IEC 61162-460

Edition 2.0 2018-05
REDLINE VERSION

INTERNATIONAL STANDARD

colour
inside

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

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

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

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

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a 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 It also gives information on projects, replaced and withdrawn publications.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

colour
inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 47.020.70

ISBN 978-2-8322-5686-2

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

CONTENTS

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

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 Bluetooth[1] 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.

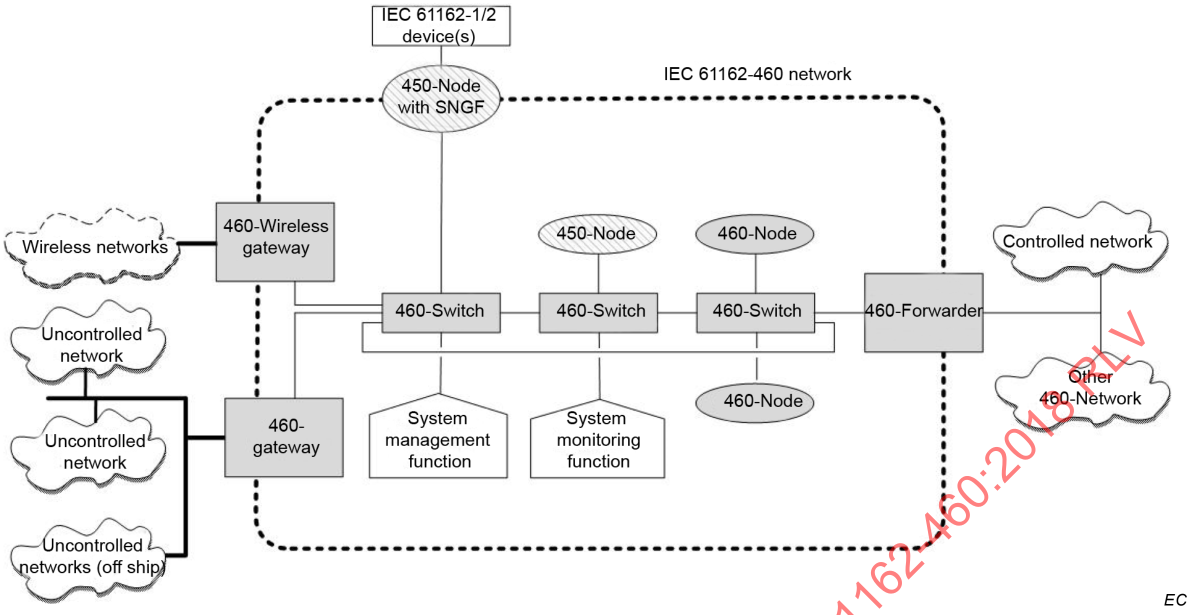


Figure 1 – Functional overview of IEC 61162-460 requirement applications

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:~~2011~~ 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

(See10.5.2.1, 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.

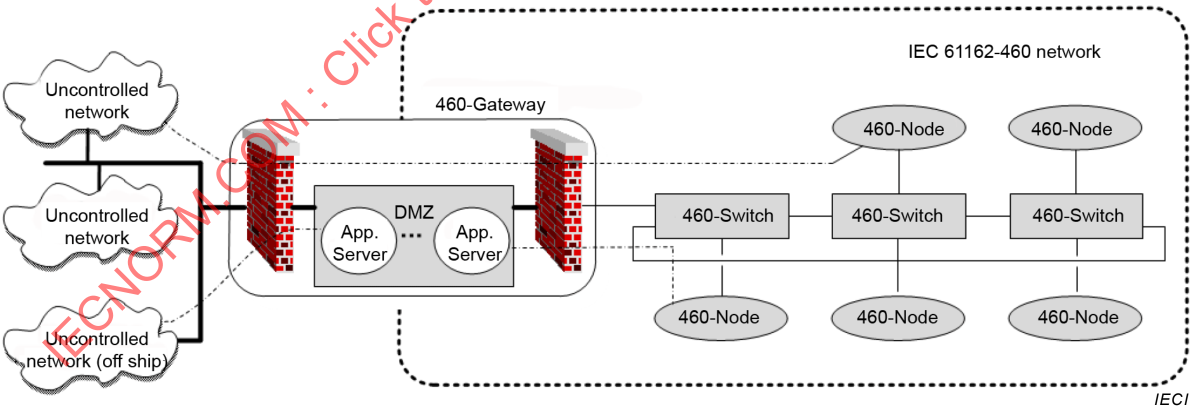


Figure 2 – 460-Network with 460-Gateway

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 Samba[2]) 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.

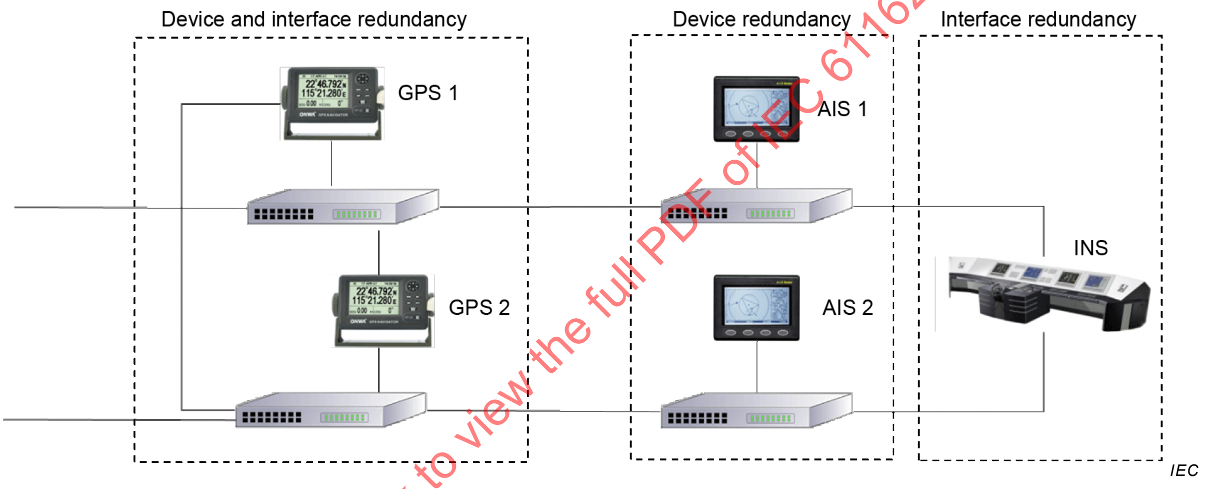


Figure 3 –Example of redundancy

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 alert~~s~~ management function (see 8.2.7).

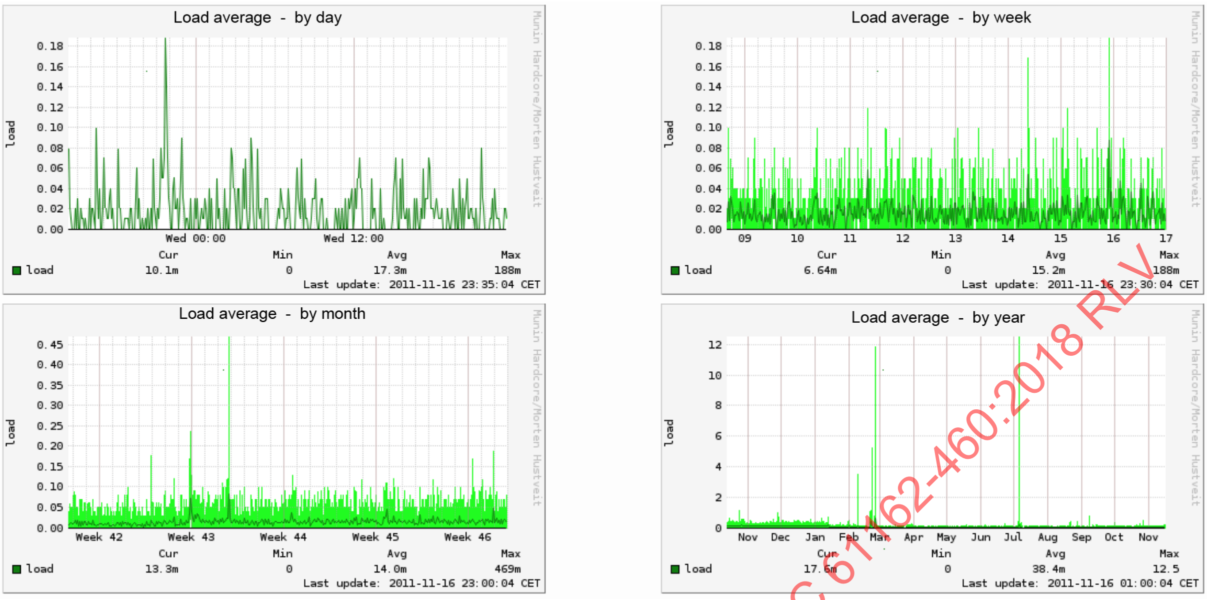
If a local HMI is provided and the system is intended for installation on the bridge, the interface for alerts (see 8.2.7) shall be provided. Compatibility for bridge installation shall be declared by the manufacturer.

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:

a) periodically every 30 s using SNMP query;

b) using a combination of SNMP-Trap method (i.e. by requesting RMON statistics) and periodic SNMP query every 15 min;

c) 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 available 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 Wireshark[3]).

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.

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

10.8.3 Communication security

(See 6.3.3)

Confirm by inspection of manufacturer's documentation that a direct connection between uncontrolled networks and a 460-Network can only be enabled from a 460-Gateway or from a 460-Wireless gateway.

Use a simulation arrangement to establish a VPN connection ~~through~~ originating at the EUT between 460-Network and uncontrolled network. Confirm by analytical evaluation that VPN ~~with TCP~~ is provided over the connection.

Confirm by inspection of the documented evidence that the encryption algorithm used for VPN meets the requirement of encryption strength as follows:

- an asymmetric encryption algorithm with at least a 2 048-bit key length (256 B);
- symmetric encryption algorithm with at least a 256-bit key length (32 B).

Confirm by inspection of the documented evidence that the delivery of certificates is based on a chain of trust or that the private keys/certificates are exchanged in secure manual way or using a combination of manual methods and messages.

10.8.4 Firewall

(See 6.3.5.1)

Confirm by analytical evaluation that all direct connections to the 460-Network are disabled in the manufacturer's default configuration.

Set an EUT between 460-Networks and uncontrolled networks. Set a ping generator to 20 different IP addresses ~~and port number~~ for the address range of the uncontrolled network, 460-Network and DMZ. Confirm by analytical evaluation that the following packets do not pass through the EUT:

- ping test to the internal address range of the 460-Network;
- ping test to address a range of DMZ of the EUT;
- ping test to address a range of uncontrolled networks.

Confirm by observation that the EUT registers traffic as an external/internal firewall rule which consists of source and destination IP address, protocol and port number.

Confirm by observation that the EUT provides a means to list all direct connections for the last 12 months.

Confirm by analytical evaluation that the EUT provides means to list activated direct connections between 460-Networks and uncontrolled networks with status information for each of these connections including: source IP address, destination IP address, starting time and end time of the connection, protocol, and ~~TCP~~ port number.

Confirm by analytical evaluation that means provided to allow direct connection with a 460-Node from an uncontrolled network can only be activated by an operation on the 460-Network side of the firewall. Confirm by inspection of the manufacturer's documentation that this cannot be activated from uncontrolled networks. Confirm that means are provided to ensure that the operation can only be performed after obtaining permission, for instance from the bridge officers.

Confirm by observation that the EUT terminates all direct connection automatically after a predefined time not exceeding 4 h unless there is user intervention to extend the time.

Confirm by observation that the EUT terminates all direct connection automatically after the connection is idle for a pre-defined time not exceeding 10 min.

If direct connection between 460-Networks and an uncontrolled network is provided, either confirm by observation that the activated state is indicated or confirm by analytical evaluation that the activated state generates a caution.

NOTE The generation and presentation of the caution can be performed by the device presenting the alerts for network monitoring.

10.8.5 Application server

(See 6.3.5.2)

Confirm by inspection of the manufacturer's documentation that an application server provides means to authenticate clients connected over uncontrolled networks, for example by password.

Confirm by analytical evaluation that Layer 3 forwarding or routing is disabled (i.e. no routing of packets is allowed).

Verify compliance with 460-Node requirements in accordance with 10.5.

Confirm by inspection of the manufacturer's documentation that means for protection from malware are described as appropriate to the computer platform.

10.8.6 Interoperable access to file storage of DMZ

(See 6.3.5.3)

Confirm by observation that a file can be downloaded and uploaded between the DMZ and uncontrolled networks if provided.

Confirm by observation that a file can be downloaded and uploaded between the DMZ and 460-Networks if provided.

If access to the file storage within the DMZ is provided, confirm by inspection of the manufacturer's documentation that a protocol is provided, such as SMB or SFTP.

If implemented, confirm by inspection of the documented evidence that the EUT access to file storage and related data traffic of DMZ satisfies the requirements for ONF, NF as specified in IEC 61162-450 and the 460-Node.

10.8.7 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.

~~10.8.8 Monitoring~~

~~(See 8.1.5)~~

~~Confirm by observation that the monitoring information is provided by the EUT of interface information.~~

~~Confirm by observation that the network configuration information is sent through SNMP or syslog periodically every 30 min by the EUT. Confirm by observation that the information is reported whenever some changes in the configuration occur such as changes of flows. 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 or syslog 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 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.~~

10.9 460-Wireless gateway

10.9.1 General

Confirm by inspection of documented evidence that the EUT satisfies the requirements of the 460-Gateway (see 10.8).

10.9.2 Security

(See 6.3.6)

Confirm by observation that wireless access point (AP) functions are not activated.

Confirm by observation that the forwarding function is not allowed.

Confirm by the manufacturer's documentation that all traffic to a 460-Network is compliant with IEC 61162-450 traffic.

Confirm by inspection of the documented evidence that the encryption algorithm used for VPN meets the requirement of encryption strength as follows:

- an asymmetric encryption algorithm with at least a 2 048-bit key length (256 B);
- symmetric encryption algorithm with at least 256-bit key length (32 B).

Activate wireless AP and confirm by observation that all connections to wireless AP are established only with authentication.

~~10.9.3 Monitoring~~

~~(See 8.1.5)~~

~~Confirm by observation that the monitoring information is provided by the EUT of Interface information.~~

~~Confirm by observation that the network configuration information is sent through SNMP or syslog periodically every 30 min by the EUT. Confirm by observation that the information is reported whenever some changes in the configuration occur such as changes of flows.~~

~~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 or syslog 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 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.~~

10.10 Controlled network

(See Clause 9)

Confirm by inspection of the documented evidence that the controlled network is not able to insert non-authorised traffic into the network, neither by direct access to the physical infrastructure nor through, for example, wireless interface.

Confirm by inspection of the documented evidence that the controlled network provide means to prevent direct access to operating systems or functions that can be used to insert non-authorised traffic into the network, unless this user is specially authorised to perform these operations.

Confirm by inspection of the documented evidence that the controlled network provides means to prevent transferring data from a non-authorised REDS or a REDS with un-authorised contents to any node or device in the network.

10.11 Network monitoring function

10.11.1 General

(See 8.2.1)

If the EUT does not provide network monitoring function, confirm by inspection of installation documentation that the EUT shall only be connected to a network in which another equipment provide network monitoring function.

Confirm by observation that the EUT provides monitoring either through a local human machine interface or an alert management interface.

If compatibility for bridge installation has been declared by the manufacturer, confirm by observation that the EUT provides an alert management interface.

Set a simulation arrangement to cause cautions and warnings. Confirm by observation that the EUT reports all alerts and is capable of accepting responsibility transferred, remote acknowledge and remote silence commands if an alert management interface is provided.

Set a simulation arrangement to cause cautions and warnings, and to generate events and reports from 460-Switches and 460-Forwarders. Confirm by observation that all alerts from the network monitoring function and, events and reports from 460-Switches and 460-Forwarders are recorded in the EUT.

Confirm by the documented evidence that the EUT has a capability to store events for at least the last 3 months or last 10 000 events, whichever is smaller, together with the capability of displaying the information.

10.11.2 Network load monitoring function

(See 8.2.2)

Confirm by observation that the system documentation includes an analysis for every switch and between switches, forwarders and gateways of the maximum network load.

~~Confirm by observation that the EUT requests the network monitoring information from all 460-Switches using SNMP periodically every 30 s.~~

Use the simulation arrangement and confirm by observation that the EUT requests the traffic flow information from all 460-Switches and 460-Forwarders either periodically every 30 s using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from SNMP or syslog or a combination of both for the following functionality:

a) generate~~s~~ cautions when the observed network load exceeds the 80 % limit of its maximum network capacity for a period of 30 s more than 3 times within a period of 10 min.

b) generate~~s alerts~~ warnings when the observed network load has exceeded the 80 % limit of the maximum network capacity for a period of 30 s more than 10 times within a period of 10 min.

10.11.3 Redundancy monitoring function

(See 8.2.3)

Confirm by observation that the system documentation includes a list of data sources that are redundantly available.

Confirm by observation that the list provides the names of data sources, two or more MAC addresses, interface number and interface available alternatives for each redundant network address from which this data is available.

~~Confirm by observation that the EUT generates cautions when less than two MAC addresses, or one MAC address with less than two interfaces available for a source of data in the list, has been lost for a period of 2 min for all SNMP requests performed every 30 s by the EUT.~~

Use the simulation arrangement and confirm by observation that the EUT requests the network configuration information from all 460-Switches and 460-Forwarders either periodically every 30 s using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from both SNMP and syslog to generate cautions when fewer than two MAC addresses, or one MAC address with fewer than two interfaces available for a source of data in the list, has been lost for a period of 2 min for all SNMP requests performed every 30 s by the EUT.

Confirm by observation that the caution complies with the requirement.

10.11.4 Network topology monitoring function

(See 8.2.4)

Confirm by observation that the system documentation includes a list of accepted devices.

Use the simulation arrangement and confirm by observation that the EUT requests the network topology information from all 460-Switches ~~using SNMP request/response messages~~ and 460-Forwarders either periodically every 30 min using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from SNMP or syslog or a combination of both to generate~~s~~ cautions when a MAC address, which is not included in the list of accepted devices, has been found.

Use the simulation arrangement and confirm by observation that the EUT creates the SFI Table based on received SRP sentences.

Use the simulation arrangement to include multiple, at least two, different SFI with any value of "Instance number of redundant alternative", any MAC address or any IP address reported by the SRP sentences, and confirm by observation that the EUT does not generate a caution.

Use the simulation arrangement to include two equal SFI, both with "Instance number of redundant alternative" fields of SRP sentence set as different values and with equal IP addresses reported by the SRP sentences and confirm by observation that the EUT does not generate a caution.

Use the simulation arrangement to include two equal SFI, both with "Instance number of redundant alternative" fields of SRP sentence set as null or set as same number and with different MAC addresses reported by the SRP sentences and confirm by observation that the EUT generates a caution.

Confirm by observation that the cautions comply with the requirements.

10.11.5 Syslog recording function

(See 8.2.5)

Set a simulation arrangement to cause syslog messages. Confirm by observation that the network monitoring function provides recording and ~~viewing of~~ internal or external possibility to view the syslog information from the 450-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways in 460-Network.

Confirm by inspection of the documented evidence that the minimum capacity of the recording is 100 000 messages and that the recorded syslog messages are available at least for the last 30 days.

10.11.6 Alert management

10.11.6.1 Alerts and indications

(See 8.2.7.1)

~~Verify in accordance with IEC 62288 that the presentation of alerts and indications complies with the requirement.~~

Confirm by analytical evaluation that the alerts comply with the criteria as required in Table 2.

10.11.6.2 Alert management interface

(See 8.2.7.2)

Confirm by inspection of the manufacturer's documentation that manufacturer defined alerts are in compliance with the criteria for classification and categories of alerts defined in IEC 61924-2:2012, 8.3 ~~and the alerts for ECDIS listed in IEC 61924-2:2012, Annex C~~.

~~For test of alert~~ In order to test the communication and presentation of the alerts, refer to the manufacturer's documentation to identify at least 1 of the available warnings, which may be chosen at random, and 2 of the available cautions, which may be chosen at random. Then, perform the following test using a simulator for BAM:

- confirm by analytical evaluation that the alert communication complies with the sentences listed in Annex E~~, the detailed sentence definitions of IEC 61924-2:2012, Annex K~~ and the state diagram of IEC 61924-2:2012, Annex J;
- confirm by analytical evaluation that, if means are provided to interface to a centralised alert management system, a caution alert is provided when the periodic receptions of the HBT sentence are interrupted.

10.11.6.3 Unacknowledged warnings

(See 8.2.7.3)

Confirm by inspection of the manufacturer's documentation that the default value for alert escalation is 60 s.

Confirm by observation that the user selectable time period for alert escalation is less than 5 min.

Confirm by inspection of the manufacturer's documentation that the manufacturer provides information about:

- which warnings are repeated as warning;
- which warnings are changed to alarms after the user-selectable time period;
- which warnings are changed to alarms after the manufacturer's fixed time period.

Refer to the manufacturer's documentation to identify at least 2 cases, which may be chosen at random, if available, in which a warning is repeated as warning. Confirm by observation that the time between repetitions is as selected by the user.

Refer to the manufacturer's documentation to identify at least 2 cases which may be chosen at random, if available, in which a warning is changed to alarm. Confirm by observation that the time before change of priority is as selected by the user.

10.11.6.4 Remote acknowledgements and silencing of alerts

(See 8.2.7.4)

Create 2 alerts, at least one of category B. Confirm by observation that ALF, ALC and HBT (if the EUT supports ‘responsibility transfer’) sentences are transmitted from the EUT to the alert management interface.

Use a simulator to send an ACN sentence to the EUT to silence one of the alerts. Confirm by observation that ALF, ALC and HBT (if provided) sentences report correctly the new state of the alerts.

Use a simulator to send an ACN sentence to the EUT to acknowledge the category B alert. Confirm by observation that ALF, ALC and HBT (if provided) sentences report correctly the new state of the alerts.

