document.

Table 2 – Summary of alert of network monitoring

Source	Cause	Alarm	Warn.	Caut.	Categ. A	Categ. B	Unique identifier at alert source
460-Node	Direct connection to uncontrolled network as a caution (see 6.3.4)			x		x	3109
460-Node	Direct connection to uncontrolled network as a warning (see 6.3.4)		x			x	3108
460-Gateway	Connected to uncontrolled network (see 6.3.5.1)			x		x	3113
Network monitoring function	Network traffic capacity may be exceeded (see 8.2.2)			x		x	3116
Network monitoring function	Network traffic capacity exceeded (see 8.2.2)		x			x	3118
Network monitoring function	Network redundancy lost for xxxx (see 8.2.3)			x		x	3123
Network monitoring function	New device is detected in the network (see 8.2.4)			x		x	3126
Network monitoring function	SFI conflict detected (see 8.2.4)			x		x	3129

8.2.7.2 Alert management interface

(See 10.11.6.2)

A bi-directional interface facilitates communication so that alerts can be transferred to external systems and audible alarms (if provided) can be muted or acknowledged from external systems.

The alert management interface, if provided, shall be compliant with the requirements of Annex E and the state diagram of IEC 61924-2:2012, Annex J ~~and the detailed sentence definitions of IEC 61924-2:2012, Annex K.~~

Alert management requires:

- classification of alerts;
- presentation of the alerts;
- reporting of alerts;
- handling of unacknowledged warnings;
- functionality of remote acknowledge and remote silencing.

8.2.7.3 Unacknowledged warnings

(See 10.11.6.3)

An unacknowledged warning shall be:

- repeated as a warning after a limited time period not exceeding 5 min; or
- changed to alarm priority after a limited time period not exceeding 5 min; or
- changed to alarm priority after a user selectable time not more than 5 min.

The default time for the user selected period shall be 60 s.

8.2.7.4 Remote acknowledgments and silencing of alerts

(See 10.11.6.4)

Remote acknowledgement shall only be possible for category B alerts (see IEC 61924-2:2012, Annex C).

Remote silencing of the relevant audible alarms of the network monitoring function shall be possible at any time if provided.

9 Controlled network requirements

(See 10.10)

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

- it shall not be possible to connect devices to the network that can be used to insert non-authorised traffic into the network, neither by direct access to the physical infrastructure nor through wireless interfaces;
- network nodes shall not allow a user direct access to operating systems or functions that can be used to insert non-authorised traffic into the network, unless this user is authorised to perform these operations;
- it shall not be possible to transfer data from a non-authorised REDS or a REDS with un-authorised contents to any node or device in the network.

NOTE Most controlled networks would also include provisions for hindering unauthorised reading of data in the network, hindering changes in network topology, etc. However, such provisions are not required for the controlled networks connected to the 460-Network.

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

10 Methods of testing and required test results

10.1 Subject of tests

The equipment under test (EUT) may be an individual network/system component as defined in this document or a system based on this document.

10.2 Test site

The test site may be either a laboratory test bed or an installation in a test facility or on-board of a vessel depending on the manufacturer's choice.

NOTE A laboratory test bed is typically chosen for individual network/system components. A full system installation in the test facility is more appropriate for complex systems. Alternatively, they can be tested on-board as well.

A network protocol analyser is required (for example Wireshark³).

A simulator arrangement with the following characteristics is required:

- capable of transmitting and receiving IEC 61162-450-compliant data and data not compliant with IEC 61162-450;
- capable of generating invalid data;
- capable of supporting the Ethernet interface appropriate to the EUT;
- capable of providing SNMP and syslog client-server data;
- capable of monitoring network configuration and status information over SNMP;
- capable of monitoring network configuration and status information over syslog;
- capable of providing ICMP packets;
- capable of providing network load from 0 % to 100 % using IEC 61162-450-compliant data and data not compliant with IEC 61162-450 (for example TCP/IP, UDP/IP, multicast and broadcast);
- capable of providing IEC 61162-450-compliant data with priority as specified in Table 1, if the EUT supports this functionality;
- capable of providing IEC 61162-450-compliant data to multiple networks including VLANs and subnets.