10.12 System level

10.12.1 General

Subclause 10.12 contains methods of testing and required results for system level confirmation of the requirements. The system level confirmation may be performed for:

- a typical system setup, as described by the applicant of conformance testing; or
- a real onboard installation, as described by the applicant of conformance testing.

The system level conformance testing is based on real-life equipment instead of simulation arrangements. The target of system level conformance testing is to prove that a real life system consisting of network infrastructure and equipment (for example navigation instruments like radar, ECDIS, gyro-compass~~, etc.~~) fulfil the system requirements of this document.

The basis of system-level conformance is that each individual component has been beforehand separately tested according to this document for the corresponding individual function(s) – see 10.4 to 10.9.

The minimum system for system level conformance testing consists at least of the following functions:

- two ~~pieces of~~ 460-Switches;
- two ~~pieces of~~ nodes of either type 450-Node or 460-Node; and
- a network monitoring function.

The test site requirements are:

- a network protocol analyser (for example Wireshark[4]) for monitoring of traffic;
- an arrangement capable of injecting more network traffic into the 460-Switches using IEC 61162-450 compliant data and non IEC 61162-450 compliant data (for example TCP/IP, UDP/IP, multicast and broadcast) to increase the network line load from the normal network load level up to the 100 % line load;
- an arrangement capable of injecting DoS attack into the 460-Switches.

10.12.2 System management function

(See 4.5.2)

Confirm by observation that the configuration information for a 460-Switch can be stored in the system. Replace a 460-Switch with another un-configured 460-Switch. Confirm by observation that, by using a system management function, it is possible to restore the original configuration to the new 460-Switch. This test shall be repeated for all 460-Switches and 460-Forwarders.

Remove one 460-Node and replace it with another equivalent device with a different MAC address. Confirm by observation that, by using the system management function, it is possible to change the original configuration to accept the new device.

Switch off the first system management function or if EUT has interface redundancy, disconnect one cable. Confirm by observation that the second system management function is available.

10.12.3 System design

10.12.3.1 General

(See 4.3.2, 4.3.3, 4.6, 4.7)

[4] 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 inspection of documented evidence that the following information is provided:

- the ~~structure~~ topology and devices of the network, including networks in a secure area, if provided;
- that the network consists of only 460-Network physical components, 460-Network nodes and network infrastructure components;
- that all networks connected with a 460-Forwarder are either controlled networks or other 460-Networks.

Confirm by ~~observation~~ inspection of documented evidence that both a network monitoring function and a system management function are available in the network.

10.12.3.2 Documentation

(See 4.6, 5.4.1)

Confirm by inspection of documented evidence that the following information is provided:

- the 460-Network traffic flow analysis and network topology;
- the total amount of network traffic and 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 if provided;
- the prioritization of each traffic type at each 460-Forwarder if provided;
- an analysis of the maximum network load;
- a list of data sources which are redundantly available;
- a list of accepted devices.

10.12.3.3 Network traffic design

(See 5.4.2)

Confirm by inspection of the document evidence that the amount of bandwidth allocated at each 460-Switch is more than, or equal to, the sum of all traffic volumes of each traffic class allocated to the network connected to the switch.

Use a network design document and select three ports to confirm by observation that the measured traffic is lower than or equal to the defined value of sum of traffic load. Confirm by observation that the average load of all traffic in a 460-Network does not exceed 95 % of the nominal network capacity planned over a period of 1 s and does not exceed 80 % of the nominal network capacity planned over a period of 10 s.

10.12.3.4 Loop prevention

Use a network design document and select at least two 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.

10.12.3.5 Resource allocation

Confirm by inspection of the document evidence that the amount of bandwidth allocated at each 460-Forwarder is more than, or equal to, the sum of all traffic volumes of each traffic class allocated to the network connected to the 460-Forwarder.

Use a network design document and select two ports to confirm by observation that the measured traffic is lower than, or equal to, the defined value of the sum of the traffic load.

10.12.3.6 Traffic prioritisation

If available in the system under test, select two traffic flows with different priority for which connected 460-Node based devices show activity. Use a simulation arrangement to inject additional traffic with a priority level between two selected priorities up to full line load. Confirm by observation that the device using highest priority traffic flow continues to show activity while the device using lowest priority traffic is distorted.

10.12.3.7 Denial of service behaviour

Use a network design document and select three 460-Nodes to inject additional traffic flows up to line load for 1 h. If the number of 460-Nodes is less than three, select all 460-Nodes. Confirm by observation that 460-Nodes continue their normal operation as stand-alone devices. Remove the injected additional traffic and confirm by observation that 460-Nodes resume their operation based on information received from the 460-Network.

10.12.3.8 Uncontrolled network security

If the system under test includes a 460-Gateway, repeat all tests as described in 10.8.

If the system under test includes a 460-Wireless gateway, repeat all tests as described in 10.9.

10.12.3.9 Connections between secure and non-secure areas

If the system under test includes a connection between a 460-Network installed in a secure area and a 460-Network installed in a non-secure area, repeat all tests as described in 10.7.

10.12.3.10 Redundancy

(See 7.1, 7.7)

Confirm by inspection of documented evidence that FMEA or FMECA is available for its redundancy capability and critical nodes are identified, and that no single points of failure affect the functionality of the critical nodes.

Use FMEA or FMECA documents and select 20 % of critical devices or at least three devices as representative devices. Cause a single failure one by one for each representative device and confirm by analytical evaluation that redundant devices continue normal operation within 5 s.

Select two traffic flows for connected 460-Node-based devices and show activities. Disconnect a cable between two 460-Switches and confirm by analytical evaluation that the interruption of data transfer is 5 s or less.

10.12.4 Network monitoring function

For the network monitoring function, repeat all tests as described in 10.11.1.

10.12.5 Network load monitoring function

For network load monitoring function, repeat all tests as described in 10.11.2.

10.12.6 Redundancy monitoring function

For network redundancy monitoring function, repeat all tests as described in 10.11.3.

10.12.7 Network topology monitoring function

10.12.7.1 General

For network topology monitoring function, repeat all tests as described in 10.11.4.

10.12.7.2 Syslog recording function

For syslog recording function, repeat all tests as described in 10.11.5.

10.12.7.3 Redundancy of network monitoring function

(See 8.2.6)

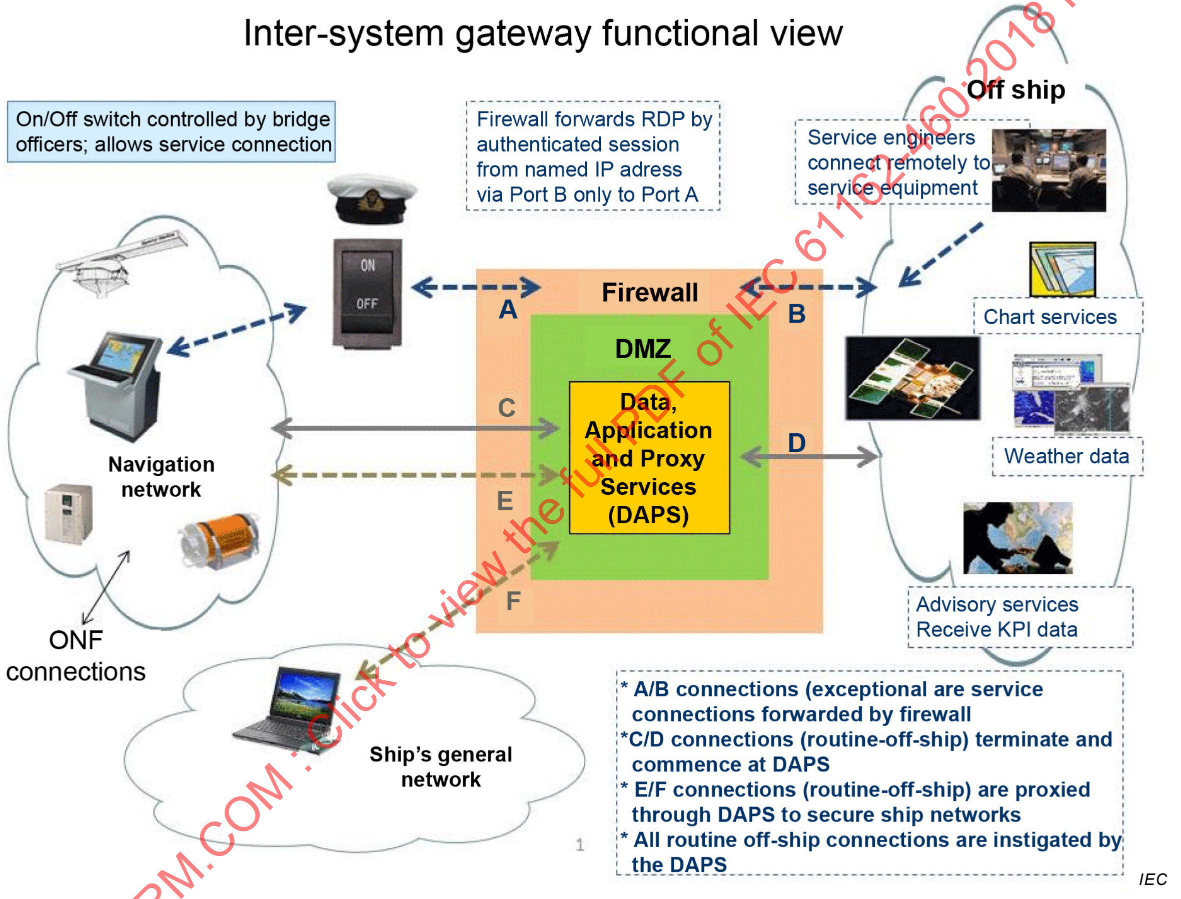
Switch off the first network monitoring function or if EUT has interface redundancy, disconnect one cable. Confirm by observation that the second network monitoring function is available.

Annex A
(informative)

Communication scenarios between an IEC 61162-460 network and uncontrolled networks

A.1 General

Annex A gives some example scenarios for the usage of a 460-Gateway as shown in Figure A.1.


Inter-system gateway functional view
On/Off switch controlled by bridge officers; allows service connection
Firewall forwards RDP by authenticated session from named IP adress via Port B only to Port A
Off ship
Service engineers connect remotely to service equipment
ON
OFF
Firewall
A
B
DMZ
Chart services
C
Data, Application and Proxy Services (DAPS)
D
Weather data
E
F
Navigation network
ONF connections
Advisory services Receive KPI data
Ship's general network
1
IEC

* A/B connections (exceptional are service connections forwarded by firewall
*C/D connections (routine-off-ship) terminate and commence at DAPS
* E/F connections (routine-off-ship) are proxied through DAPS to secure ship networks
* All routine off-ship connections are instigated by the DAPS

Figure A.1 – Usage model for communication between a IEC ~~61162-450~~ 61162-460 network and shore networks

A.2 Routine off-ship

- Data exchange from ship to shore, for example KPI data
  - energy usage reports
  - environnemental data (SOx, NOx, etc.)
  - CBM (conditioned base maintenance data)
  - diagnostic data (logs, etc.)
  - operations reports (noon reports, electronic log data)
- Data exchange shore to ship
  - chart services (licences, updates)

- weather
- ocean currents

A.3 Routine on-ship

Some navigational data is required in non-operational, secure ships networks, such as

- the ECDIS/bridge information channel on the captain's PC, and
- the GPS data.

A.4 460-Gateway usage for direct connection with equipment

Direct connection to an IEC 61162-460 network is provided through service connection through ~~ports~~ connections A-B. The following are examples for this scenario.

- An issue arises on the bridge. It is a safety issue concerning the display on the ECDIS and requires a patch.
- While the ship is in port a remote connection is planned at 18 h 00.
- The ECDIS service engineer coordinates the connection with the ship's IT department and crew.
- The IT department opens the Remote Desktop Protocol port on the perimeter firewall for a registered IP address or an authenticated user and forwards to it to the ~~Inter-system~~ 460-Gateway Firewall.
- The crew coordinates the on/off switch timing with the service engineer. They turn on the connection.
- The service engineer connects and repairs the system.
- The crew disconnects the bridge for remote service.
- The IT department closes the RDP port on the perimeter firewall.

Annex B
(informative)

Summary of redundancy protocols in IEC 62439 (all parts)

~~B.1 Summary of redundancy protocols~~

Table B.1 summarises the redundancy protocols and recovery times specified in IEC 62439 (all parts).

Table B.1 – Redundancy protocols and recovery times

Protocol	Solution	Frame loss	Redundancy protocol	End node attachment	Network topology	Recovery time for the considered failures
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30 s typical not deterministic
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20 s typical not deterministic
RSTP	IEEE ~~802.10~~ 802.1D	Yes	Within the network	Single	Single meshed, ring	~~Can be deterministic following the rules of Clause 8~~ ≤100 ms
MSTP	IEEE 802.1Q	Yes	Within the network	Single	Single meshed, ring	See STP and RSTP, compatible with both
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, cross-connected	1 s worst case for 512 end nodes
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches
MRP	IEC 62439-2	Yes	Within the network	Single	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 ms worst case for 500 end nodes
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0 s
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0 s
For the redundancy protocols specified in IEC 62439 (all parts), the recovery times in this table are guaranteed when using the settings and parameters specified in the associated part of the IEC 62439 series. Faster recovery times may be achieved using different settings and parameters under the user's responsibility.						

~~B.2 RSTP recovery time~~

~~The fault recovery time in the ring topology for RSTP is calculated as follows:~~

~~$T_{\mathrm{L}} + N^{*} \max (T_{\mathrm{PA}},(T_{\mathrm{TC}}+T_{\mathrm{F}}))$: for inter-switch link failure and non-root switch failure~~

~~$T_L + 2^* N^* T_{PA}$: for inter-switch link failure and non-root switch failure~~

~~where~~

~~N is the number of switches in the ring;~~

~~T_L is the time required by a switch to detect a link failure;~~

~~T_{PA} is the time required by a pair of switches to perform RSTP proposal-agreement handshaking; equal to the sum of BPDU processing times in both switches of the pair;~~

~~T_{TC} is the time required by a pair of switches to propagate a topology change BPDU; equal to the sum of the BPDU processing times in both switches of the pair.~~

~~RSTP performance is usually defined as failover time or recovery time per single hop. The latest RSTP standard specified in IEEE 802.1D-2004 limits the maximum network diameter to 40 hops. RSTP is both predictable and repeatable for failure and recovery of a link or switch in a ring topology. Precise equations can be used to determine the network outage time; for a ring of twenty switches, worst case failover times on the order of 100 ms are quite realistic. Typical RSTP performance is much better.~~

Annex C
(informative)

Guidance for testing

C.1 Methods of test

For the purposes of this document, Annex C gives guidance on methods of test based on ISO 9241-12~~ (see Bibliography)~~. It is intended to provide guidance to accredited testing laboratories for the development of test plans and test procedures that evaluate a minimum degree of compliance with the requirements specified. They do not identify specific processes, approaches or facilities.

C.2 Observation

Observation refers to simple examination of the presentation of information to confirm that a particular observable condition has been met. Observations may be made by any person with the necessary skill to understand the presentation of information to determine if a statement concerning an observable property has been correctly applied. It is used when suitably trained individuals with a broad range of education and/or experience can be confidently expected to reach the same conclusion about a property of presented information or the performance of display equipment.

The phrase "confirm by observation" is used in the method of test. Conformance is determined by comparing the observed property to the requirement. Some observations may be made directly from the presentation. Other observations may require simulation of input from sensors or other sources. Typical confirmations by observation include

- the existence of functions or features,
- the use of symbols or a defined range of words, and
- a system output in response to a defined input.

C.3 Inspection of documented evidence

Inspection of documented evidence refers to examination of relevant documents to confirm that a particular presentation or display requirement has been met. Documented evidence may include manuals, system requirements, design justification, industry conventions, etc. Inspections may be made by a suitably qualified person who has the necessary education, skill and/or experience to apply the documentation to the system's presentation or display equipment. ~~It~~ Inspection of documented evidence is used when performance of a system's presentation or display equipment is not directly observable or measurable. It may also be used when observation would be excessively repetitious, time consuming, or expensive.

The phrase "confirm by inspection of documented evidence" is used in the method of test. Conformance is determined by comparing the documented property to the requirement. Typical confirmations by inspection of documented evidence include

- the conformance to a standard or other documented evidence,
- the existence of optional features or functions, and
- the design and/or operation of algorithms.

C.4 Measurement

In this document, measurement refers to measuring or calculating a value or variable for comparison to a specified value to determine that a particular requirement has been met.

Measurements may require the use of test facilities and equipment. Measurements may be made by any person with the necessary skill to measure and/or calculate the value and compare it against a requirement, standard or other documented evidence. Compliance is determined by comparing the measured or calculated value or variable to the requirement.

C.5 Analytical evaluation

The test method "analytical evaluation" refers to detailed examination of the presentation of information to confirm that a particular condition has been met.

The phrase "confirm by analytical evaluation" is used in the method of test. Analytical evaluations may be made by a relevant expert with the necessary education, skills and/or experience to make an informed and reliable judgement concerning the presentation of information, its appropriateness and usability. It is used for the evaluation of properties that can be judged only in context of other information or knowledge that requires the tester's presentation. Compliance is determined by comparing the observed property to the requirement.

Annex D
(informative)

Some examples to use this document

Figure D.1 to Figure D.6 gives some examples of how this document could be used.

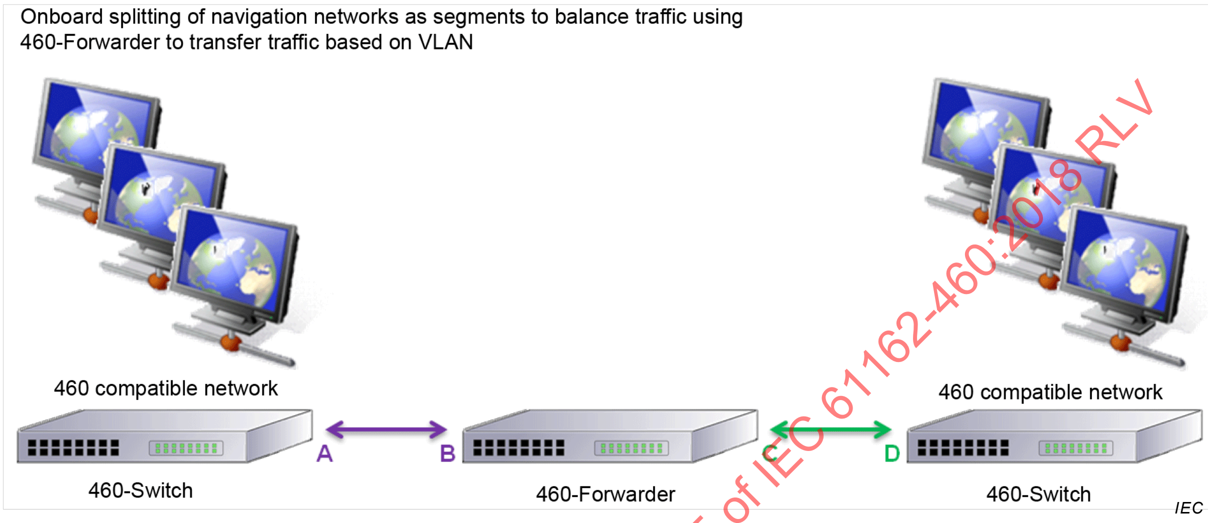

Onboard splitting of navigation networks as segments to balance traffic using 460-Forwarder to transfer traffic based on VLAN
460 compatible network
460 compatible network
A
B
C
D
460-Switch
460-Forwarder
460-Switch
IEC

Figure D.1 – 460-Forwarder used between two networks

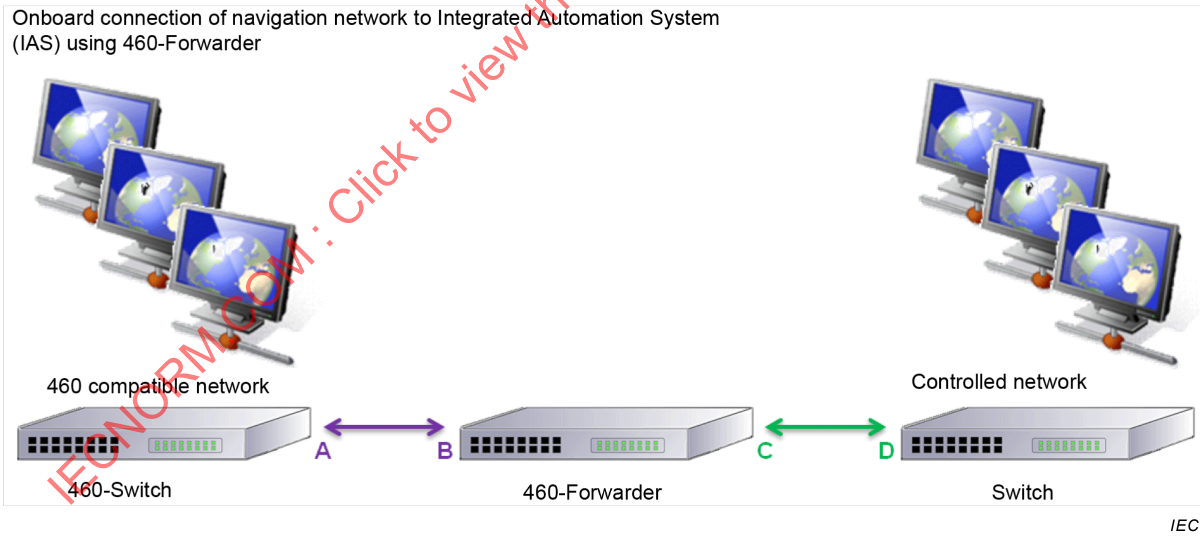

Onboard connection of navigation network to Integrated Automation System (IAS) using 460-Forwarder
460 compatible network
Controlled network
A
B
C
D
460-Switch
460-Forwarder
Switch
IEC

Figure D.2 – 460-Forwarder used between two networks

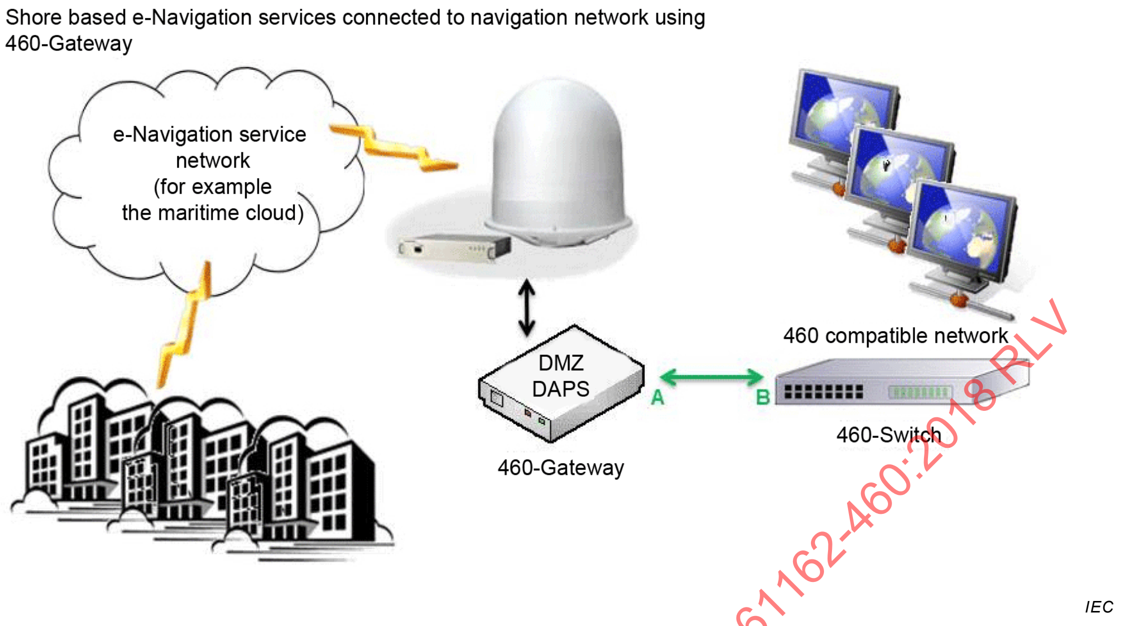

Shore based e-Navigation services connected to navigation network using 460-Gateway
e-Navigation service network (for example the maritime cloud)
DMZ
DAPS
A
B
460-Gateway
460 compatible network
460-Switch
IEC

Figure D.3 – 460-Gateway used for e-Navigation services

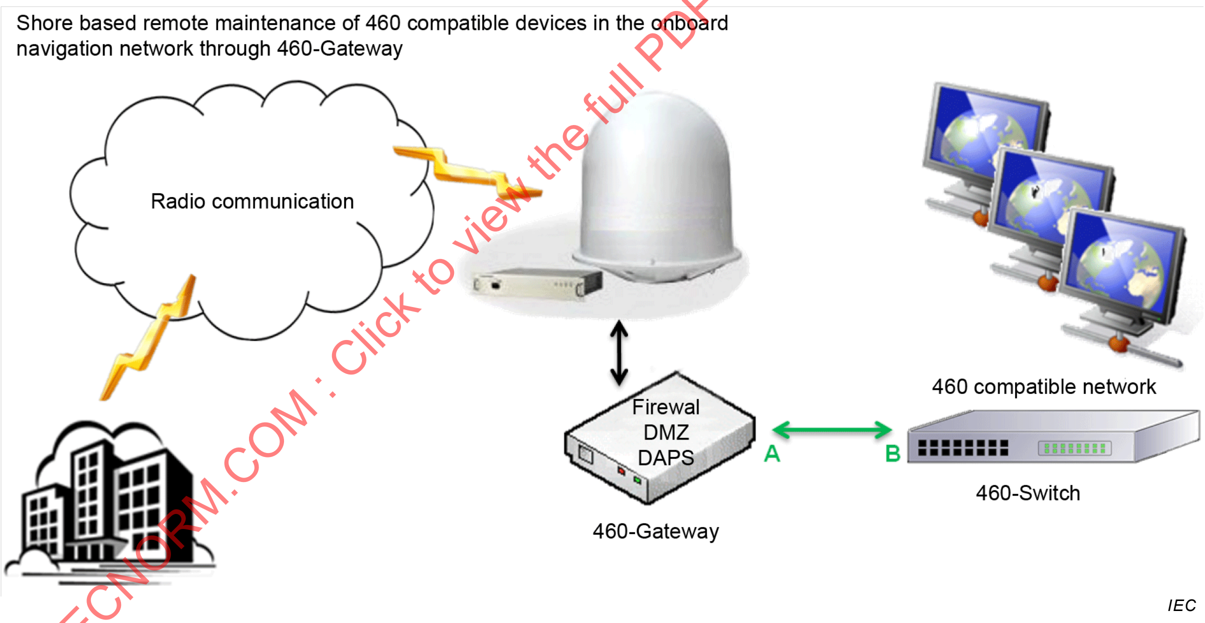

Shore based remote maintenance of 460 compatible devices in the onboard navigation network through 460-Gateway
Radio communication
Firewal
DMZ
DAPS
A
B
460-Gateway
460 compatible network
460-Switch
IEC

Figure D.4 – 460-Gateway used for remote maintenance

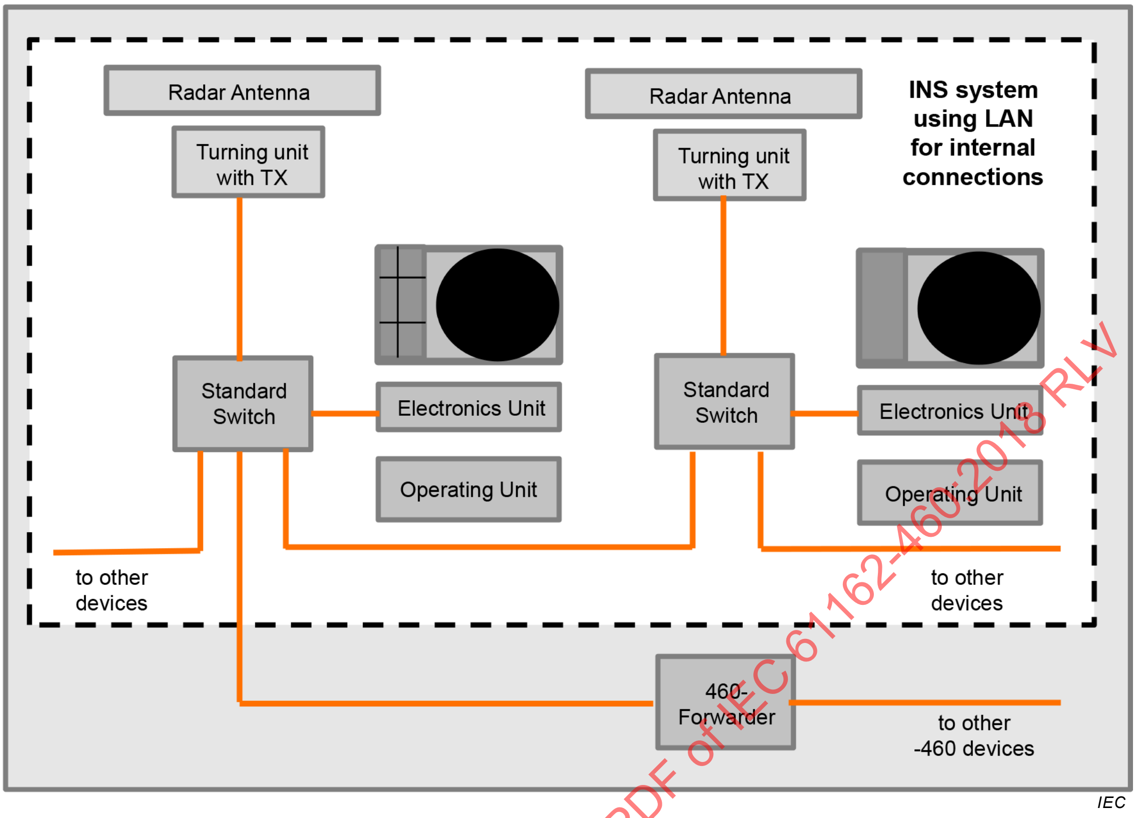


Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices

Figure D.5 shows an example of an INS system fulfilling requirements of IEC 61924-2. This INS system uses internally Local Area Network technology to connect various components of the INS system. Figure D.5 shows how a 460-Forwarder is used to separate this INS system into its own controlled network.

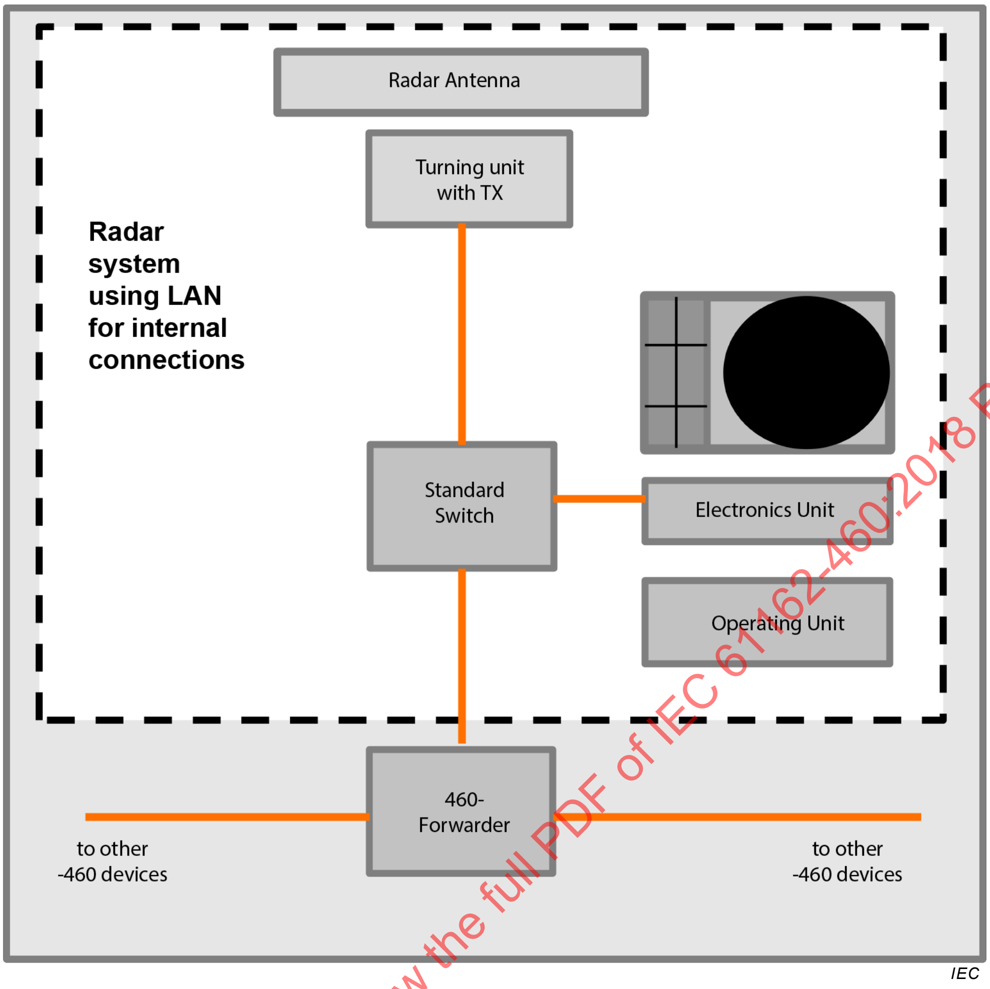


Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices

Figure D.6 shows an example of a radar system fulfilling requirements of IEC 62388. This radar system uses internally Local Area Network technology to connect various components of the radar system. Figure D.6 shows how a 460-Forwarder is used to separate this radar system into its own controlled network.

Annex E
(normative)

IEC 61162 interfaces for the network monitoring function

The network monitoring function shall be capable of at least transmitting and receiving data with the optional logical interfaces in Figure E.1 using the sentences specified in Table E.1 and Table E.2.

Figure E.1 shows the logical interfaces. If more than one logical interface is implemented on a single physical interface then all aspects of each logical interface, including alert communication, heartbeat, etc. shall be distinguishable from those of other logical interfaces implemented on the same physical interface.

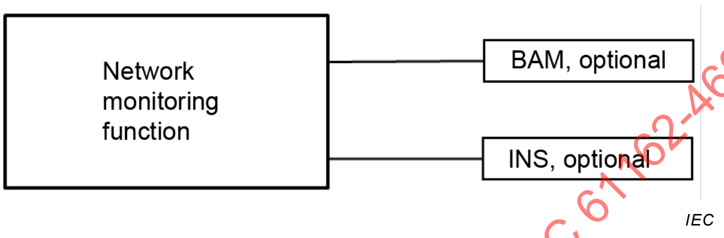


Figure E.1 – Network monitoring function logical interfaces

Table E.1 and Table E.2 specify sentences which can be used with interface alternatives IEC 61162-1, IEC 61162-2 and IEC 61162-450. The manufacturer shall specify which interface is supported.

Table E.1 – Sentences received by the network monitoring function

Mnemonic	Interface (see Figure E.1)	Name	Comment
ACN~~[a]~~	BAM, INS	Alert command	Alert command, e.g. acknowledge
HBT~~[b]~~	BAM, INS	Heartbeat	Support reliable alert related communication Repeated once per 1 min

~~[a] See IEC 61924-2.~~

~~[b] See IEC 61162-1.~~

Table E.2 – Sentences transmitted by the network monitoring function

Mnemonic	Interface (see Figure E.1)	Name	Comment
ALC~~[a]~~	BAM, INS	Cyclic alert list	List of current alert
ALF~~[a]~~	BAM, INS	Alert sentence	Details of a new alert
ARC~~[a]~~	BAM, INS	Alert command refused	Alert command not accepted
HBT~~[b]~~	BAM, INS	Heartbeat	Support reliable alert related communication

~~[a] See IEC 61924-2.~~

~~[b] See IEC 61162-1.~~

Annex F
(informative)

Distribution of functions around 460-Network

Annex F provides guidance about the distribution of various functions around components of the 460-Network.

Table F.1 – Distribution of functions around 460-Network

Function	460-Node	460-Switch	460-Forwarder	460-Gateway
No REDS or external networks(6.2.3, 6.2.4.2)	✓	✓	✓	✓
Syslog implemented (source) (8.1)	✓	✓	✓	✓
Data output bandwidth defined (5.1, 6.2.2.1)	✓	✓	✓	✓
ONF specified (4.4.1, 4.4.2, 5.1)	✓			
Network traffic management (5.1)	✓	✓	✓	
Security – no wireless (6.2.1)	✓		✓	
Security – excessive traffic protection (6.2.2.1, 5.3.3)	✓		✓	
Security – DoS Attack ICMP IGMP protection (6.2.2.2)	✓		✓	
Security – access control (password) (6.2.4.1)	✓	✓	✓	✓
Redundancy (7.1, 7.2)	✓	As installed ✓	As installed ✓	✓
Network monitoring	✓(for at least one node or switch, 8.2.1)	✓(for at least one node or switch, 8.2.1)		✓ (list of connections)
If applicable – application level check of external network packets (4.4.2)	✓			
If applicable – REDS security (6.2.3)	✓			
If applicable – direct connection only with admin permission (6.3.3, 6.3.4, 6.3.5)	✓			
Configuration of network flows (5.2.1, 5.3.2)		✓	✓	
Allocation of bandwidth (5.2.1, 5.3.2)		✓	✓	
In/out traffic in register allowed, deny other traffic (6.2.4.2)		✓		
If applicable – VLAN config per interface (5.2.1)		✓		
IGMP multicast snooping (5.2.1)		✓		
Syslog (sink)	✓(for at least one node or switch, 8.2.1)	✓(for at least one node or switch, 8.2.1)		
Caution/warning source (6.3.4, 6.3.5, 8.2.7.1)	✓	✓		✓
Caution/warning sink	External CAM of BAM			
Firewall (6.3.2)				✓

Table F.2 – Equipment standards referencing IEC 61162-460

Standard	460-Node	460-Switch	460-Forwarder	460-Gateway
IEC 62940:2016, ICS, 5.1.1				✓

Bibliography

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61162 (all parts), *Maritime navigation and radiocommunication equipment and systems – Digital interfaces*

IEC 61162-1, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 1: Single talker and multiple listeners*

IEC 61162-2, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 2: Single talker and multiple listeners, high-speed transmission*

IEC 62388, *Maritime navigation and radiocommunication equipment and systems – Shipborne radar – Performance requirements, methods of testing and required test results*

IEC 62439 (all parts), *Industrial communication networks – High availability automation networks*

IEC 62439-1, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*

IEC 62439-2, *Industrial communication networks – High availability automation networks – Part 2: Media Redundancy Protocol (MRP)*

IEC 62439-3, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

IEC 62439-4, *Industrial communication networks – High availability automation networks – Part 4: Cross-network Redundancy Protocol (CRP)*

IEC 62439-5, *Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)*

IEC 62439-6, *Industrial communication networks – High availability automation networks – Part 6: Distributed Redundancy Protocol (DRP)*

IEC 62940, *Maritime navigation and radiocommunication equipment and systems – Integrated communication system (ICS) – Operational and performance requirements, methods of testing and required test results*

ISO/IEC 10118-3, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO 9241-12, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 12 – Presentation of information*

ISO 16425, *Ships and marine technology – Guidelines for the installation of ship communication networks for shipboard equipment and systems*

IMO Resolution MSC.302(87), *Performance standards for bridge alert management (BAM)*

CIGRE B5-109, *Redundancy challenges on IEC 61850 systems and Migration Paths for IEC 61850 Substation Communication Networks*

~~IEEE 802.1Q, *Virtual bridged local area networks*~~

IEEE 802.3, *IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

IEEE 802.10, *IEEE Standard for Interoperable LAN/MAN Security (SILS)*

IEEE 802.11, *Wireless Local Area Networks*

IEEE 802.15.4, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*

IEEE 1363, *IEEE Standard Specifications for Public-Key Cryptography*

ISOC RFC 768, *User Datagram Protocol (UDP), Standard STD0006*

ISOC RFC 791, *Internet Protocol (IP), Standard STD0005 (and updates)*

ISOC RFC 793, *Transmission control protocol (TCP)*

ISOC RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets*

ISOC RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

ISOC RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

ISOC RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

Universal Serial Bus Revision 2.0 specification. Available at www.usb.org

Universal Serial Bus Revision 3.1 specification. Available at www.usb.org

____

IEC 61162-460

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

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

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

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

a) 460-Switches and 460-Forwarders are required to implement IGMP snooping;

b) connection between secure and non-secure areas requires a 460-Forwarder as an isolation element;

c) SFI collision detection added as function of network monitoring;

d) 460-Gateway and 460-Wireless gateway are no longer required to report to the network monitoring;

e) all alerts from network monitoring have standardized alert identifiers.

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

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

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

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

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

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

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

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

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

1 Scope

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

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

3.1
450-Node
device compliant with IEC 61162-450 and which satisfies additional requirements specified in this document

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

3.2
460-Forwarder
network infrastructure device that can safely exchange data streams between a 460-Network and other controlled networks including other 460-Networks

3.3
460-Gateway
network infrastructure device that connects 460-Networks and uncontrolled networks and which satisfies the safety and security requirements as specified in this document

3.4
460-Network
network which consists of only 460-Nodes, 460-Switches, 460-Forwarder, 460-Gateway and 460-Wireless gateway as well as 450-Nodes

3.5
460-Node
device compliant with the requirement of a 450-Node and which satisfies the safety and security requirements as specified in this document

3.6
460-Switch
network infrastructure device used to interconnect nodes on a 460-Network and which satisfies the safety and security requirements as specified in this document

3.7
460-Wireless gateway
network infrastructure device that connects a 460-Network and wireless networks and which satisfies the safety and security requirements as specified in this document

3.8
advanced encryption standard
AES
symmetric-key block cipher algorithm which is based on a substitution-permutation network (SPN) and does not use the data encryption standard (DES) Feistel network

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

3.9
alarm
highest priority of an alert, announcing a situation or condition requiring immediate attention, decision and, if necessary, action by the bridge team, to maintain the safe navigation of the ship

3.10
application level gateway
network infrastructure device that connects 460-Networks with other networks and which satisfies the safety and security requirements as specified in this document

3.11
backdoor
installed program allowing remote access to a computer by providing a method of bypassing normal authentication

3.12
controlled network
any network that has been designed to operate such that authorities are satisfied by documented evidence that the network does not pose any security risks to any connected network nodes

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

3.13
category B alert
alert where no additional information for decision support is necessary besides the information which can be presented at the central alert management HMI

3.14
caution
lowest priority of an alert

Note 1 to entry: "Caution" raises a bridge team's awareness of a condition which does not warrant an alarm or warning condition, but still requires attention out of the ordinary consideration of the situation or of given information.

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

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

3.16
denial of service
DoS
attempt to prevent legitimate users from accessing a machine or network resource

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

3.17
flow
combination of the following information: source and destination MAC address, source and destination IP address, protocol, source and destination port number

3.18
failure mode and effects analysis
FMEA
method as specified in IEC 60812 for the analysis of a system to identify the potential failure modes, their causes and effects on system performance

3.19
failure mode, effects and criticality analysis
FMECA
analytic method as specified in IEC 60812 that includes a means of ranking the severity of the failure modes

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

3.20
internet control message protocol
ICMP
protocol according to ISOC RFC 792

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

3.21
internet group management protocol
IGMP
protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and ISOC RFC 4604 (version 3)

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

3.22
loss rate
amount of lost data by the receiving device of a flow as lost packets per total amount of packets, measured at the input port of a device

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

3.23
malware
malicious code
software used or created to disrupt computer operation

3.24
maximum network load
cumulative maximum amount of all traffic from all network nodes and network infrastructure components of a single 460-Network

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

3.25
maximum transmission rate
maximum number of bytes per second that can be transmitted by a network node or network infrastructure equipment

3.26
multiple spanning tree protocol
MSTP
protocol, according to IEEE 802.1Q, which is an extension of RSTP for VLANs

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

3.27
neighbour MAC address
MAC (media access control) address of connected 450-Node or 460-Node as seen by 460 Switch and as reported by SNMP (simple network management protocol)

3.28
network infrastructure component
device that connect at least two nodes in a 460-Network and two different networks, such as 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

3.29
nominal network capacity
network capacity as a byte rate which is based on the configuration

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

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

3.30
other network function
ONF
function block that interfaces to the network as specified in IEC 61162-450

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

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

3.31
rapid spanning tree protocol
RSTP
protocol according to IEEE 802.1D for calculating and configuring the active topology of a network

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

3.32
removable external data source
REDS
user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth[1] 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.