A simulator arrangement for security testing with the following characteristics is also required:

- capable of providing client-server connection;
- capable of providing DoS attack packet generation.

Guidance on testing is given in Annex C.

10.3 General requirements

(See 4.3.1)

Confirm compliance of each 460-Network component with the general requirements for shipboard navigation radiocommunication equipment in accordance with IEC 60945.

Confirm compliance of each 460-Network component with general requirements in accordance with Clauses 4 and 5 of IEC 61162-450:2011 2018.

Confirm by inspection of the manufacturer's documentation that a list of all applicable MAC addresses is provided for the 460-Network.

Test data or test reports from tests previously conducted in accordance with the referenced IEC standards may allow compliance to be verified by inspection of the test documents.

10.4 450-Node

(See 4.4.1)

³ Wireshark is the trademark of a product supplied by the Wireshark organization (www.wireshark.org). 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.

Confirm by ~~observation~~ **analytic evaluation** that ~~there is~~ no connection to external networks or REDS **can be established in normal operation**.

Confirm by analytical evaluation that syslog is implemented as defined in IEC 61162-450:~~2011~~ **2018**, 4.3.3.2.

Confirm by inspection of the manufacturer's documentation that the data output from a node is documented as described in 6.2.2.1.

If ONF services are provided, confirm by inspection of the manufacturer's documentation that they include necessary protocol parameters, for instance for IP **addresses** and ~~UDP/TCP~~ port numbers.

10.5 460-Node

10.5.1 Network traffic management

(See 5.1)

Confirm by analytical evaluation of documented evidence that the 460-Node does not create non-IEC 61162-450-compliant traffic.

NOTE Most of the use cases for traffic can be described as ONF, in which case they are IEC 61162-450 compliant traffic. Clear non-compliant cases are typically based on using reserved IP-addresses or port numbers for other purposes than allowed in the IEC 61162-450, for example a video service broadcasting in 239.192.0.1.

Refer to the manufacturer's documentation and confirm by inspection of documented evidence that the maximum transmission rate for all supported services is specified and confirm by analytical evaluation of documented evidence that all IEC 61162-450 compliant data meet their maximum transmission rate.

Confirm by analytical evaluation that a device meets its equipment performance requirements with a loss rate of packets up to 0,1 % for a time period of 10 min.

Confirm by inspection of documented evidence that the manufacturer has specified device behaviour when the maximum input data rate has been exceeded.

Confirm by ~~analytical evaluation~~ **inspection of documented evidence** of the 460-Node that it discards all other received data except data it supports.

If provided, refer to the manufacturer's documentation and confirm by inspection of documented evidence that the maximum transmission rate for all supported VLAN services is specified and confirm by analytical evaluation of documented evidence that all IEC 61162-450 compliant data in each VLAN meet their maximum transmission rate.

If VLAN is provided, confirm by inspection of documented evidence that the 460-Node supports VLAN ~~version~~ IEEE 802.1Q:~~2005~~.

10.5.2 Security

10.5.2.1 Security **in** general

(See 6.2.1)

Confirm by inspection of the manufacturer's documentation that the EUT does not use any wireless LAN interface or Wireless AP functions.

Confirm by analytical evaluation that there is no VLAN tunnelling protocol in use if VLAN is provided.

10.5.2.2 Denial of service behaviour

(See 6.2.2.1)

Confirm by inspection of the manufacturer's documentation that the maximum operational input bandwidth is declared by the manufacturer.

Use simulation arrangements to create traffics up to maximum that is declared by the manufacturer. Confirm by observation that the EUT meets its performance requirements.

Use simulation arrangements to create traffics of 200 % of the maximum that is declared by the manufacturer for a period of at least 10 min. After 10 min, return to the 100 % traffic. Confirm by analytical evaluation that the 460-Node behaves during and after the change in traffic as described by the manufacturer's documentation.

Confirm by inspection of the manufacturer's documentation that the maximum operational output bandwidth is declared by the manufacturer.