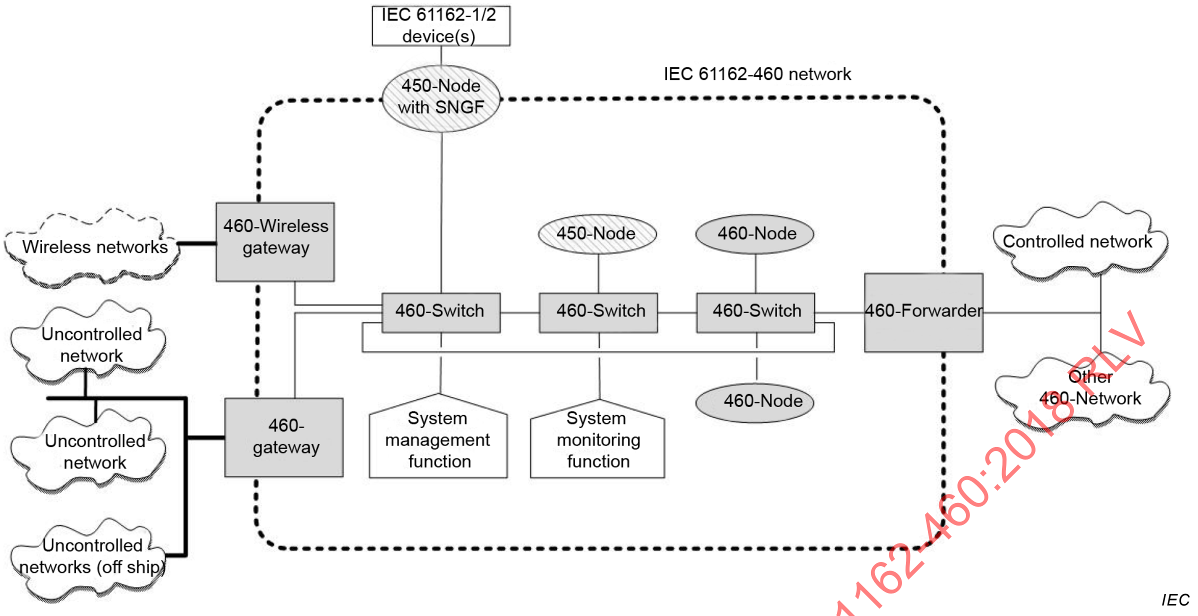


Figure 1 – Functional overview of IEC 61162-460 requirement applications

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

4.3 General requirements

4.3.1 Equipment and system requirements

(See 10.3)

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

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

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

All network nodes, network infrastructure components and cables shall satisfy the requirements in Clauses 4 and 5 of IEC 61162-450:2018.

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

The list can be a label or list or equivalent.

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

4.3.2 Physical composition requirements

(See 10.12.3.1)

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

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

4.3.3 Logical composition requirements

(See 10.12.3.1)

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

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

4.4 Physical component requirements

4.4.1 450-Node

(See 10.4)

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

- no connection to external networks or REDS;
- syslog implemented as defined IEC 61162-450:2018, 4.3.3.2;
- data output bandwidth documented by the manufacturer as described in 6.2.2.1;
- implemented ONF services specified by the manufacturer, including the necessary protocol parameters, at least IP address and port number;
- ephemeral ports, if used, indicated by the manufacturer.

4.4.2 460-Node

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

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

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

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

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

- – if a connection with the controlled network is used to forward unmodified datagrams between the 460-Network and controlled networks or other 460-Networks, then this forwarding shall be handled by a 460-Forwarder;

- support for REDS as specified in 6.2.3;
- direct connection with uncontrolled networks as specified in 6.3.4;
- VLAN compatibility as specified in 5.1;
- implemented ONF services specified by the manufacturer including the necessary protocol parameters, at least IP address and port number;
- ephemeral ports if used indicated by the manufacturer.

4.4.3 460-Switch

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

- network traffic management as specified in 5.2;
- security requirement as specified in 6.2.1, 6.2.2.2, 6.2.4 and 6.4;
- network monitoring as specified in 8.1.3;
- VLAN compatibility, if provided, as specified in 5.2.1.

4.4.4 460-Forwarder

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

- network traffic management as specified in 5.3;
- security requirements as specified in 6.2.1, 6.2.2.2, 6.2.4 and 6.4;
- network monitoring as specified in 8.1.4;
- VLAN functionality to combine two physical networks (controlled networks and other 460-Networks) into a logical network, if provided, as specified in 5.3.

4.4.5 460-Gateway and 460-Wireless gateway

Connections to uncontrolled networks shall be protected by a gateway fulfilling the requirements for a 460-Gateway as specified in 6.3.5 or a 460-Wireless gateway as specified in 6.3.6. Security requirements as specified in 6.2, 6.3 and 6.4 shall be implemented.

4.5 Logical component requirements

4.5.1 Network monitoring function

The network monitoring function shall perform the following functions:

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

4.5.2 System management function

(See 10.12.2)

The system management function shall perform the following functions:

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

The system management function shall be redundantly available.

4.6 System documentation requirements

(See 10.12.3.1)

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

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

See also 5.4.

4.7 Secure area requirements

(See 10.12.3.1)

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

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

5 Network traffic management requirements

5.1 460-Node requirements

(See 10.5.1)

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

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

  NOTE 1 Chart update is an example of ONF.

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

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

- device behaviour shall be specified by the manufacturer when its maximum input data rate is exceeded. The input data rate shall be expressed in bytes per second as available in the network line including all protocol-specific overheads;
- only data specified 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, 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 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 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 port;
- if VLAN is provided, a means to configure virtual networks (VLAN) per interface shall be provided;
- if VLAN is provided, VLAN protocol IEEE 802.1Q 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 IEEE 802.1Q 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 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 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 means shall be provided for traffic prioritisation at a 460-Forwarder:

a) means to handle dropping of lower priority traffic based on priority;

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

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

c) means to continue lossless traffic in each priority until the amount of traffic to be transferred is higher than 100 % of the set maximum as set for the priority in the switch;

d) means to report the use of dropping by syslog for each period of 30 s during which the dropping has been used or by responding to SNMP-Trap method (i.e. by requesting RMON alerts) about the use of dropping (see 8.2.2).

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

5.4 System design requirements

5.4.1 Documentation

(See 10.12.3.2)

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 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

(See10.5.2.1, 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 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 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.

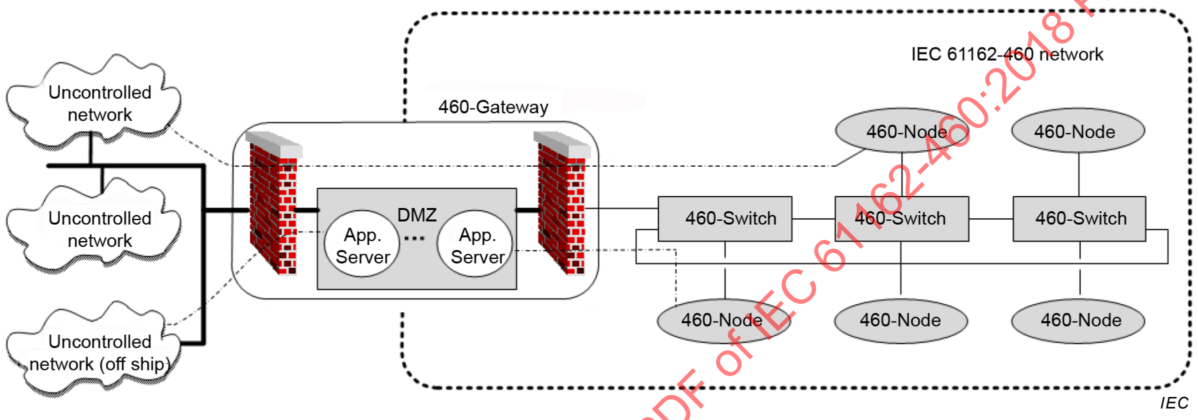


Figure 2 – 460-Network with 460-Gateway

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).

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; 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, 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 a pre-defined time period;
- all connections between uncontrolled networks and a 460-Node shall satisfy 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;
- 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 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 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 Samba[2]) 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)

[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.

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)

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.

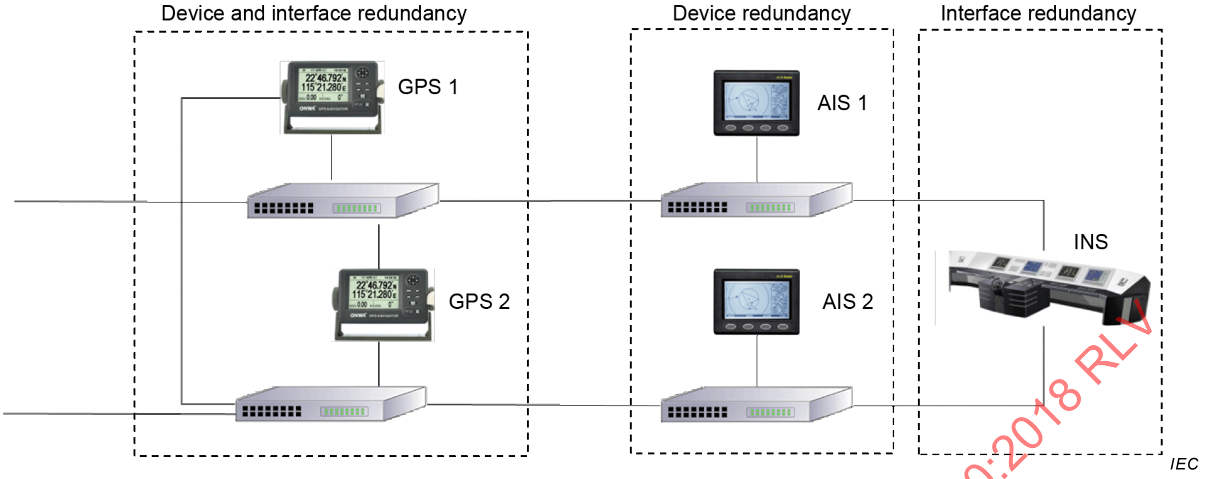


Figure 3 –Example of redundancy

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, 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, whenever significant changes (traffic is more than 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) 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, 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 reported by a 460-Forwarder in the same way as for a 460-Switch (see 8.1.3).

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 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 the functionality of the alert management and shall provide human machine interface (HMI) to access the alert 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.

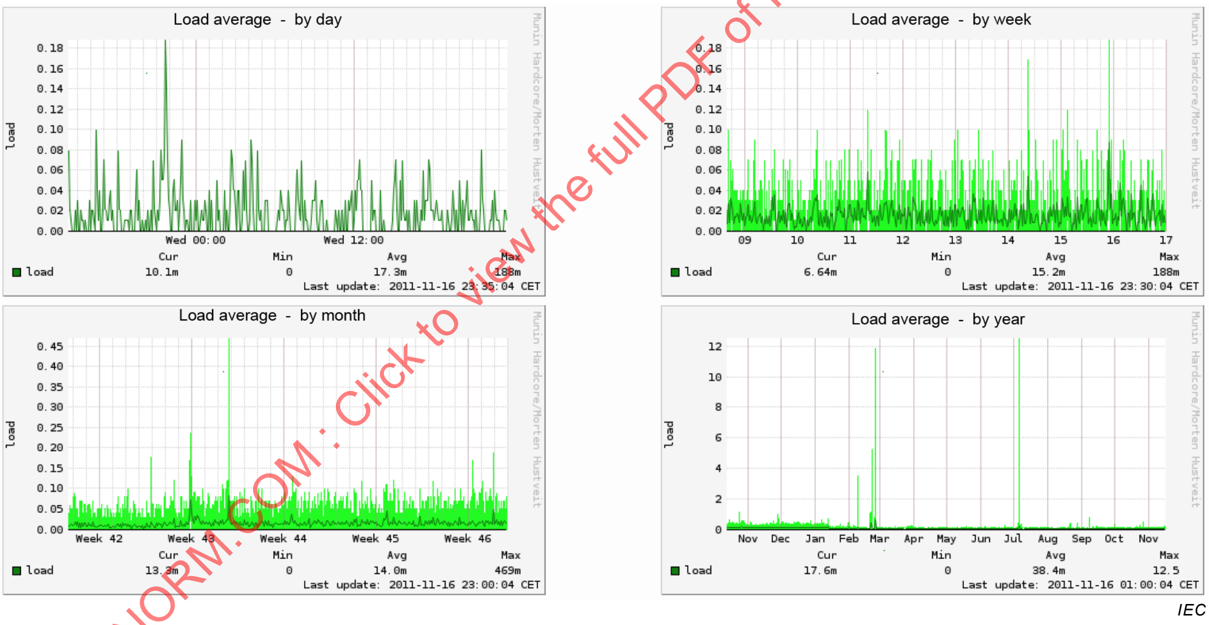


Figure 4 – Example of network status recording information

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 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 statistics) and periodic SNMP query every 15 min;

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

The network monitoring function shall 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 use at least one of the alternatives below to collect information from the 460-Switches and 460-Forwarders as specified in 8.1.3 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 20 000 messages. The recorded syslog messages shall be available for at least the last 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.

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.

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 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 Wireshark[3]).

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 61162-450:2018.

[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 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)

Confirm by analytic evaluation that 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 61162-450:2018, 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 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 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 IEEE 802.1Q.

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 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 the direct connection.

For each direct data exchange, confirm by observation that:

- there is a permanent indication when direct connection is active;
- a caution is created when the direct connection is activated;
- if provided, the caution is replaced by a warning after 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 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 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 IEEE 802.1Q 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 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 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 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 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 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.

10.7 460-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 IEEE 802.1Q.

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 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 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 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 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 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.

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

10.8.3 Communication security

(See 6.3.3)

Confirm by inspection of manufacturer's documentation that a direct connection between uncontrolled networks and a 460-Network can only be enabled from a 460-Gateway or from a 460-Wireless gateway.

Use a simulation arrangement to establish a VPN connection originating at the EUT between 460-Network and uncontrolled network. Confirm by analytical evaluation that VPN is provided over the connection.

Confirm by inspection of the documented evidence that the encryption algorithm used for VPN meets the requirement of encryption strength as follows:

- an asymmetric encryption algorithm with at least a 2 048-bit key length (256 B);
- symmetric encryption algorithm with at least a 256-bit key length (32 B).

Confirm by inspection of the documented evidence that the delivery of certificates is based on a chain of trust or that the private keys/certificates are exchanged in secure manual way or using a combination of manual methods and messages.

10.8.4 Firewall

(See 6.3.5.1)

Confirm by analytical evaluation that all direct connections to the 460-Network are disabled in the manufacturer's default configuration.

Set an EUT between 460-Networks and uncontrolled networks. Set a ping generator to 20 different IP addresses for the address range of the uncontrolled network, 460-Network and DMZ. Confirm by analytical evaluation that the following packets do not pass through the EUT:

- ping test to the internal address range of the 460-Network;
- ping test to address a range of DMZ of the EUT;
- ping test to address a range of uncontrolled networks.

Confirm by observation that the EUT registers traffic as an external/internal firewall rule which consists of source and destination IP address, protocol and port number.

Confirm by observation that the EUT provides a means to list all direct connections for the last 12 months.

Confirm by analytical evaluation that the EUT provides means to list activated direct connections between 460-Networks and uncontrolled networks with status information for each of these connections including: source IP address, destination IP address, starting time and end time of the connection, protocol, and port number.

Confirm by analytical evaluation that means provided to allow direct connection with a 460-Node from an uncontrolled network can only be activated by an operation on the 460-Network side of the firewall. Confirm by inspection of the manufacturer's documentation that this cannot be activated from uncontrolled networks. Confirm that means are provided to ensure that the operation can only be performed after obtaining permission, for instance from the bridge officers.

Confirm by observation that the EUT terminates all direct connection automatically after a predefined time not exceeding 4 h unless there is user intervention to extend the time.

Confirm by observation that the EUT terminates all direct connection automatically after the connection is idle for a pre-defined time not exceeding 10 min.

If direct connection between 460-Networks and an uncontrolled network is provided, either confirm by observation that the activated state is indicated or confirm by analytical evaluation that the activated state generates a caution.

NOTE The generation and presentation of the caution can be performed by the device presenting the alerts for network monitoring.

10.8.5 Application server

(See 6.3.5.2)

Confirm by inspection of the manufacturer's documentation that an application server provides means to authenticate clients connected over uncontrolled networks, for example by password.

Confirm by analytical evaluation that Layer 3 forwarding or routing is disabled (i.e. no routing of packets is allowed).

Verify compliance with 460-Node requirements in accordance with 10.5.

Confirm by inspection of the manufacturer's documentation that means for protection from malware are described as appropriate to the computer platform.

10.8.6 Interoperable access to file storage of DMZ

(See 6.3.5.3)

Confirm by observation that a file can be downloaded and uploaded between the DMZ and uncontrolled networks if provided.

Confirm by observation that a file can be downloaded and uploaded between the DMZ and 460-Networks if provided.

If access to the file storage within the DMZ is provided, confirm by inspection of the manufacturer's documentation that a protocol is provided, such as SMB or SFTP.

If implemented, confirm by inspection of the documented evidence that the EUT access to file storage and related data traffic of DMZ satisfies the requirements for ONF, NF as specified in IEC 61162-450 and the 460-Node.

10.8.7 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.

10.9 460-Wireless gateway

10.9.1 General

Confirm by inspection of documented evidence that the EUT satisfies the requirements of the 460-Gateway (see 10.8).

10.9.2 Security

(See 6.3.6)

Confirm by observation that wireless access point (AP) functions are not activated.

Confirm by observation that the forwarding function is not allowed.

Confirm by the manufacturer's documentation that all traffic to a 460-Network is compliant with IEC 61162-450 traffic.

Confirm by inspection of the documented evidence that the encryption algorithm used for VPN meets the requirement of encryption strength as follows:

- an asymmetric encryption algorithm with at least a 2 048-bit key length (256 B);
- symmetric encryption algorithm with at least 256-bit key length (32 B).

Activate wireless AP and confirm by observation that all connections to wireless AP are established only with authentication.

10.10 Controlled network

(See Clause 9)

Confirm by inspection of the documented evidence that the controlled network is not able to insert non-authorised traffic into the network, neither by direct access to the physical infrastructure nor through, for example, wireless interface.

Confirm by inspection of the documented evidence that the controlled network provide means to prevent direct access to operating systems or functions that can be used to insert non-authorised traffic into the network, unless this user is specially authorised to perform these operations.

Confirm by inspection of the documented evidence that the controlled network provides means to prevent transferring data from a non-authorised REDS or a REDS with un-authorised contents to any node or device in the network.

10.11 Network monitoring function

10.11.1 General

(See 8.2.1)

If the EUT does not provide network monitoring function, confirm by inspection of installation documentation that the EUT shall only be connected to a network in which another equipment provide network monitoring function.

Confirm by observation that the EUT provides monitoring either through a local human machine interface or an alert management interface.

If compatibility for bridge installation has been declared by the manufacturer, confirm by observation that the EUT provides an alert management interface.

Set a simulation arrangement to cause cautions and warnings. Confirm by observation that the EUT reports all alerts and is capable of accepting responsibility transferred, remote acknowledge and remote silence commands if an alert management interface is provided.

Set a simulation arrangement to cause cautions and warnings, and to generate events and reports from 460-Switches and 460-Forwarders. Confirm by observation that all alerts from the network monitoring function and, events and reports from 460-Switches and 460-Forwarders are recorded in the EUT.

Confirm by the documented evidence that the EUT has a capability to store events for at least the last 3 months or last 10 000 events, whichever is smaller, together with the capability of displaying the information.

10.11.2 Network load monitoring function

(See 8.2.2)

Confirm by observation that the system documentation includes an analysis for every switch and between switches, forwarders and gateways of the maximum network load.

Use the simulation arrangement and confirm by observation that the EUT requests the traffic flow information from all 460-Switches and 460-Forwarders either periodically every 30 s using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from SNMP or syslog or a combination of both for the following functionality:

a) generate cautions when the observed network load exceeds the 80 % limit of its maximum network capacity for a period of 30 s more than 3 times within a period of 10 min.

b) generate warnings when the observed network load has exceeded the 80 % limit of the maximum network capacity for a period of 30 s more than 10 times within a period of 10 min.

10.11.3 Redundancy monitoring function

(See 8.2.3)

Confirm by observation that the system documentation includes a list of data sources that are redundantly available.

Confirm by observation that the list provides the names of data sources, two or more MAC addresses, interface number and interface available alternatives for each redundant network address from which this data is available.

Use the simulation arrangement and confirm by observation that the EUT requests the network configuration information from all 460-Switches and 460-Forwarders either periodically every 30 s using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from both SNMP and syslog to generate cautions when fewer than two MAC addresses, or one MAC address with fewer than two interfaces available for a source of data in the list, has been lost for a period of 2 min for all SNMP requests performed every 30 s by the EUT.

Confirm by observation that the caution complies with the requirement.

10.11.4 Network topology monitoring function

(See 8.2.4)

Confirm by observation that the system documentation includes a list of accepted devices.

Use the simulation arrangement and confirm by observation that the EUT requests the network topology information from all 460-Switches and 460-Forwarders either periodically every 30 min using SNMP query or using a combination of SNMP-Trap method and periodic SNMP query every 15 min.

Use the simulation arrangement and confirm by observation that the EUT is able to use information from SNMP or syslog or a combination of both to generate cautions when a MAC address, which is not included in the list of accepted devices, has been found.

Use the simulation arrangement and confirm by observation that the EUT creates the SFI Table based on received SRP sentences.

Use the simulation arrangement to include multiple, at least two, different SFI with any value of "Instance number of redundant alternative", any MAC address or any IP address reported by the SRP sentences, and confirm by observation that the EUT does not generate a caution.

Use the simulation arrangement to include two equal SFI, both with "Instance number of redundant alternative" fields of SRP sentence set as different values and with equal IP addresses reported by the SRP sentences and confirm by observation that the EUT does not generate a caution.

Use the simulation arrangement to include two equal SFI, both with "Instance number of redundant alternative" fields of SRP sentence set as null or set as same number and with different MAC addresses reported by the SRP sentences and confirm by observation that the EUT generates a caution.

Confirm by observation that the cautions comply with the requirements.

10.11.5 Syslog recording function

(See 8.2.5)

Set a simulation arrangement to cause syslog messages. Confirm by observation that the network monitoring function provides recording and internal or external possibility to view the syslog information from the 450-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways in 460-Network.

Confirm by inspection of the documented evidence that the minimum capacity of the recording is 100 000 messages and that the recorded syslog messages are available at least for the last 30 days.

10.11.6 Alert management

10.11.6.1 Alerts and indications

(See 8.2.7.1)

Confirm by analytical evaluation that the alerts comply with the criteria as required in Table 2.

10.11.6.2 Alert management interface

(See 8.2.7.2)

Confirm by inspection of the manufacturer's documentation that manufacturer defined alerts are in compliance with the criteria for classification and categories of alerts defined in IEC 61924-2:2012, 8.3.

In order to test the communication and presentation of the alerts, refer to the manufacturer's documentation to identify at least 1 of the available warnings, which may be chosen at random, and 2 of the available cautions, which may be chosen at random. Then, perform the following test using a simulator for BAM:

- confirm by analytical evaluation that the alert communication complies with the sentences listed in Annex E and the state diagram of IEC 61924-2:2012, Annex J;

- confirm by analytical evaluation that, if means are provided to interface to a centralised alert management system, a caution alert is provided when the periodic receptions of the HBT sentence are interrupted.

10.11.6.3 Unacknowledged warnings

(See 8.2.7.3)

Confirm by inspection of the manufacturer's documentation that the default value for alert escalation is 60 s.

Confirm by observation that the user selectable time period for alert escalation is less than 5 min.

Confirm by inspection of the manufacturer's documentation that the manufacturer provides information about:

- which warnings are repeated as warning;
- which warnings are changed to alarms after the user-selectable time period;
- which warnings are changed to alarms after the manufacturer's fixed time period.

Refer to the manufacturer's documentation to identify at least 2 cases, which may be chosen at random, if available, in which a warning is repeated as warning. Confirm by observation that the time between repetitions is as selected by the user.

Refer to the manufacturer's documentation to identify at least 2 cases which may be chosen at random, if available, in which a warning is changed to alarm. Confirm by observation that the time before change of priority is as selected by the user.

10.11.6.4 Remote acknowledgements and silencing of alerts

(See 8.2.7.4)

Create 2 alerts, at least one of category B. Confirm by observation that ALF, ALC and HBT (if the EUT supports ‘responsibility transfer’) sentences are transmitted from the EUT to the alert management interface.

Use a simulator to send an ACN sentence to the EUT to silence one of the alerts. Confirm by observation that ALF, ALC and HBT (if provided) sentences report correctly the new state of the alerts.

Use a simulator to send an ACN sentence to the EUT to acknowledge the category B alert. Confirm by observation that ALF, ALC and HBT (if provided) sentences report correctly the new state of the alerts.

10.12 System level

10.12.1 General

Subclause 10.12 contains methods of testing and required results for system level confirmation of the requirements. The system level confirmation may be performed for:

- a typical system setup, as described by the applicant of conformance testing; or
- a real onboard installation, as described by the applicant of conformance testing.

The system level conformance testing is based on real-life equipment instead of simulation arrangements. The target of system level conformance testing is to prove that a real life system consisting of network infrastructure and equipment (for example navigation instruments like radar, ECDIS, gyro-compass) fulfil the system requirements of this document.

The basis of system-level conformance is that each individual component has been beforehand separately tested according to this document for the corresponding individual function(s) – see 10.4 to 10.9.

The minimum system for system level conformance testing consists at least of the following functions:

- two 460-Switches;
- two nodes of either type 450-Node or 460-Node; and
- a network monitoring function.

The test site requirements are:

- a network protocol analyser (for example Wireshark[4]) for monitoring of traffic;
- an arrangement capable of injecting more network traffic into the 460-Switches using IEC 61162-450 compliant data and non IEC 61162-450 compliant data (for example TCP/IP, UDP/IP, multicast and broadcast) to increase the network line load from the normal network load level up to the 100 % line load;
- an arrangement capable of injecting DoS attack into the 460-Switches.

10.12.2 System management function

(See 4.5.2)

Confirm by observation that the configuration information for a 460-Switch can be stored in the system. Replace a 460-Switch with another un-configured 460-Switch. Confirm by observation that, by using a system management function, it is possible to restore the original configuration to the new 460-Switch. This test shall be repeated for all 460-Switches and 460-Forwarders.

Remove one 460-Node and replace it with another equivalent device with a different MAC address. Confirm by observation that, by using the system management function, it is possible to change the original configuration to accept the new device.

Switch off the first system management function or if EUT has interface redundancy, disconnect one cable. Confirm by observation that the second system management function is available.

10.12.3 System design

10.12.3.1 General

(See 4.3.2, 4.3.3, 4.6, 4.7)

Confirm by inspection of documented evidence that the following information is provided:

- the topology and devices of the network, including networks in a secure area, if provided;
- that the network consists of only 460-Network physical components, 460-Network nodes and network infrastructure components;
- that all networks connected with a 460-Forwarder are either controlled networks or other 460-Networks.

Confirm by inspection of documented evidence that both a network monitoring function and a system management function are available in the network.

[4] 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.

10.12.3.2 Documentation

(See 4.6, 5.4.1)

Confirm by inspection of documented evidence that the following information is provided:

- the 460-Network traffic flow analysis and network topology;
- the total amount of network traffic and 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 if provided;
- the prioritization of each traffic type at each 460-Forwarder if provided;
- an analysis of the maximum network load;
- a list of data sources which are redundantly available;
- a list of accepted devices.

10.12.3.3 Network traffic design

(See 5.4.2)

Confirm by inspection of the document evidence that the amount of bandwidth allocated at each 460-Switch is more than, or equal to, the sum of all traffic volumes of each traffic class allocated to the network connected to the switch.

Use a network design document and select three ports to confirm by observation that the measured traffic is lower than or equal to the defined value of sum of traffic load. Confirm by observation that the average load of all traffic in a 460-Network does not exceed 95 % of the nominal network capacity planned over a period of 1 s and does not exceed 80 % of the nominal network capacity planned over a period of 10 s.

10.12.3.4 Loop prevention

Use a network design document and select at least two 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.

10.12.3.5 Resource allocation

Confirm by inspection of the document evidence that the amount of bandwidth allocated at each 460-Forwarder is more than, or equal to, the sum of all traffic volumes of each traffic class allocated to the network connected to the 460-Forwarder.

Use a network design document and select two ports to confirm by observation that the measured traffic is lower than, or equal to, the defined value of the sum of the traffic load.

10.12.3.6 Traffic prioritisation

If available in the system under test, select two traffic flows with different priority for which connected 460-Node based devices show activity. Use a simulation arrangement to inject additional traffic with a priority level between two selected priorities up to full line load. Confirm by observation that the device using highest priority traffic flow continues to show activity while the device using lowest priority traffic is distorted.

10.12.3.7 Denial of service behaviour

Use a network design document and select three 460-Nodes to inject additional traffic flows up to line load for 1 h. If the number of 460-Nodes is less than three, select all 460-Nodes. Confirm by observation that 460-Nodes continue their normal operation as stand-alone devices. Remove the injected additional traffic and confirm by observation that 460-Nodes resume their operation based on information received from the 460-Network.

10.12.3.8 Uncontrolled network security

If the system under test includes a 460-Gateway, repeat all tests as described in 10.8.

If the system under test includes a 460-Wireless gateway, repeat all tests as described in 10.9.

10.12.3.9 Connections between secure and non-secure areas

If the system under test includes a connection between a 460-Network installed in a secure area and a 460-Network installed in a non-secure area, repeat all tests as described in 10.7.

10.12.3.10 Redundancy

(See 7.1, 7.7)

Confirm by inspection of documented evidence that FMEA or FMECA is available for its redundancy capability and critical nodes are identified, and that no single points of failure affect the functionality of the critical nodes.

Use FMEA or FMECA documents and select 20 % of critical devices or at least three devices as representative devices. Cause a single failure one by one for each representative device and confirm by analytical evaluation that redundant devices continue normal operation within 5 s.

Select two traffic flows for connected 460-Node-based devices and show activities. Disconnect a cable between two 460-Switches and confirm by analytical evaluation that the interruption of data transfer is 5 s or less.

10.12.4 Network monitoring function

For the network monitoring function, repeat all tests as described in 10.11.1.

10.12.5 Network load monitoring function

For network load monitoring function, repeat all tests as described in 10.11.2.

10.12.6 Redundancy monitoring function

For network redundancy monitoring function, repeat all tests as described in 10.11.3.

10.12.7 Network topology monitoring function

10.12.7.1 General

For network topology monitoring function, repeat all tests as described in 10.11.4.

10.12.7.2 Syslog recording function

For syslog recording function, repeat all tests as described in 10.11.5.

10.12.7.3 Redundancy of network monitoring function

(See 8.2.6)

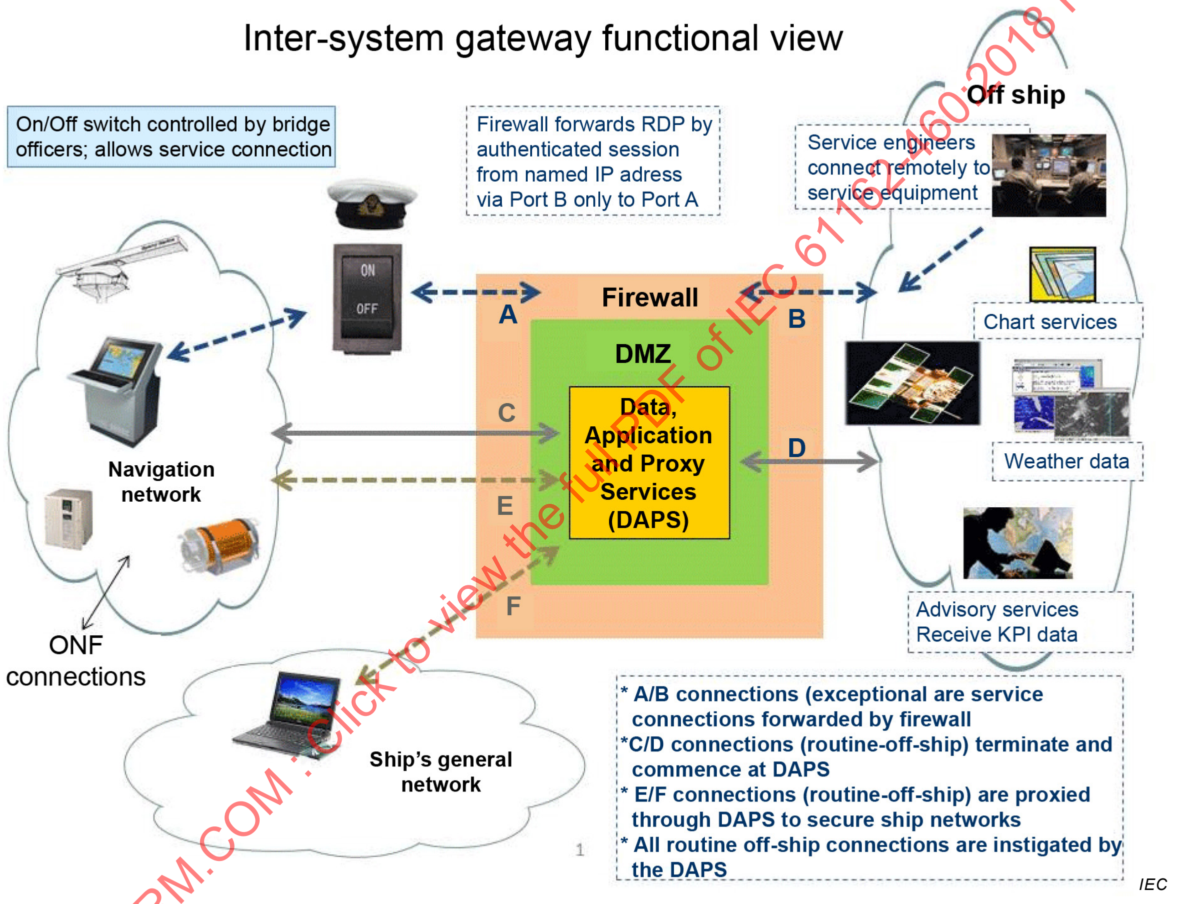
Switch off the first network monitoring function or if EUT has interface redundancy, disconnect one cable. Confirm by observation that the second network monitoring function is available.

Annex A
(informative)

Communication scenarios between an IEC 61162-460 network and uncontrolled networks

A.1 General

Annex A gives some example scenarios for the usage of a 460-Gateway as shown in Figure A.1.



Inter-system gateway functional view

On/Off switch controlled by bridge officers; allows service connection

Firewall forwards RDP by authenticated session from named IP adress via Port B only to Port A

Service engineers connect remotely to service equipment

Advisory services Receive KPI data

* A/B connections (exceptional are service connections forwarded by firewall
*C/D connections (routine-off-ship) terminate and commence at DAPS
* E/F connections (routine-off-ship) are proxied through DAPS to secure ship networks
* All routine off-ship connections are instigated by the DAPS

Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks

A.2 Routine off-ship

- Data exchange from ship to shore, for example KPI data
  - energy usage reports
  - environnemental data (SOx, NOx, etc.)
  - CBM (conditioned base maintenance data)
  - diagnostic data (logs, etc.)
  - operations reports (noon reports, electronic log data)
- Data exchange shore to ship
  - chart services (licences, updates)

- weather
- ocean currents

A.3 Routine on-ship

Some navigational data is required in non-operational, secure ships networks, such as

- the ECDIS/bridge information channel on the captain's PC, and
- the GPS data.

A.4 460-Gateway usage for direct connection with equipment

Direct connection to an IEC 61162-460 network is provided through service connection through connections A-B. The following are examples for this scenario.

- An issue arises on the bridge. It is a safety issue concerning the display on the ECDIS and requires a patch.
- While the ship is in port a remote connection is planned at 18 h 00.
- The ECDIS service engineer coordinates the connection with the ship's IT department and crew.
- The IT department opens the Remote Desktop Protocol port on the perimeter firewall for a registered IP address or an authenticated user and forwards to it to the 460-Gateway Firewall.
- The crew coordinates the on/off switch timing with the service engineer. They turn on the connection.
- The service engineer connects and repairs the system.
- The crew disconnects the bridge for remote service.
- The IT department closes the RDP port on the perimeter firewall.

Annex B
(informative)

Summary of redundancy protocols in IEC 62439 (all parts)

Table B.1 summarises the redundancy protocols and recovery times specified in IEC 62439 (all parts).

Table B.1 – Redundancy protocols and recovery times

Protocol	Solution	Frame loss	Redundancy protocol	End node attachment	Network topology	Recovery time for the considered failures
IP	IP routing	Yes	Within the network	Single	Single meshed	> 30 s typical not deterministic
STP	IEEE 802.1D	Yes	Within the network	Single	Single meshed	> 20 s typical not deterministic
RSTP	IEEE 802.1D	Yes	Within the network	Single	Single meshed, ring	≤100 ms
MSTP	IEEE 802.1Q	Yes	Within the network	Single	Single meshed, ring	See STP and RSTP, compatible with both
CRP	IEC 62439-4	Yes	In the end nodes	Single and double	Doubly meshed, cross-connected	1 s worst case for 512 end nodes
DRP	IEC 62439-6	Yes	Within the network	Single and double	Ring, double ring	100 ms worst case for 50 switches
MRP	IEC 62439-2	Yes	Within the network	Single	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set
BRP	IEC 62439-5	Yes	In the end nodes	Double	Doubly meshed, connected	4,8 ms worst case for 500 end nodes
PRP	IEC 62439-3	No	In the end nodes	Double	Doubly meshed, independent	0 s
HSR	IEC 62439-3	No	In the end nodes	Double	Ring, meshed	0 s

For the redundancy protocols specified in IEC 62439 (all parts), the recovery times in this table are guaranteed when using the settings and parameters specified in the associated part of the IEC 62439 series. Faster recovery times may be achieved using different settings and parameters under the user's responsibility.

Annex C
(informative)

Guidance for testing

C.1 Methods of test

For the purposes of this document, Annex C gives guidance on methods of test based on ISO 9241-12. It is intended to provide guidance to accredited testing laboratories for the development of test plans and test procedures that evaluate a minimum degree of compliance with the requirements specified. They do not identify specific processes, approaches or facilities.

C.2 Observation

Observation refers to simple examination of the presentation of information to confirm that a particular observable condition has been met. Observations may be made by any person with the necessary skill to understand the presentation of information to determine if a statement concerning an observable property has been correctly applied. It is used when suitably trained individuals with a broad range of education and/or experience can be confidently expected to reach the same conclusion about a property of presented information or the performance of display equipment.

The phrase "confirm by observation" is used in the method of test. Conformance is determined by comparing the observed property to the requirement. Some observations may be made directly from the presentation. Other observations may require simulation of input from sensors or other sources. Typical confirmations by observation include

- the existence of functions or features,
- the use of symbols or a defined range of words, and
- a system output in response to a defined input.

C.3 Inspection of documented evidence

Inspection of documented evidence refers to examination of relevant documents to confirm that a particular presentation or display requirement has been met. Documented evidence may include manuals, system requirements, design justification, industry conventions, etc. Inspections may be made by a suitably qualified person who has the necessary education, skill and/or experience to apply the documentation to the system's presentation or display equipment. Inspection of documented evidence is used when performance of a system's presentation or display equipment is not directly observable or measurable. It may also be used when observation would be excessively repetitious, time consuming, or expensive.

The phrase "confirm by inspection of documented evidence" is used in the method of test. Conformance is determined by comparing the documented property to the requirement. Typical confirmations by inspection of documented evidence include

- the conformance to a standard or other documented evidence,
- the existence of optional features or functions, and
- the design and/or operation of algorithms.

C.4 Measurement

In this document, measurement refers to measuring or calculating a value or variable for comparison to a specified value to determine that a particular requirement has been met.

Measurements may require the use of test facilities and equipment. Measurements may be made by any person with the necessary skill to measure and/or calculate the value and compare it against a requirement, standard or other documented evidence. Compliance is determined by comparing the measured or calculated value or variable to the requirement.

C.5 Analytical evaluation

The test method "analytical evaluation" refers to detailed examination of the presentation of information to confirm that a particular condition has been met.

The phrase "confirm by analytical evaluation" is used in the method of test. Analytical evaluations may be made by a relevant expert with the necessary education, skills and/or experience to make an informed and reliable judgement concerning the presentation of information, its appropriateness and usability. It is used for the evaluation of properties that can be judged only in context of other information or knowledge that requires the tester's presentation. Compliance is determined by comparing the observed property to the requirement.

Annex D
(informative)

Some examples to use this document

Figure D.1 to Figure D.6 gives some examples of how this document could be used.