Confirm by analytical evaluation of the documented evidence or confirm by analytical evaluation of the EUT itself that the EUT does not exceed the declared maximum operational output bandwidth.

10.5.2.3 Security for REDS

(See 6.2.3)

Refer to ~~the device~~ the manufacturer's documentation and confirm by inspection of the documented evidence that the number of connection points for REDS (USB ports, disc drives, etc.) are limited to the absolute minimum required for the operation of the system and its lifetime maintenance and support. Confirm by observation that any other connection points are blocked from easy access by a user without a tool or key.

For USB based connection points for REDS, attach one by one a keyboard or mouse device (i.e. USB device class other than 08h) to the port and confirm by analytical evaluation that the EUT both refuses to recognize the attached device and refuses to perform any functionality with the attached device.

For USB based ports for other purposes than data sources, confirm by observation that they are blocked from easy access by a user.

For other connection points than for USB based REDS, use information provided by the manufacturer about the technologically possible roles of the REDS. If such a REDS is technologically subject for possible change of role, then attach one by one an example of non-data storage device to the port and confirm by analytical evaluation that the EUT both refuses to recognize the attached device and refuses to perform any functionality with the attached device.

One by one attach a device to the connection points for REDS or insert a media into the REDS (disc drives, etc.) and confirm by analytical evaluation that all automatic executions at the EUT is prohibited.

If the EUT provides manual execution of any type of files from REDS, confirm by analytical evaluation that manual execution is only possible for files which have been verified by digital signatures or special keys.

Use the manufacturer's documentation about non-executable files which can be used by EUT. Confirm by analytical evaluation that all non-executable files are verified as described in the manufacturer's documentation before use by the EUT.

10.5.2.4 Access control to configuration setup

(See 6.2.4.1)

Confirm by inspection of the manufacturer's documentation that the access to make changes in the configuration of the EUT is subject to user authentication.

Confirm by analytical evaluation that the user authentication before changing device settings is based on an at least 8 character long password, RSA keys, or another appropriate method.

Confirm by observation that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character.

Confirm by inspection of the manufacturer's documentation that the operator's manual includes guidance on the use of strong passwords, if appropriate.

10.5.2.5 Direct access to uncontrolled network

(See 6.3.4)

The following tests are applicable if the 460-Node provides direct connection for exchange of information with other equipment connected to an uncontrolled network.

Confirm by analytical evaluation that the manufacturing default settings of the EUT enable no direct connections with uncontrolled networks.

For each configured direct data exchange, confirm by analytical evaluation that as precondition for activation the direct connection the VPN has been established from a 460-Gateway or from a 460-Wireless gateway and that only the operator of the 460-Node can activate it the direct connection.

For each direct data exchange, confirm by observation that:

- there is a permanent indication when direct-data-exchange connection is active;
- a caution is created after a pre-defined time period when the direct connection is activated;
- if provided, the caution is replaced by a warning after another pre-defined time period;
- the caution and warning are removed after closing of the direct connection.

~~Confirm by inspection of the manufacturer's documentation that the VPN is used for communication with uncontrolled networks.~~

Confirm by inspection of the manufacturer's documentation that the encryption algorithm used for VPN meets the requirements of the encryption strength as specified in 6.3.3.

10.5.3 Redundancy

(See 7.2, 7.3)

Refer to the manufacturer's documentation and confirm by inspection of the documented evidence which means are provided for redundancy capability of the EUT.

10.5.4 Monitoring

(See 8.1.2)

Confirm by observation that monitoring information to syslog is provided by the EUT periodically each 30 min and not more often than once per minute of configuration information.

10.6 460-Switch

10.6.1 Resource allocation

(See 5.2.1)

Confirm by inspection of the manufacturer's documentation that a means is provided to configure a stream or a network flow that is identified by the combination of the interface identifier, the MAC address or IP address, protocol number and ~~TCP or UDP~~ port number.

Confirm by inspection of the manufacturer's documentation that means are provided to allocate a network resource for all registered streams.

Register all incoming and outgoing traffic. Use simulation arrangements to create both registered and non-registered traffic. Confirm by analytical evaluation that only incoming and outgoing traffic goes through and all non-registered traffic is blocked.

Confirm by inspection of the manufacturer's documentation that means are provided for limiting the total amount of traffic for each interface to a 450-Node and 460-Node using the resource allocation.

Use a simulation arrangement to interface two 460-Nodes to the EUT and set the nodes to communicate with each other using the set maximum traffic. Confirm by analytical evaluation that all traffic passes the EUT. Increase the traffic by 50 % over the set maximum traffic for a period of 10 min. Confirm by analytical evaluation that excessive traffic is blocked.

Confirm by inspection of the manufacturer's documentation that, if a VLAN is provided, a means is provided to configure virtual networks (VLAN) for each interface.

Confirm by inspection of the manufacturer's documentation that, if VLAN is provided, the VLAN protocol ~~version~~ IEEE 802.1Q:2005 is supported.

Confirm by inspection of documentation that the EUT has means to filter multicast traffic by IGMP snooping.

Use a simulation arrangement to interface the EUT in parallel or one by one to a 460-Switch, a 460-Forwarder, a 460-Node and a 450-Node. Set a multicasting group in the EUT for filtering network traffic by IGMP snooping. Confirm by observation that the EUT sends IGMP membership queries for this multicast group.

10.6.2 Loop prevention

(See 5.2.2)

Confirm by the documented evidence that the EUT provides a loop prevention mechanism.

If an RSTP is provided, confirm by inspection of the manufacturer's documentation that the RSTP protocol version IEEE 802.1D-2004 is supported.

Set three 460-Switches for loop topology connect with at least one 460-Node at each switch, for example using unicast. Confirm by analytical evaluation that the switch does not duplicate data at switches.

Set three 460-Switches for loop topology connect with at least one 460-Node per switch for example using unicast. Disconnect one by one the cables between each neighbouring 460-Switch. Confirm by analytical evaluation that the data is reachable among 460-Nodes within 5 s.

10.6.3 Security

10.6.3.1 Security general

(See 6.2.1)

Confirm by inspection of the manufacturer's documentation that the EUT does not use any wireless LAN interface or wireless AP functions.

Confirm by analytical evaluation that there is no VLAN tunnelling protocol in use if VLAN is provided.

10.6.3.2 Denial of service behaviour

(See 6.2.2.2)

Confirm by inspection of documented evidence that the EUT provides ICMP and IGMP DoS prevention.

10.6.3.3 Access control to configuration setup

(See 6.2.4.1)

Confirm by inspection of the manufacturer's documentation that the access to make changes in the configuration of the EUT is subject to user authentication.

Confirm by analytical evaluation that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method.

Confirm by observation that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character.

Confirm by inspection of the manufacturer's documentation that the operator's manual includes guidance on the use of strong passwords, if appropriate.

10.6.3.4 Access control for network

(See 6.2.4.2)

Confirm by inspection of the manufacturer's documentation that means are provided to permit or deny a flow based on the IP address, protocol number and ~~UDP/TCP~~ port number for each physical port.

Confirm by analytical evaluation that means are provided to permit or deny a device based on the MAC address for each physical port. If the EUT supports installation in a secure area, confirm by analytical evaluation that the means are configurable to either enable or disable authorisation by the MAC address.

10.6.3.5 Additional security issues

(See 6.4)

Confirm by analytical evaluation that the EUT continues normal operation with the previous configuration when power is reapplied after a switch off or power failure.

Confirm by analytical evaluation that means are provided in the system management function to revert to the previous stored configuration.

Confirm by inspection of the documented evidence that guidance is given to install the EUT in a physically protected location.

10.6.4 Monitoring

(See 8.1.3)

Confirm by ~~analytical evaluation~~ observation that the following monitoring information is provided by the EUT:

- interface information;
- list of neighbouring MAC addresses per interface;
- the change of neighbouring MAC address.