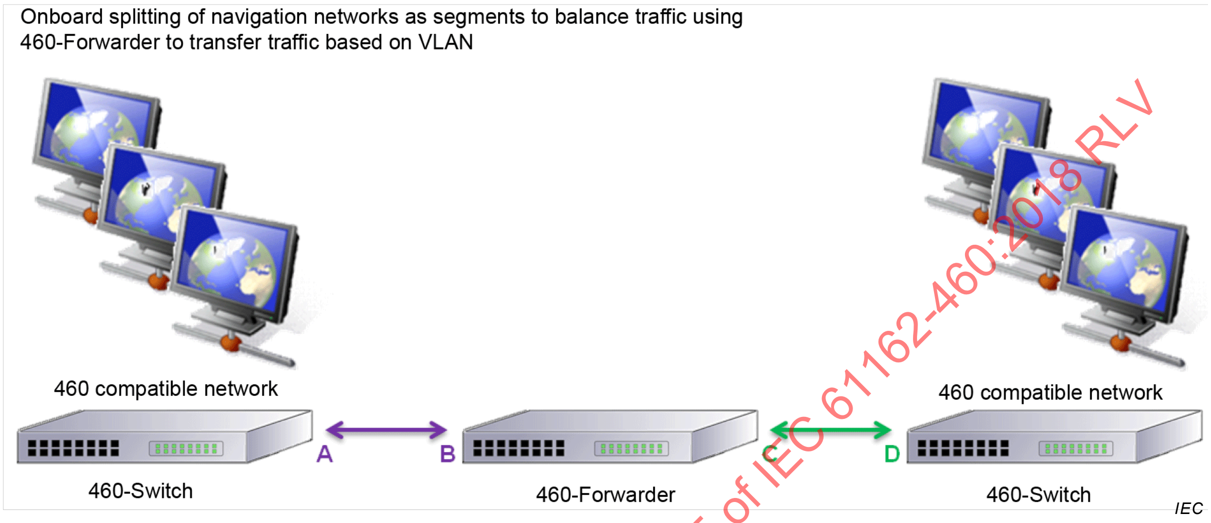

Onboard splitting of navigation networks as segments to balance traffic using
460-Forwarder to transfer traffic based on VLAN
460 compatible network
460 compatible network
A
B
C
D
460-Switch
460-Forwarder
460-Switch
IEC

Figure D.1 – 460-Forwarder used between two networks

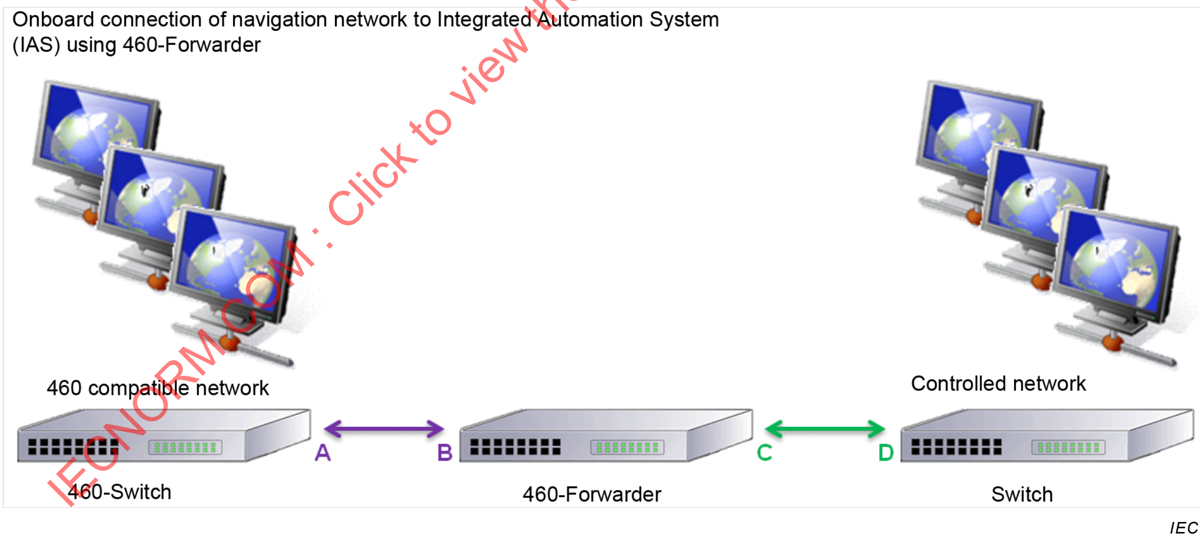
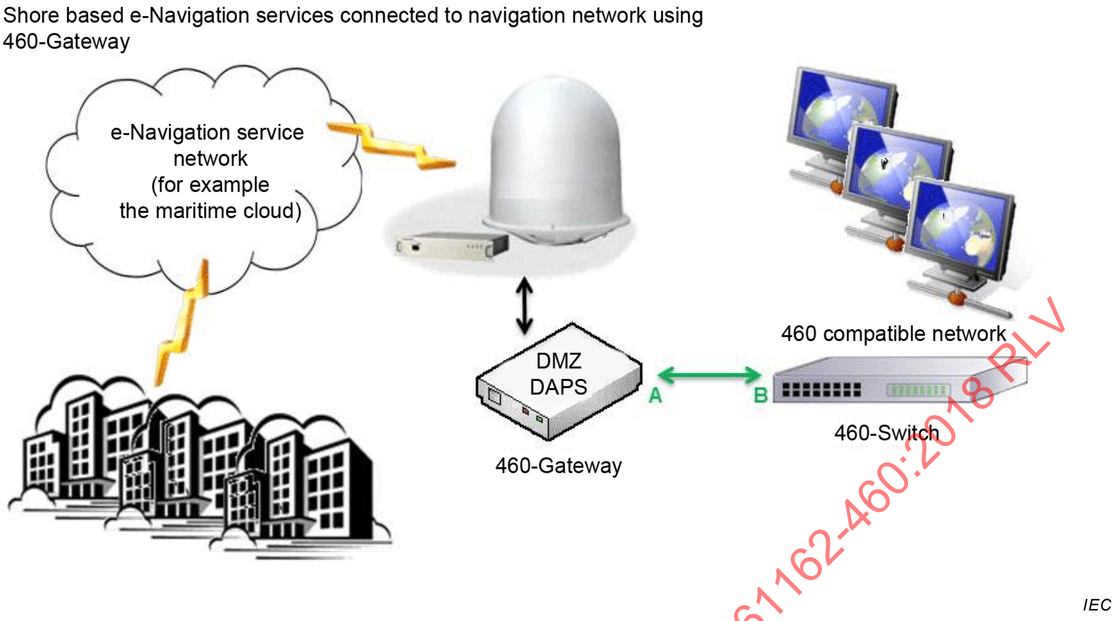

Onboard connection of navigation network to Integrated Automation System
(IAS) using 460-Forwarder
460 compatible network
Controlled network
A
B
C
D
460-Switch
460-Forwarder
Switch
IEC

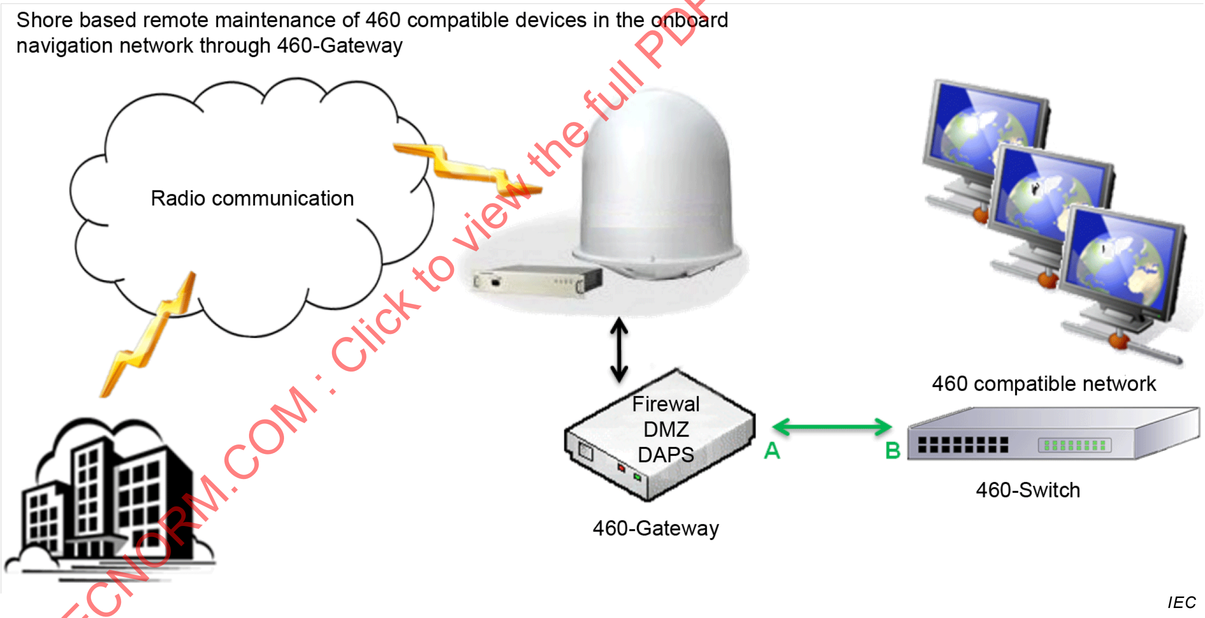
Figure D.2 – 460-Forwarder used between two networks



Shore based e-Navigation services connected to navigation network using 460-Gateway

e-Navigation service network (for example the maritime cloud)
DMZ
DAPS
A
B
460 compatible network
460-Switch
460-Gateway
IEC

Figure D.3 – 460-Gateway used for e-Navigation services



Shore based remote maintenance of 460 compatible devices in the onboard navigation network through 460-Gateway

Figure D.4 – 460-Gateway used for remote maintenance

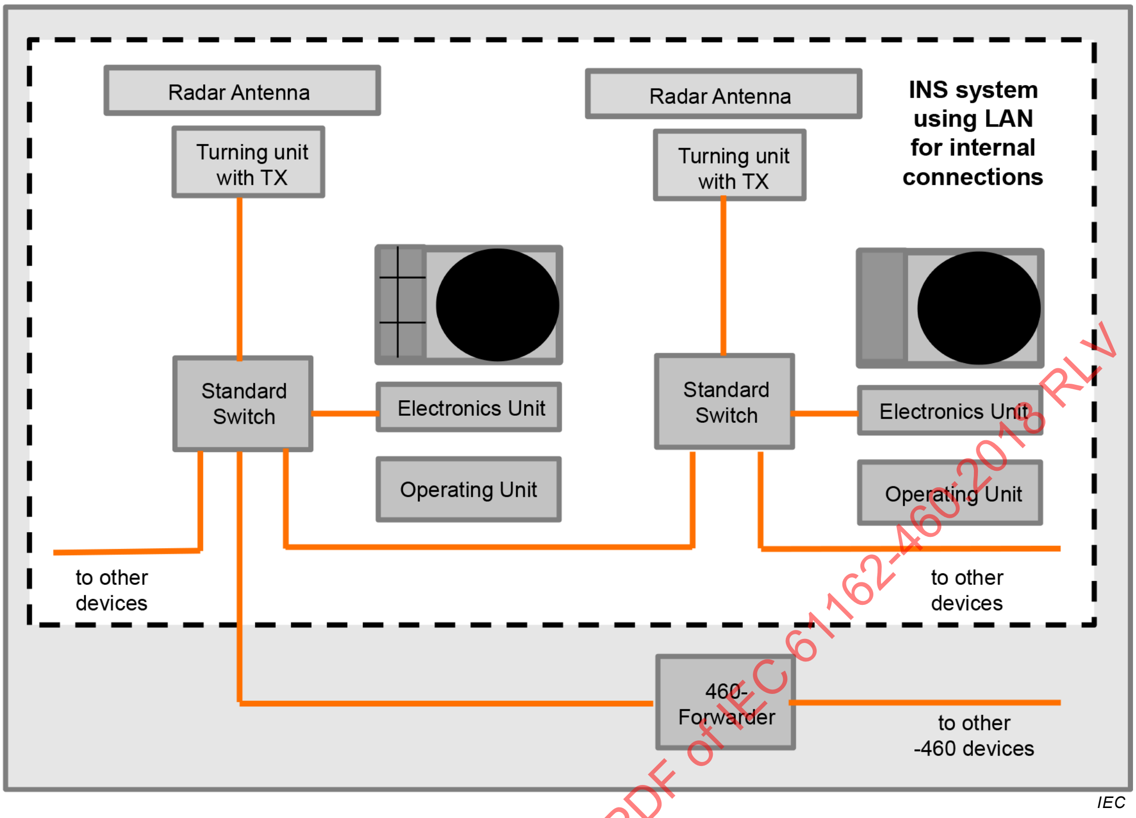


Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices

Figure D.5 shows an example of an INS system fulfilling requirements of IEC 61924-2. This INS system uses internally Local Area Network technology to connect various components of the INS system. Figure D.5 shows how a 460-Forwarder is used to separate this INS system into its own controlled network.

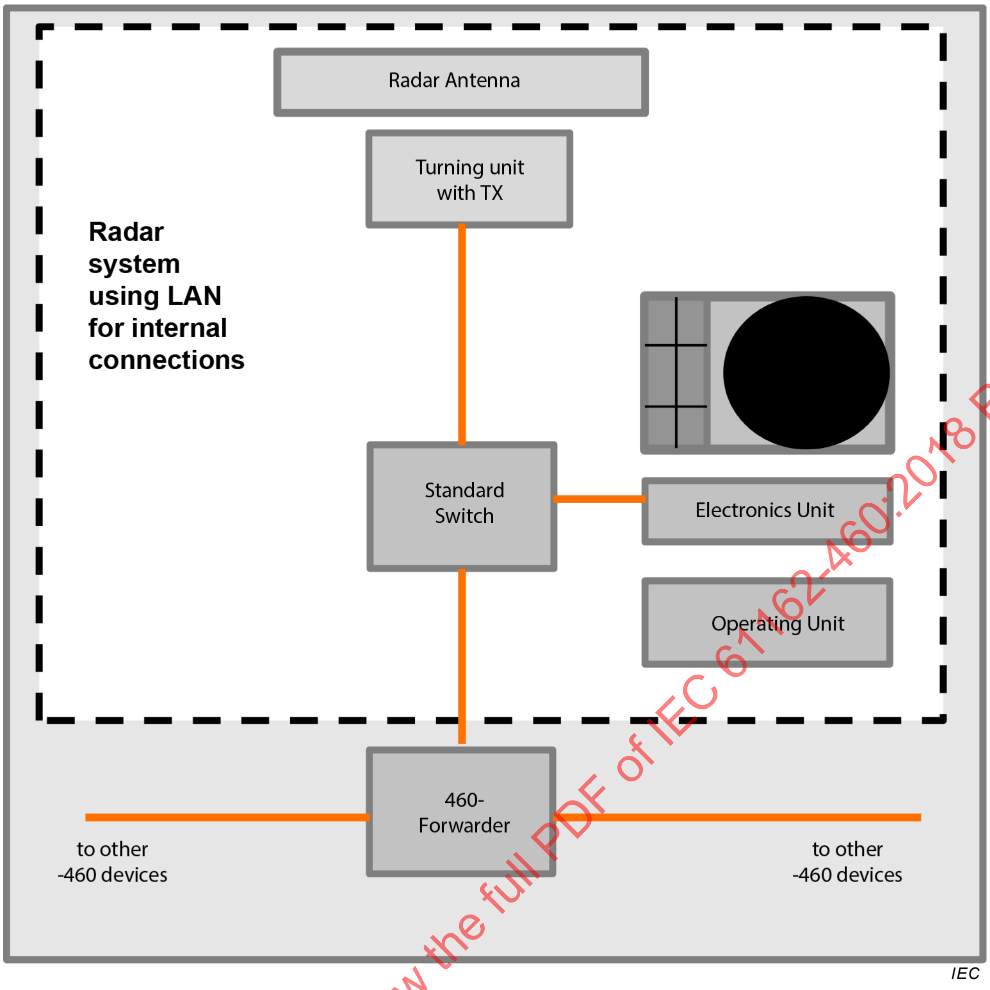


Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices

Figure D.6 shows an example of a radar system fulfilling requirements of IEC 62388. This radar system uses internally Local Area Network technology to connect various components of the radar system. Figure D.6 shows how a 460-Forwarder is used to separate this radar system into its own controlled network.

Annex E
(normative)

IEC 61162 interfaces for the network monitoring function

The network monitoring function shall be capable of at least transmitting and receiving data with the optional logical interfaces in Figure E.1 using the sentences specified in Table E.1 and Table E.2.

Figure E.1 shows the logical interfaces. If more than one logical interface is implemented on a single physical interface then all aspects of each logical interface, including alert communication, heartbeat, etc. shall be distinguishable from those of other logical interfaces implemented on the same physical interface.

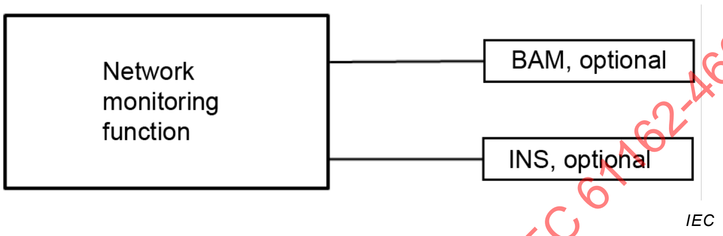


Figure E.1 – Network monitoring function logical interfaces

Table E.1 and Table E.2 specify sentences which can be used with interface alternatives IEC 61162-1, IEC 61162-2 and IEC 61162-450. The manufacturer shall specify which interface is supported.

Table E.1 – Sentences received by the network monitoring function

Mnemonic	Interface (see Figure E.1)	Name	Comment
ACN	BAM, INS	Alert command	Alert command, e.g. acknowledge
HBT	BAM, INS	Heartbeat	Support reliable alert related communication Repeated once per 1 min

Table E.2 – Sentences transmitted by the network monitoring function

Mnemonic	Interface (see Figure E.1)	Name	Comment
ALC	BAM, INS	Cyclic alert list	List of current alert
ALF	BAM, INS	Alert sentence	Details of a new alert
ARC	BAM, INS	Alert command refused	Alert command not accepted
HBT	BAM, INS	Heartbeat	Support reliable alert related communication

Annex F
(informative)

Distribution of functions around 460-Network

Annex F provides guidance about the distribution of various functions around components of the 460-Network.

Table F.1 – Distribution of functions around 460-Network

Function	460-Node	460-Switch	460-Forwarder	460-Gateway
No REDS or external networks(6.2.3, 6.2.4.2)	✓	✓	✓	✓
Syslog implemented (source) (8.1)	✓	✓	✓	✓
Data output bandwidth defined (5.1, 6.2.2.1)	✓	✓	✓	✓
ONF specified (4.4.1, 4.4.2, 5.1)	✓			
Network traffic management (5.1)	✓	✓	✓	
Security – no wireless (6.2.1)	✓		✓	
Security – excessive traffic protection (6.2.2.1, 5.3.3)	✓		✓	
Security – DoS Attack ICMP IGMP protection (6.2.2.2)	✓		✓	
Security – access control (password) (6.2.4.1)	✓	✓	✓	✓
Redundancy (7.1, 7.2)	✓	As installed ✓	As installed ✓	✓
Network monitoring	✓(for at least one node or switch, 8.2.1)	✓(for at least one node or switch, 8.2.1)		✓ (list of connections)
If applicable – application level check of external network packets (4.4.2)	✓			
If applicable – REDS security (6.2.3)	✓			
If applicable – direct connection only with admin permission (6.3.3, 6.3.4, 6.3.5)	✓			
Configuration of network flows (5.2.1, 5.3.2)		✓	✓	
Allocation of bandwidth (5.2.1, 5.3.2)		✓	✓	
In/out traffic in register allowed, deny other traffic (6.2.4.2)		✓		
If applicable – VLAN config per interface (5.2.1)		✓		
IGMP multicast snooping (5.2.1)		✓		
Syslog (sink)	✓(for at least one node or switch, 8.2.1)	✓(for at least one node or switch, 8.2.1)		
Caution/warning source (6.3.4, 6.3.5, 8.2.7.1)	✓	✓		✓
Caution/warning sink	External CAM of BAM			
Firewall (6.3.2)				✓

Table F.2 – Equipment standards referencing IEC 61162-460

Standard	460-Node	460-Switch	460-Forwarder	460-Gateway
IEC 62940:2016, ICS, 5.1.1				✓

Bibliography

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61162 (all parts), *Maritime navigation and radiocommunication equipment and systems – Digital interfaces*

IEC 61162-1, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 1: Single talker and multiple listeners*

IEC 61162-2, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 2: Single talker and multiple listeners, high-speed transmission*

IEC 62388, *Maritime navigation and radiocommunication equipment and systems – Shipborne radar – Performance requirements, methods of testing and required test results*

IEC 62439 (all parts), *Industrial communication networks – High availability automation networks*

IEC 62439-1, *Industrial communication networks – High availability automation networks – Part 1: General concepts and calculation methods*

IEC 62439-2, *Industrial communication networks – High availability automation networks – Part 2: Media Redundancy Protocol (MRP)*

IEC 62439-3, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*

IEC 62439-4, *Industrial communication networks – High availability automation networks – Part 4: Cross-network Redundancy Protocol (CRP)*

IEC 62439-5, *Industrial communication networks – High availability automation networks – Part 5: Beacon Redundancy Protocol (BRP)*

IEC 62439-6, *Industrial communication networks – High availability automation networks – Part 6: Distributed Redundancy Protocol (DRP)*

IEC 62940, *Maritime navigation and radiocommunication equipment and systems – Integrated communication system (ICS) – Operational and performance requirements, methods of testing and required test results*

ISO/IEC 10118-3, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO 9241-12, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 12 – Presentation of information*

ISO 16425, *Ships and marine technology – Guidelines for the installation of ship communication networks for shipboard equipment and systems*

IMO Resolution MSC.302(87), *Performance standards for bridge alert management (BAM)*

CIGRE B5-109, *Redundancy challenges on IEC 61850 systems and Migration Paths for IEC 61850 Substation Communication Networks*

IEEE 802.3, *IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

IEEE 802.10, *IEEE Standard for Interoperable LAN/MAN Security (SILS)*

IEEE 802.11, *Wireless Local Area Networks*

IEEE 802.15.4, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*

IEEE 1363, *IEEE Standard Specifications for Public-Key Cryptography*

ISOC RFC 768, *User Datagram Protocol (UDP), Standard STD0006*

ISOC RFC 791, *Internet Protocol (IP), Standard STD0005 (and updates)*

ISOC RFC 793, *Transmission control protocol (TCP)*

ISOC RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets*

ISOC RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

ISOC RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

ISOC RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

Universal Serial Bus Revision 2.0 specification. Available at www.usb.org

Universal Serial Bus Revision 3.1 specification. Available at www.usb.org

____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

____

MATÉRIELS ET SYSTÈMES DE NAVIGATION ET DE RADIOCOMMUNICATION MARITIMES – INTERFACES NUMÉRIQUES –

Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.

6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.

7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.

8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61162-460 a été établie par le comité d'études 80 de l'IEC: Matériels et systèmes de navigation et de radiocommunication maritimes.

Cette deuxième édition de l'IEC 61162-460 annule et remplace la première édition parue en 2015. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) les commutateurs-460 et les redirecteurs-460 sont exigés pour la mise en œuvre de la surveillance du trafic des protocoles Internet de gestion de groupe (IGMP – *Internet group management protocol*);

b) le raccordement entre des zones protégées et des zones non protégées exige un redirecteur-460 en tant qu'élément isolant;

c) ajout de la détection de collision par ID de fonction du système (SFI – *system function ID*) comme fonction de surveillance du réseau;

d) la consignation de la passerelle-460 et de la passerelle sans fil-460 à la surveillance du réseau n'est plus exigée;

e) toutes les alertes issues de la surveillance du réseau ont des identificateurs d'alerte normalisés.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
80/879/FDIS	80/884/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Cette Norme internationale doit être utilisée conjointement avec l'IEC 61162-450:2018.