Confirm by observation that the network configuration information is sent ~~through SNMP periodically every 30 min~~ by the EUT as a response to the SNMP query from the network monitoring function. Confirm by analytical evaluation that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by the Network monitoring function) whenever some changes in the configuration occur, such as changes of a neighbour MAC address. Confirm by observation that the configuration information using syslog is never reported more often than once per minute.

Confirm by observation that the interface input and output link utilization in percent (average over 5 min) is ~~provided sent~~ by the EUT as a response to the SNMP query from the network monitoring function. ~~Confirm by observation that the network status information is sent through SNMP periodically every 30 s by the EUT.~~ Confirm by observation that the information is reported ~~whenever significant changes (more than 10 % difference with the previous information)~~ at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by network monitoring function) whenever significant changes (traffic is more than predefined limit in a 0 % to 100 % scale of network capacity) have been made. Confirm by observation that the ~~status~~ information using syslog is never reported more often than once per 3 s.

10.7 460-Forwarder

10.7.1 Traffic separation

(See 5.3.1)

Confirm by inspection of the manufacturer's documentation that means are provided to transmit all or a subset of the traffic between a 460-Network and controlled networks or other 460-Networks.

Follow instructions given by the manufacturer and set the EUT to limit the maximum traffic flow between a 460-Network and controlled networks or other 460-Networks. Confirm by analytical evaluation that the total traffic transferred does not exceed the set maximum.

If VLAN capability is provided, confirm by inspection of the manufacturer's documentation that means are provided to configure transmitting/disconnecting between a 460-Network and controlled networks or other 460-Networks with VLAN at the EUT.

If VLAN capability is provided, confirm by inspection of the manufacturer's documentation that the 460-Forwarder implements the VLAN protocol ~~version~~ IEEE 802.1Q:2005.

Confirm by inspection of documentation that the EUT has means to filter multicast traffic by IGMP snooping.

Use a simulation arrangement to interface the EUT in parallel or one by one to a 460-Switch, a 460-Forwarder, a 460-Node and a 450-Node. Set a multicasting group in the EUT for filtering network traffic by IGMP snooping. Confirm by observation that the EUT sends IGMP membership queries for this multicast group.

10.7.2 Resource allocation

(See 5.3.2)

Register all incoming and outgoing traffic. Use simulation arrangement to create both registered and non-registered traffic. Confirm by observation that only incoming and outgoing traffic goes through and all non-registered traffic is blocked.

Confirm by analytical evaluation that means are provided for limiting the total amount of traffic for each interface to a 450-Node and 460-Node for a given value of that interface using resource allocation.

Connect two 460-Nodes to the EUT and set the nodes to communicate with each other using set maximum traffic. Confirm by observation that all traffic passes the EUT. Increase the traffic beyond the set maximum traffic. Confirm by analytical evaluation that excessive traffic is blocked.

Confirm by inspection of the manufacturer's documentation that a means is provided 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 ~~TCP or UDP~~ port number. Confirm by observation that means are provided to allocate a network resource for all registered streams.

If VLAN capability is provided, confirm by analytical evaluation that means are provided for limiting the total amount of traffic for each VLAN to controlled networks or 460-Networks for a given value using resource allocation.

10.7.3 Traffic prioritisation

(See 5.3.3)

Use a simulation arrangement to set three different types of traffic with different priorities that include the lowest priority. Set the traffic limit to be enough only for the highest priority traffic. Increase the traffic with the lowest priority until data loss occurs.

Confirm by analytical evaluation that the loss rate of the highest priority traffic is lowest and that of lowest priority is the highest.

For each port, create increased traffic higher than 50 % of physical capacity of the line or higher than the set maximum input data rate set for the port for 30 s and return to below 50 % of physical capacity of the line and below the set maximum input data rate set for the port. Confirm by analytical evaluation that there was a drop in lower priority traffic until the traffic was below 50 % of physical capacity of the line and below the set maximum input data rate set for the port.

For each port confirm by analytical evaluation that the highest priority traffic continues lossless until the amount of traffic transferred in the last 30 s is higher than the set maximum input data rate set for the port, after which also a part of highest priority traffic ~~is~~ may be dropped.

Confirm by analytical evaluation that the use of dropping is reported either by syslog for each period of 30 s during which the dropping has been used or as response to SNMP-Trap method.

10.7.4 Security

10.7.4.1 ~~Security in~~ General

(See 6.2.1)

Confirm by inspection of the manufacturer's documentation that the EUT does not use any wireless LAN interface or wireless AP functions.

Confirm by analytical evaluation that there is no VLAN tunnelling protocol in use if VLAN is provided.

10.7.4.2 Denial of service behaviour

(See 6.2.2.2)

Confirm by inspection of documented evidence that the EUT provides ICMP and IGMP DoS prevention.

10.7.4.3 Access control to configuration setup

(See 6.2.4.1)

Confirm by inspection of the manufacturer's documentation that the access to make changes in the configuration of the EUT is subject to user authentication.

Confirm by analytical evaluation that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method.

Confirm by observation that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character.

Confirm by inspection of the manufacturer's documentation that the operator's manual includes guidance on the use of strong passwords, if appropriate.

10.7.4.4 Access control for network

(See 6.2.4.2)

Confirm by inspection of the manufacturer's documentation that means are provided to permit or deny a flow based on the IP address, protocol number and ~~UDP/TCP~~ port number for each physical port.

Confirm by analytical evaluation that means are provided to permit or deny a device based on the MAC address for each physical port. If the EUT supports installation in a secure area, confirm by analytical evaluation that the means are configurable to either enable or disable authorisation by the MAC address.

10.7.4.5 Additional security

(See 6.4)

Confirm by observation that the EUT continues normal operation with the previous configuration when power is reapplied after switch off or input power interruption.

Confirm by analytical evaluation that, after changes have been made to the EUT configuration, means are provided in the system management function to revert to the previous stored configuration.

Confirm by inspection of the manufacturer's documentation that guidance is given to install the EUT in a location with restricted physical access.

10.7.5 Monitoring

(See 8.1.4)

Confirm by observation that the following monitoring information is provided by the EUT:

- interface information;
- list of neighbouring MAC addresses per interface;
- the change of neighbouring MAC address.

~~Confirm by observation that the network configuration information is sent through SNMP periodically every 30 min by the EUT. Confirm by observation that the information is logged whenever some changes in the configuration occur such as changes of the neighbour MAC address. Confirm by observation that the configuration information is never reported more often than once per 1 min.~~

~~Confirm by observation that the interface input and output link utilization in percent (average over 5 min) is provided by the EUT together with the number of valid input and output packets per interface (average over 5 min).~~

~~Confirm by observation that the network status information is sent through SNMP periodically every 30 s by the EUT. Confirm by observation that the information is reported whenever significant changes (more than 10 % difference with the previous information in a 0 % to 100 % scale of network capacity) have been made. Confirm by observation that the status information is never reported more often than once per 3 s.~~

Confirm by observation that the network configuration information is sent by the EUT as a response to the SNMP query from the network monitoring function. If VLAN is provided, confirm by observation that the current VLAN configuration information is sent as a response to the SNMP query. Confirm by analytic evaluation that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by Network monitoring function) whenever some changes in the configuration occur, such as changes of the neighbouring MAC address. Confirm by observation that the configuration information using syslog is never reported more often than once per minute.

Confirm by observation that the interface input and output link utilization in percent (average over 5 min) is sent by the EUT as a response to the SNMP query from the network monitoring function. Confirm by observation that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by the network monitoring function) whenever significant changes (traffic is more than predefined limit in a 0 % to 100 % scale of network capacity) have been made. Confirm by observation that the information using syslog is never reported more often than once per 3 s.

10.8 460-Gateway

10.8.1 Denial of service behaviour

(See 6.2.2.2)

Confirm by inspection of documented evidence that the EUT provides ICMP and IGMP DoS prevention.

10.8.2 Access control to configuration setup

(See 6.2.4.1)

Confirm by inspection of the manufacturer's documentation that the access to make changes in the configuration of the EUT is subject to user authentication.

Confirm by analytical evaluation that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method.

Confirm by observation that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character.