Une liste de toutes les parties de la série IEC 61162, publiées sous le titre général *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

MATÉRIELS ET SYSTÈMES DE NAVIGATION ET DE RADIOCOMMUNICATION MARITIMES – INTERFACES NUMÉRIQUES –

Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité

1 Domaine d'application

La présente partie de l'IEC 61162 vient s'ajouter à la norme IEC 61162-450 lorsque des normes plus rigoureuses en matière de sûreté et de sécurité sont nécessaires, par exemple en raison d'une exposition plus importante aux menaces externes ou afin de renforcer l'intégrité du réseau. Le présent document spécifie des exigences et des méthodes d'essai pour les matériels à utiliser dans un réseau conforme à l'IEC 61162-460 ainsi que des exigences relatives au réseau proprement dit et des exigences relatives à l'interconnexion du réseau avec d'autres réseaux. Le présent document comprend également des exigences s'appliquant aux réseaux redondants conformes à l'IEC 61162-460.

Le présent document n'introduit pas de nouvelles exigences relatives aux protocoles des niveaux d'application par rapport à celles définies dans l'IEC 61162-450.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60945, *Matériels et systèmes de navigation et de radiocommunication maritimes – Spécifications générales – Méthodes d'essai et résultats exigibles*

IEC 61162-450:2018, *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques – Partie 450: Emetteurs multiples et récepteurs multiples – Interconnexion Ethernet*

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* (disponible en anglais seulement)

IEC 62288:2014, *Matériels et systèmes de navigation et de radiocommunication maritimes – Présentation des informations relatives à la navigation sur des affichages de navigation de bord – Exigences générales, méthodes d'essai et résultats d'essai exigés*

IEEE 802.1D-2004, *IEEE Standards for Local Area Networks: Media Access Control (MAC) Bridges*

IEEE 802.1Q, *Virtual Bridged Local Area Networks*

INTERNET SOCIETY (ISOC). RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)* [en ligne]. Édité par J. Postel. Septembre 1981 [consulté 2018-01-08]. Adresse
https://tools.ietf.org/html/rfc792

INTERNET SOCIETY (ISOC). RFC 1112, *Host Extensions for IP Multicasting* [en ligne]. Édité par S. Deering. Août 1989 [consulté 2018-01-08]. Adresse https://www.ietf.org/rfc/rfc1112.txt

INTERNET SOCIETY (ISOC). RFC 1157, *A Simple Network Management Protocol (SNMP)* [en ligne]. Édité par J. Case et al. Mai 1990 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc1157

INTERNET SOCIETY (ISOC). RFC 2021, *Remote Network Monitoring Management Information Base* [en ligne]. Édité par S. Waldbusser. Janvier 1997 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc2021

INTERNET SOCIETY (ISOC). RFC 2236, *Internet Group Management Protocol, Version 2* [en ligne]. Édité par W. Fenner. Novembre 1997 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc2236

INTERNET SOCIETY (ISOC). RFC 2819, *Remote Network Monitoring Management Information Base* [en ligne]. Édité par S. Waldbusser. Mai 2000 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc2819

INTERNET SOCIETY (ISOC). RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* [en ligne]. Édité par D. Harrington. Décembre 2002 [consulté 2018-01-08]. Adresse https://www.ietf.org/rfc/rfc3411.txt

INTERNET SOCIETY (ISOC). RFC 3577, *Introduction to the RMON family of MIB modules* [en ligne]. Édité par S. Waldbusser. Août 2003 [consulté 2018-01-08]. Adresse 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* [en ligne]. Édité par H. Holbrook et al. Août 2006 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc4604

INTERNET SOCIETY (ISOC). RFC 5424, *The Syslog Protocol* [en ligne]. Édité par R. Gerhards. Mars 2009 [consulté 2018-01-08]. Adresse https://tools.ietf.org/html/rfc5424

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 61162-450, ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
nœud-450
dispositif conforme à l'IEC 61162-450 et qui satisfait aux exigences complémentaires spécifiées dans le présent document

Note 1 à l'article: Comprend également les nœuds qui mettent en œuvre le bloc fonctionnel ONF.

3.2
redirecteur-460
dispositif d'infrastructure de réseau qui peut échanger des flux de données de manière sûre entre un réseau-460 et d'autres réseaux contrôlés, y compris les autres réseaux-460

3.3
passerelle-460
dispositif d'infrastructure de réseau qui raccorde des réseaux-460 et des réseaux non contrôlés et qui satisfait aux exigences en matière de sûreté et de sécurité spécifiées dans le présent document

3.4
réseau-460
réseau qui comporte uniquement des nœuds-460, des commutateurs-460, un redirecteur-460, une passerelle-460 et une passerelle sans fil-460 ainsi que des nœuds-450

3.5
nœud-460
dispositif conforme aux exigences applicables à un nœud-450 et qui satisfait aux exigences en matière de sûreté et de sécurité spécifiées dans le présent document

3.6
commutateur-460
dispositif d'infrastructure de réseau utilisé pour assurer l'interconnexion des nœuds dans un réseau-460 et qui satisfait aux exigences en matière de sûreté et de sécurité spécifiées dans le présent document

3.7
passerelle sans fil-460
dispositif d'infrastructure de réseau qui raccorde un réseau-460 à des réseaux sans fil et qui satisfait aux exigences en matière de sûreté et de sécurité spécifiées dans le présent document

3.8
norme de cryptage évolué
AES
algorithme à clés symétriques de cryptage par blocs qui s'appuie sur un réseau de substitution-permutation (SPN – *substitution-permutation network*) et qui n'utilise pas le réseau de Feistel de la norme de chiffrement de données (DES – *data encryption standard*)

Note 1 à l'article: L'abréviation "AES" est dérivée du terme anglais développé correspondant "advanced encryption standard".

3.9
alarme
priorité la plus élevée d'une alerte, annonçant une situation ou une condition exigeant une attention, une prise de décision et, si nécessaire, une action immédiates de la part de l'équipe à la passerelle, en vue de maintenir une navigation sûre du navire

3.10
passerelle de niveau application
dispositif d'infrastructure de réseau qui raccorde des réseaux-460 à d'autres réseaux et qui satisfait aux exigences en matière de sûreté et de sécurité spécifiées dans le présent document

3.11
porte dérobée
programme installé permettant un accès à distance à un ordinateur au moyen d'une méthode de contournement de l'authentification normale

3.12
réseau contrôlé
tout réseau qui a été conçu pour fonctionner de sorte que les autorités disposent de preuves documentées selon lesquelles ledit réseau ne présente aucun risque pour la sécurité des nœuds des réseaux connectés

Note 1 à l'article: Par exemple, tout réseau conforme à l'IEC 61162-450 approuvé par la société de classification, l'État du pavillon ou tout organisme reconnu (RO – *recognized organization*).

3.13
alerte de catégorie B
alerte signalant lorsqu'aucune information complémentaire pour l'aide à la décision n'est nécessaire outre les informations pouvant être présentées au niveau de l'interface centrale homme-machine (IHM) de gestion des alertes

3.14
mise en garde
priorité la plus faible d'une alerte

Note 1 à l'article: "Mise en garde" augmente la sensibilisation d'une équipe à la passerelle concernant une condition qui ne justifie pas une alarme ou une condition d'avertissement, mais qui exige tout de même une attention hors de la prise en considération ordinaire de la situation ou des informations fournies.

3.15
zone démilitarisée
DMZ
sous-réseau physique ou logique qui comprend et qui expose les services externes d'un organisme à un réseau non fiable de plus grande ampleur, généralement Internet

Note 1 à l'article: L'abréviation "DMZ" est dérivée du terme anglais développé correspondant "demilitarized zone".

3.16
déni de service
DoS
tentative visant à empêcher les utilisateurs légitimes d'accéder à une machine ou à une ressource réseau

Note 1 à l'article: L'abréviation "DoS" est dérivée du terme anglais développé correspondant "denial of service".

3.17
flux
combinaison des informations suivantes: adresse MAC source et de destination, adresse IP source et de destination, protocole, numéro de port UDP/TCP source et de destination

3.18
analyse des modes de défaillance et de leurs effets
AMDE
méthode spécifiée dans l'IEC 60812 d'analyse d'un système pour identifier les modes de défaillance potentiels, leurs causes et les effets sur l'aptitude à la fonction du système

3.19
analyse des modes de défaillance, de leurs effets et de leur criticité
AMDEC
méthode d'analyse spécifiée dans l'IEC 60812 comprenant un moyen de classer les modes de défaillance par sévérité

Note 1 à l'article: L'AMDEC est une extension de l'AMDE du fait qu'elle comprend une analyse de criticité utilisée afin de suivre la probabilité des modes de défaillance par rapport à la sévérité de leurs conséquences.

3.20
protocole de message de commande Internet
ICMP
protocole conforme à l'ISOC RFC 792

Note 1 à l'article: L'abréviation "ICMP" est dérivée du terme anglais développé correspondant "internet control message protocol".

3.21
protocole Internet de gestion de groupe
IGMP
protocole conforme à l'ISOC RFC 1112 (version 1), l'ISOC RFC 2236 (version 2) et l'ISOC RFC 4604 (version 3)

Note 1 à l'article: L'abréviation "IGMP" est dérivée du terme anglais développé correspondant "internet group management protocol".

3.22
taux de perte
quantité de données perdues par le dispositif de réception d'un flux sous la forme de paquets perdus sur la quantité totale de paquets, mesurée au port d'entrée d'un dispositif

Note 1 à l'article: Le taux de perte est exprimé en pourcentage.

3.23
logiciel malveillant
code malveillant
logiciel utilisé ou créé pour interrompre le fonctionnement d'un ordinateur

3.24
charge maximale de réseau
maximum cumulatif de tous les trafics provenant de tous les nœuds de réseau et les composants d'infrastructure de réseau d'un seul réseau-460

Note 1 à l'article: La charge maximale de réseau est mesurée en octets par seconde (o/s).

3.25
vitesse maximale de transmission
nombre maximal d'octets par seconde pouvant être émis par un nœud de réseau ou un matériel d'infrastructure de réseau

3.26
protocole d'arbre maximal multiple
MSTP
protocole, conforme à l'IEEE 802.1Q, qui est une extension de RSTP pour les VLAN

Note 1 à l'article: L'abréviation "MSTP" est dérivée du terme anglais développé correspondant "multiple spanning tree protocol".

3.27
adresse MAC voisine
adresse MAC (*media access control* – commande d'accès au support) d'un nœud-450 ou d'un nœud-460 connecté tel que perçu par un commutateur-460 et tel que signalé par SNMP (*simple network management protocol* – protocole simple de gestion de réseau)

3.28
composant d'infrastructure du réseau
dispositif qui connecte au moins deux nœuds dans un réseau-460 avec deux réseaux différents, tel qu'un commutateur-460, un redirecteur-460, une passerelle-460 et une passerelle sans fil-460

3.29
capacité nominale du réseau
capacité du réseau, en débit d'octets, d'après la configuration

Note 1 à l'article: La capacité est la capacité la plus faible de tout commutateur du réseau pour acheminer l'ensemble du trafic.

Note 2 à l'article: Elle est utilisée pour spécifier les capacités des matériels.

3.30
autre fonction du réseau
ONF
bloc fonctionnel qui assure l'interface avec le réseau, tel que spécifié dans l'IEC 61162-450

Note 1 à l'article: L'ONF représente une fonction autorisée à partager l'infrastructure d'un réseau conforme à l'IEC 61162-450 mais n'utilise pas les protocoles définis dans l'IEC 61162-450.

Note 2 à l'article: L'abréviation "ONF" est dérivée du terme anglais développé correspondant "other network function".

3.31
protocole d'arbre maximal rapide
RSTP
protocole conforme à l'IEEE 802.1D pour le calcul et la configuration de la topologie active d'un réseau

Note 1 à l'article: L'abréviation "RSTP" est dérivée du terme anglais développé correspondant "rapid spanning tree protocol".

3.32
source de données externe amovible
REDS
source de données qui n'appartient pas au réseau et qui est amovible par l'utilisateur, comprenant, entre autres, les disques compacts, les clés USB et les dispositifs Bluetooth[1]

Note 1 à l'article: L'abréviation "REDS" est dérivée du terme anglais développé correspondant "removable external data source".

3.33
surveillance à distance du réseau
RMON
spécification normalisée relative à la surveillance décrite dans l'ISOC RFC 3577

Note 1 à l'article: L'abréviation "RMON" est dérivée du terme anglais développé correspondant "remote network monitoring".

3.34
topologie en anneau
topologie dont chaque nœud est relié en série à deux autres nœuds

3.35
RSA
système cryptographique à clé publique décrit dans l'IEEE 1363

[1] Bluetooth est l'appellation commerciale d'un produit distribué par Bluetooth Special Interest Group. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il peut être démontré qu'ils conduisent aux mêmes résultats.

3.36
sûreté
protection des réseaux contre les menaces non intentionnelles telles que les dysfonctionnements du système, les erreurs de configuration et les erreurs de fonctionnement

3.37
zone protégée
zone équipée de périmètres et de barrières physiques définis, comportant des commandes physiques d'entrée ou une protection du point d'accès ou une observation du point d'accès

Note 1 à l'article: Une passerelle de navigation d'un navire à consoles fermées et à observation d'accès par le capitaine ou l'officier de quart est un exemple de zone protégée.

3.38
sécurité
protection des réseaux contre les menaces intentionnelles telles que les virus, les vers, les dénis de service, les accès illicites, etc.

3.39
protocole simple de gestion de réseau
SNMP
protocole conforme à l'ISOC RFC 3411 servant à transmettre des informations liées à la gestion

Note 1 à l'article: L'abréviation "SNMP" est dérivée du terme anglais développé correspondant "simple network management protocol".

3.40
interruption SNMP
méthode permettant de collecter des événements et des informations statistiques à partir des commutateurs, conformément à l'ISOC RFC 1157, l'ISOC RFC 2021 et l'ISOC RFC 2819

3.41
réseau embarqué
infrastructure de réseau de données à bord d'un navire visant à échanger des données entre les matériels à bord

Note 1 à l'article: Le réseau embarqué peut ou peut ne pas être raccordé au quai par des satellites ou par d'autres moyens

3.42
reniflage
surveillance et analyse du trafic du réseau

3.43
suite
combinaison de tous les flux provenant d'un dispositif qui utilisent le même protocole

3.44
syslog
protocole conforme à l'ISOC RFC 5424 qui est utilisé pour la consignation externe décrit dans l'IEC 61162-450

3.45
intégrateur de système
personne ou organisme responsable de la fonctionnalité du réseau-460 intégré

3.46
menace
cause potentielle d'incident concernant la sécurité informatique pouvant provoquer des dommages au système

3.47
trafic
combinaison de toutes les suites provenant d'un dispositif

3.48
réseau non contrôlé
réseau de données qui n'est ni conforme à l'IEC 61162-450, ni conforme à l'IEC 61162-460, ou qui n'est pas un réseau contrôlé

EXEMPLE Réseaux sans fil.

3.49
réseau local virtuel
VLAN
réseau conforme à l'IEEE 802.1Q composé de réseaux interconnectés avec des ponts

Note 1 à l'article: L'abréviation "VLAN" est dérivée du terme anglais développé correspondant "virtual local area network".

3.50
réseau privé virtuel
RPV
extension de réseau privé au moyen de liaisons encapsulées, chiffrées et authentifiées qui traversent les réseaux partagés ou publics

3.51
avertissement
annonce d'une une situation ou d'une condition exigeant une attention particulière mais pas une attention ou une action immédiate de la part de l'équipe à la passerelle

Note 1 à l'article: Les avertissements sont présentés pour des raisons de précaution afin d'attirer l'attention de l'équipe à la passerelle sur des modifications des conditions qui ne représentent pas des dangers immédiats, mais qui peuvent le devenir si aucune décision ou mesure prospective n'est entreprise.

3.52
point d'accès sans fil
AP sans fil
dispositif qui raccorde des dispositifs sans fil à des dispositifs câblés par le biais de diverses technologies sans fil, telles que le Wi-Fi et le Bluetooth

Note 1 à l'article: L'abréviation "AP" est dérivée du terme anglais développé correspondant "access point".

4 Exigences de haut niveau

4.1 Vue d'ensemble

Le présent document s'appuie sur l'IEC 61162-450, qui est indispensable pour le présent document. Le présent document spécifie des exigences plus rigoureuses concernant les matériels ainsi que la conception du système et son fonctionnement.

La conformité au présent document fournit une protection supplémentaire contre les menaces provenant de connexions externes à un réseau et de connexions à l'intérieur d'un réseau. Lorsqu'un réseau est totalement enfermé physiquement dans une zone protégée, telle que la passerelle d'un navire, au niveau de laquelle l'accès peut être contrôlé, la menace la plus importante proviendra des connexions externes. Les exigences applicables aux zones protégées sont fournies en 4.7.

4.2 Description

La Figure 1 représente un réseau mettant en œuvre les exigences du présent document sur différentes parties et différents composants du réseau. Les symboles gris représentent les matériels spécifiés dans le présent document. Les pentagones représentent les fonctions logiques logicielles spécifiées dans le présent document. Les symboles hachurés représentent les matériels conformes à l'IEC 61162-450 qui sont autorisés au sein d'un réseau-460.

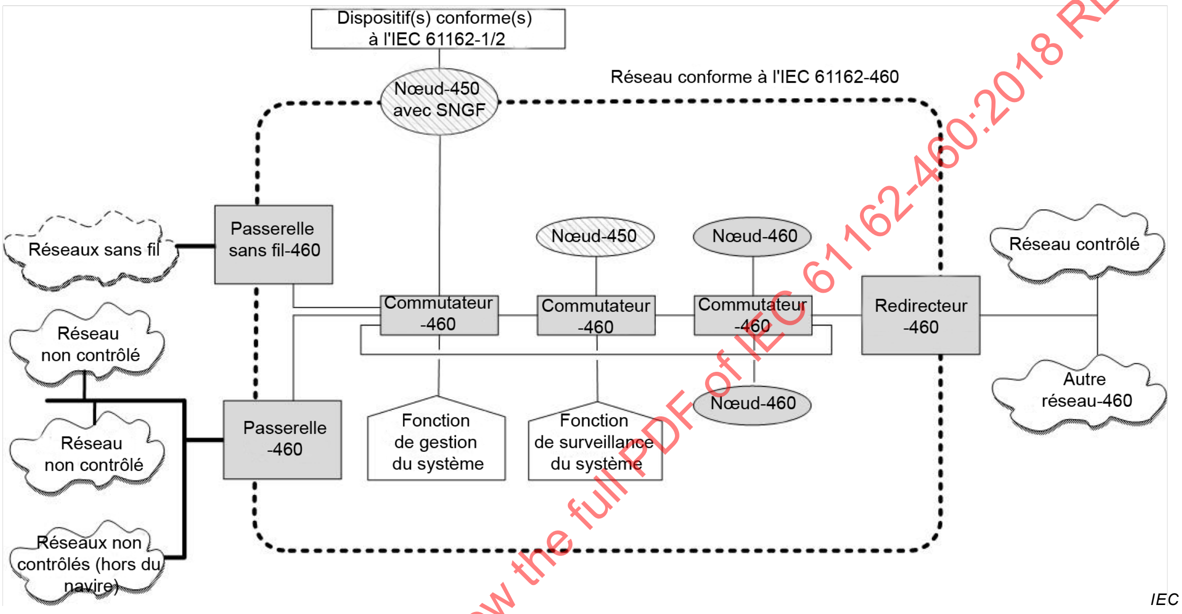


Figure 1 – Vue d'ensemble fonctionnelle des applications des exigences de l'IEC 61162-460

Certains exemples d'utilisation d'une passerelle-460 sont donnés dans l'Annexe A, et certains exemples d'utilisation du présent document sont donnés dans l'Annexe D.

4.3 Exigences générales

4.3.1 Exigences relatives aux matériels et aux systèmes

(Voir 10.3)

Les exigences de 4.3 s'appliquent à tous les matériels et systèmes conçus pour être conformes à toute partie du présent document. Les paragraphes 4.4 à 4.7 résument les exigences relatives à un type de capacité pouvant être mis en œuvre seul, sans exiger la conformité aux autres parties du présent document.

Tous les matériels qui font partie du réseau-460 doivent satisfaire aux exigences générales relatives aux matériels de navigation et de radiocommunication spécifiés dans l'IEC 60945.

NOTE L'IEC 60945 exige que les matériels soient conçus de sorte que la maintenance des logiciels puisse être facilement effectuée à bord du navire, par exemple afin de prendre en charge la mise à jour périodique du micrologiciel des matériels d'infrastructure de réseau afin d'améliorer les algorithmes de chiffrement et les caractéristiques de sécurité.

Tous les nœuds de réseaux, les composants d'infrastructure de réseau et les câbles doivent satisfaire aux exigences des Articles 4 et 5 de l'IEC 61162-450:2018.

Les fabricants de nœuds de réseaux et de composants d'infrastructure de réseau doivent fournir une liste de toutes les adresses MAC à utiliser dans un réseau-460.

Il peut s'agir d'une étiquette, d'une liste ou d'un procédé équivalent.

L'Annexe F comprend une vue d'ensemble de la répartition des différentes fonctionnalités relatives aux matériels physiques.

4.3.2 Exigences relatives à la composition physique

(Voir 10.12.3.1)

Un réseau-460 doit uniquement être composé des nœuds physiques de réseaux suivants ou des composants d'infrastructure de réseau suivants:

- nœud-450, c'est-à-dire, nœuds de réseaux conformes à l'IEC 61162-450 et qui satisfont aux exigences de 4.4.1;
- nœud-460, c'est-à-dire, nœuds de réseaux conformes à l'IEC 61162-450 et qui satisfont aux exigences complémentaires de 4.4.2;
- composants d'infrastructure de réseau conformes aux exigences relatives aux commutateurs-460 ou aux redirecteurs-460 de 4.4.3 et de 4.4.4;
- passerelles de niveau application conformes aux exigences relatives aux passerelles-460 et aux passerelles sans fil-460 de 4.4.5.

4.3.3 Exigences relatives à la composition logique

(Voir 10.12.3.1)

Un réseau-460 doit également comprendre les composants fonctionnels de système logique suivants, lesquels couvrent tous les nœuds d'un réseau-460:

- fonction de surveillance du réseau, qui peut être un SF (bloc fonctionnel du système, voir l'IEC 61162-450) ou un ONF (autre bloc fonctionnel du réseau, voir l'IEC 61162-450) conforme aux exigences de 4.5.1;
- fonction de gestion du réseau, qui peut être un SF ou un ONF conforme aux exigences de 4.5.2.

4.4 Exigences relatives aux composants physiques

4.4.1 Nœud-450

(Voir 10.4)

Les nœuds du réseau qui satisfont aux exigences de l'IEC 61162-450 doivent également satisfaire aux exigences suivantes afin d'être utilisés dans un réseau-460:

- aucune connexion aux réseaux externes ou aux REDS;
- syslog mis en œuvre tel que défini en 4.3.3.2 de l'IEC 61162-450:2018;
- bande passante de sortie de données documentée par le fabricant telle que définie en 6.2.2.1;
- mise en œuvre des services ONF fournis par le fabricant, y compris les paramètres de protocole nécessaires, au minimum l'adresse IP et le numéro de port;
- les ports éphémères, en cas d'utilisation, indiqués par le fabricant.

4.4.2 Nœud-460

Les fonctions suivantes doivent être mises en œuvre dans un nœud-460:

- gestion des trafics du réseau telle que spécifiée en 5.1;

- exigences relatives à la sûreté telles que spécifiées en 6.2.1, 6.2.2.1 et 6.2.4.1;
- redondance telle que spécifiée en 7.2;
- surveillance du réseau telle que spécifiée en 8.1.2.

Si l'une quelconque des fonctions suivantes est prise en charge par un nœud-460, elle doit être mise en œuvre comme suit:

- connexion aux réseaux contrôlés externes:
  – tous les paquets de données valides avec une adresse IP et un numéro de port corrects reçus de la part d'un réseau contrôlé externe par connexion directe via une passerelle-460 ou une passerelle sans fil-460 (voir 6.3.5.1 et 6.3.6) doivent être traités et vérifiés par un logiciel de niveau d'application dans le nœud-460; ou

    NOTE Ceci peut être effectué pour créer des passerelles vers d'autres protocoles réseau tels que MODBUS ou OPC.

  – si une connexion avec le réseau contrôlé est utilisée afin de transmettre des datagrammes non modifiés entre le réseau-460 et les réseaux contrôlés ou d'autres réseaux-460, alors cette transmission doit être traitée par un redirecteur-460;
- prise en charge des REDS, tel que spécifié en 6.2.3;
- connexion directe aux réseaux non contrôlés, tel que spécifié en 6.3.4;
- compatibilité avec les VLAN, tel que spécifié en 5.1;
- mise en œuvre des services ONF spécifiés par le fabricant, y compris les paramètres de protocole nécessaires, au minimum l'adresse IP et le numéro de port;
- les ports éphémères, en cas d'utilisation, indiqués par le fabricant.

4.4.3 Commutateur-460

Les fonctions suivantes doivent être mises en œuvre dans les composants d'infrastructure de réseau qui relient les matériels dans un réseau-460:

- gestion des trafics du réseau telle que spécifiée en 5.2;
- exigences en matière de sécurité telles que spécifiées en 6.2.1, 6.2.2.2, 6.2.4 et 6.4;
- surveillance du réseau telle que spécifiée en 8.1.3;
- compatibilité avec les VLAN, le cas échéant, telle que spécifiée en 5.2.1.

4.4.4 Redirecteur-460

Les fonctions suivantes doivent être mises en œuvre dans un redirecteur-460:

- gestion des trafics du réseau telle que spécifiée en 5.3;
- exigences en matière de sécurité telles que spécifiées en 6.2.1, 6.2.2.2, 6.2.4 et 6.4;
- surveillance du réseau telle que spécifiée en 8.1.4;
- fonctionnalité du VLAN permettant de combiner deux réseaux physiques (réseaux contrôlés et autres réseaux-460) dans un réseau logique, le cas échéant, tel que spécifié en 5.3.

4.4.5 Passerelle-460 et passerelle sans fil-460

Les connexions aux réseaux non contrôlés doivent être protégées par une passerelle qui satisfait aux exigences applicables aux passerelles-460 spécifiées en 6.3.5 ou aux exigences applicables aux passerelles sans fil-460 spécifiées en 6.3.6. Les exigences en matière de sécurité spécifiées en 6.2, 6.3 et 6.4 doivent être mises en œuvre.

4.5 Exigences relatives aux composants logiques

4.5.1 Fonction de surveillance du réseau

La fonction de surveillance du réseau doit effectuer les fonctions suivantes:

- charge de réseau spécifiée en 8.2.2;
- redondance de réseau spécifiée en 8.2.3;
- topologie de réseau spécifiée en 8.2.4.1;
- détection de collision SFI spécifiée en 8.2.4.2.

4.5.2 Fonction de gestion du système

(Voir 10.12.2)

La fonction de gestion du système doit effectuer les fonctions suivantes:

- conserver toutes les informations de configuration d'infrastructure de réseau et être en mesure de rétablir ces informations aux matériels lorsque cela est demandé. La fonction de gestion doit conserver un historique de la configuration précédente au minimum;
- sauvegarder et restaurer les informations de configuration automatiquement ou manuellement à partir de commutateurs-460, redirecteurs-460, passerelles-460 et passerelles sans fil-460;
- modifier la configuration de l'infrastructure – cette fonction est nécessaire pour permettre l'échange des matériels avec de nouvelles adresses MAC tels que, par exemple, les commutateurs-460, qui autorisent uniquement de connecter une MAC reconnue à un port spécifique.

La fonction de gestion du système doit être disponible de manière redondante.

4.6 Exigences relatives à la documentation du système

(Voir 10.12.3.1)

Un intégrateur de système d'un réseau-460 doit fournir la documentation relative à la topologie du réseau et ces fonctions et dispositifs.

Un intégrateur de système d'un réseau-460 doit fournir la documentation selon laquelle le réseau-460 comprend uniquement les matériels énumérés en 4.3.2.

Voir également 5.4.

4.7 Exigences relatives à la zone protégée

(Voir 10.12.3.1)

Le commutateur-460 et le redirecteur-460 peuvent prendre en charge la désactivation des exigences d'autorisation de l'adresse MAC dans les zones protégées décrites en 6.2.4.2.

La documentation relative au commutateur-460 et au redirecteur-460 doit décrire la zone protégée et les caractéristiques qui peuvent être assouplies à l'installation dans la zone protégée.

5 Exigences relatives à la gestion des trafics du réseau

5.1 Exigences relatives au nœud-460

(Voir 10.5.1)

Le nœud-460 doit satisfaire aux exigences suivantes relatives à la gestion des trafics du réseau:

- tous les trafics doivent être spécifiés comme étant du type comprenant des données conformes à l'IEC 61162-450, par exemple, l'émission de sentences décrite dans l'IEC 61162-1, le trafic de fichiers binaires ou l'ONF;

  NOTE 1 La mise à jour de carte est un exemple d'ONF.

- la sortie maximale de données opérationnelles pour un dispositif doit être déclarée par le fabricant sous la forme d'une moyenne d'octets par seconde calculée sur une période de temps spécifiée;

  NOTE 2 La période de temps spécifiée dépend des caractéristiques de la sortie de données et est choisie de sorte à être appropriée à des fins de gestion des trafics du réseau.

- le comportement du dispositif doit être spécifié par le fabricant lorsque le débit maximal de données d'entrée est dépassé. Le débit de données d'entrée doit être exprimé en octets par seconde tel que disponible dans la ligne réseau comprenant toutes les charges spécifiques aux protocoles;
- seules les données spécifiées pour le nœud doivent être traitées par le nœud;
- les dispositifs doivent continuer à fonctionner normalement avec un taux de perte d'entrée de paquets de 0,1 % au maximum pendant une période de 10 min.

  NOTE 3 Le fonctionnement normal comprend l'aptitude à survivre même en cas de perte dans les interfaces. La réaction normale à ces pertes consiste à continuer comme s'il n'y avait pas eu de perte (c'est-à-dire qu'il y a suffisamment d'informations disponibles pour continuer sans que cela ait de répercutions) ou à produire une indication et/ou une alerte selon la perte.

Si un VLAN est fourni, tout trafic de VLAN doit être compris dans la vitesse maximale de transmission.

NOTE 4 Par exemple, un VLAN est utilisé pour la création d'un segment séparé.

5.2 Exigences relatives aux commutateurs-460

5.2.1 Affectation des ressources

(Voir 10.6.1)

Les exigences suivantes s'appliquent pour l'affectation des ressources:

- un moyen de configurer une suite ou un flux de réseau identifié(e) par la combinaison de l'identificateur d'interface, de l'adresse MAC ou de l'adresse IP, du numéro de protocole et du numéro de port ou une plage de numéros de port;
- moyen d'affecter une ressource de bande passante de réseau à chaque suite enregistrée;
- tout trafic entrant et sortant doit être enregistré;
- tout trafic non enregistré doit être interdit;
- la quantité de bande passante attribuée à un commutateur-460 doit être supérieure à la somme de tous les volumes normaux de trafic de chaque classe de trafic affectée au réseau connecté au commutateur;
- la quantité totale de trafic par interface avec un nœud-450 et un nœud-460 doit être limitée à la valeur de conception du réseau de cette interface. Il doit être possible de sélectionner la valeur de conception du réseau entre 0 % et 50 % de la capacité du port;
- si un VLAN est fourni, un moyen de configurer les réseaux virtuels (VLAN) par interface doit être fourni;
- si un VLAN est fourni, le protocole VLAN de l'IEEE 802.1Q doit être pris en charge;
- un moyen de filtrer le trafic multidiffusion par surveillance du trafic IGMP tel qu'exigé par l'IEC 61162-450:2018;

- un moyen d'envoyer des requêtes d'adhésion IGMP aux autres commutateurs-460, redirecteurs-460, nœuds-460 et nœuds-450.

5.2.2 Prévention de boucles

(Voir 10.6.2)

Le commutateur doit fournir un mécanisme de prévention des boucles, par exemple, RSTP, MSTP. La topologie du réseau et la configuration du commutateur doivent prendre en charge sa convergence en 5 s.

NOTE En présence d'une boucle dans un réseau, le trafic n'est jamais interrompu. Cela augmente le trafic du réseau de manière considérable. Ce problème devient grave lorsque le trafic multidiffusion est multiplié par un commutateur. Une boucle de réseau peut être causée par une erreur de configuration du réseau. Les boucles surviennent également lorsque plusieurs chemins mènent à la destination du fait de la topologie du réseau (c'est-à-dire en cas de topologie maillée de réseau) ou de la redondance du réseau.

Les exigences suivantes sont relatives au RSTP, le cas échéant:

- la version de protocole RSTP de l'IEEE 802.1D-2004 doit être prise en charge;
- un commutateur-460 doit fournir une capacité permettant d'activer le RSTP dans toutes les interfaces.

5.3 Exigences relatives aux redirecteurs-460

5.3.1 Séparation du trafic

(Voir 10.7.1)

Les exigences suivantes s'appliquent pour la séparation du trafic:

- moyen de configurer l'émission de l'ensemble ou d'un sous-ensemble du trafic;
- moyen de configurer le flux maximal du trafic;
- si un VLAN est fourni, moyen de configurer les réseaux virtuels (VLAN) par interface;
- si un VLAN est fourni, le protocole VLAN de l'IEEE 802.1Q doit être pris en charge;
- moyen de filtrer le trafic multidiffusion par surveillance du trafic IGMP tel qu'exigé par l'IEC 61162-450:2018;
- moyen d'envoyer des requêtes d'adhésion IGMP aux autres commutateurs-460, redirecteurs-460, nœuds-460 et nœuds-450.

5.3.2 Affectation des ressources

(Voir 10.7.2)

Les exigences suivantes s'appliquent pour l'affectation des ressources:

- le redirecteur-460 doit avoir une capacité supérieure au total de tous les volumes de trafic de chaque classe de trafic affectée au réseau connecté au redirecteur;
- il doit être possible de configurer le redirecteur-460 de sorte à obtenir un flux maximal de trafic;
- un moyen doit être fourni pour configurer une suite ou un flux de réseau identifié(e) par la combinaison de l'identificateur d'interface, de l'adresse MAC ou de l'adresse IP, du numéro de protocole et du numéro de port;
- un moyen doit être fourni pour affecter une ressource réseau à toutes les suites enregistrées;
- un moyen doit être fourni pour affecter une ressource réseau à chaque réseau virtuel, le cas échéant.

5.3.3 Priorisation du trafic

(Voir 10.7.3)

La totalité ou une partie du trafic peut être priorisée en vue de contrôler le transfert de trafic d'un réseau-460 aux réseaux contrôlés. Par défaut, tout trafic doit avoir une priorité par défaut d'une valeur de zéro. La priorisation peut être fournie par le DSCP (*Differentiated Service Code Point* – code d'accès aux services différenciés) IP ou la CoS (*Class of Service* – classe de service) dans le VLAN, le cas échéant. Il existe huit priorités, pour lesquelles zéro (=000) est la valeur la plus basse et sept (=111) est la valeur la plus élevée.

La priorité de chaque paquet est fournie en fonction du type de trafic. Les informations relatives à la priorité sont fournies dans la préséance du champ DSCP IP ou du champ CoS. Le Tableau 1 est un exemple de relation entre les types de trafics et la priorisation des trafics spécifiée dans DSCP IP et CoS dans le VLAN.

Tableau 1 – Priorisation du trafic avec CoS et DSCP

Valeur CoS	Valeur DSCP	Type de trafic d'après l'IEC 61162-450
000	000000	Données fournies par l'ONF à l'exception du contrôle du réseau et de la gestion du trafic
001	001000	PROP, USR1 à USR8
010	010000	MISC, image binaire simple
011	011000	VDRD, TIME
100	100000	RCOM, image binaire retransmissible
101	101000	TGTD, SATD, NAVD
110	110000	Réservé
111	111000	Contrôle du réseau et gestion du trafic

Les moyens suivants doivent être fournis pour la priorisation du trafic aux bornes d'un redirecteur-460:

a) moyen permettant de gérer la chute du trafic de priorité inférieure en fonction de la priorité;

b) moyen permettant de gérer la chute si la quantité de trafic à transférer par port physique est supérieure à 50 % de la capacité physique de la ligne ou dépasse la capacité maximale définie du débit de données d'entrée du nœud-460 ou du nœud-450. La priorisation du trafic doit être utilisée pour faire chuter le trafic de priorité inférieure jusqu'à ce que le trafic soit en dessous de 50 % de la capacité physique de la ligne ou en dessous de la capacité maximale définie du débit de données d'entrée du nœud-460 ou du nœud-450;

NOTE 1 Un exemple de moyen permettant de gérer la chute est une méthode de configuration dans laquelle la quantité de trafic des différentes priorités peut être assignée.

c) moyen permettant de conserver un trafic sans perte dans chaque priorité jusqu'à ce que la quantité de trafic à transférer soit supérieure à 100 % de la valeur maximale définie pour la priorité dans le commutateur;

d) moyen permettant de signaler l'utilisation de la chute par syslog pour chaque période de 30 s au cours de laquelle la chute a été utilisée ou en répondant à la méthode «interruption SNMP» (c'est-à-dire en demandant des alertes RMON) concernant l'utilisation de la chute (voir 8.2.2).

NOTE 2 Par exemple, la fonction de surveillance du réseau utilisant la méthode "interruption SNMP" interroge le redirecteur-460 concernant l'utilisation de la chute.

5.4 Exigences relatives à la conception du système

5.4.1 Documentation

(Voir 10.12.3.2)

Les documents comprenant les informations suivantes doivent être fournis:

- informations relatives à l'analyse des flux de trafic du réseau-460 et à la topologie du réseau;
- documents spécifiant la quantité totale de trafic du réseau et la charge moyenne de l'ensemble du trafic pour le réseau-460;
- flux maximal du trafic transféré entre un réseau-460 et un autre réseau-460 aux bornes de chaque redirecteur-460;
- priorisation de chaque type de trafic aux bornes de chaque redirecteur-460.

Voir également 4.6.

5.4.2 Trafic

(Voir 10.12.3.3)

La conception du système pour les réseaux-460 doit satisfaire aux exigences suivantes:

- la charge maximale du réseau conçu ne doit pas dépasser la capacité nominale du réseau;
- la charge moyenne de tout trafic dans un réseau-460 ne doit pas dépasser 95 % de la capacité nominale du réseau sur une période de 1 s et ne doit pas dépasser 80 % de la capacité nominale du réseau sur une période de 10 s.

5.4.3 Connexions entre les zones protégées et les zones non protégées

(Voir 10.12.3.9)

La connexion entre un réseau-460 installé dans une zone protégée et un réseau-460 installé dans une zone non protégée doit être établie à l'aide d'un redirecteur-460 (voir Figure 1).

6 Exigences en matière de sécurité

6.1 Scénarios de sécurité

6.1.1 Scénarios de menaces

Comme l'indique l'exemple de topologie de réseau représenté à la Figure 1, les réseaux-460 sont menacés en interne par les nœuds-450 et en externe par les réseaux non contrôlés tels que les autres matériels embarqués ou hors du navire. Par conséquent, il est exigé de protéger les réseaux-460 non seulement contre les menaces internes, mais également contre les menaces externes.

6.1.2 Menaces internes

Les scénarios suivants peuvent se produire dans les réseaux:

- reproduction d'un logiciel malveillant à partir d'autres matériels issus d'un réseau-460 tel qu'un ordinateur bloc-notes infecté par le logiciel malveillant;
- infection provenant de dispositifs de stockage de masse (par exemple, clé USB) corrompus ou lecteurs multimédia amovibles (CD/DVD) utilisés dans le réseau-460, par exemple, en rapport avec la maintenance et l'assistance (autorisées ou non autorisées);
- installation d'une porte dérobée dans un des matériels pour obtenir des privilèges système; d'autres matériels sont ensuite attaqués;

- suppression du fichier système ou modification du fichier de configuration par erreur (erreur de fonctionnement);
- accès illicite interdisant le fonctionnement normal du matériel;
- production de données erronées interdisant le fonctionnement normal du matériel;
- menaces pour la sécurité dans les réseaux contrôlés qui se propagent facilement dans les réseaux-460;
- menaces pour la sécurité dans les autres réseaux-460 qui se propagent facilement dans les réseaux-460;
- interruption du service réseau en raison du volume important du trafic hertzien et des paquets ICMP et IGMP.

Les exigences relatives à la sécurité contre les menaces internes sont décrites en 6.2.

6.1.3 Menaces externes

Les scénarios suivants sont provoqués par les réseaux externes:

- menaces issues des réseaux non sécurisés sans fil;
- infection d'un matériel du réseau-460 par un logiciel malveillant dans d'autres réseaux embarqués;
- connexion à distance à un réseau-460 par l'utilisateur d'un réseau embarqué, qui supprime un fichier important ou modifie la configuration par erreur (erreur de fonctionnement);
- installation d'une porte dérobée par le matériel embarqué afin de l'utiliser comme agent d'attaque; attaque directe aux matériels par le biais de l'infrastructure du réseau, par exemple par le biais du commutateur ou du routeur;
- attaque par balayage – Une personne malveillante trouve un port pour effectuer une attaque en commençant par balayer les ports. Si cette personne trouve le service, elle le balaie avec le port. Par exemple, lorsque le numéro de port 80 est ouvert pour le service Web, la personne malveillante collecte les informations relatives au type et à la version du serveur Web;
- attaque indirecte au réseau-460 par le biais de réseaux non contrôlés tels qu'un autre réseau embarqué;
- attaque consistant à renifler et à modifier les données au cours de la communication avec les matériels et systèmes externes – Lorsque les matériels d'un réseau-460 communiquent avec les systèmes de réseaux hors du navire, l'attaque extrait et modifie les données par reniflage. Par exemple, les informations de la route de la navigation peuvent être exposées aux pirates et aux terroristes et modifiées par ceux-ci;
- trafic excessif de données entrant dans les réseaux-460 et attaques des caractéristiques de protocole, y compris inondation SYN.

Les exigences en matière de sécurité contre les menaces externes sont décrites en 6.3.

6.2 Exigences relatives à la sécurité interne

6.2.1 Généralités

(Voir 10.5.2.1, 10.6.3.1, 10.7.4.1)

Les nœuds-460, commutateurs-460 et redirecteurs-460 ne doivent pas utiliser de fonctions d'interface LAN sans fil et de point d'accès (AP – *access point*) sans fil.

Tous les protocoles VLAN de tunnellisation doivent être désactivés dans les nœuds-460, les commutateurs-460 et les redirecteurs-460.

6.2.2 Protection contre les dénis de service

6.2.2.1 Nœud-460

(Voir 10.5.2.2)

La bande passante maximale opérationnelle d'entrée et de sortie pour un dispositif doit être déclarée par le fabricant sous forme d'une moyenne calculée sur une période de temps spécifiée.

Un moyen d'assurer le fonctionnement normal du nœud dans des conditions de trafic entrant excessif aux bornes de son port Ethernet doit être fourni.

6.2.2.2 Commutateur-460, redirecteur-460, passerelle-460 et passerelle sans fil-460

(Voir 10.6.3.2, 10.7.4.2, 10.8.1)

Une protection contre les attaques DoS utilisant les protocoles ICMP et IGMP doit être fournie. Des méthodes complémentaires de prévention contre les attaques DoS doivent être fournies.

6.2.3 Sécurité de la REDS

(Voir 10.5.2.3)

6.2.3.1 Protection physique

Le nombre de points de connexion (ports USB, lecteurs de disques, etc.) doit être limité au minimum absolu exigé pour le fonctionnement du système ainsi que sa maintenance et sa prise en charge permanentes. Tous les autres points doivent être bloqués physiquement contre tout accès facile par un utilisateur sans outil ou clé.

6.2.3.2 Protection opérationnelle

Les points de connexion doivent limiter leur fonctionnement pour permettre la connexion exclusive avec des sources de données.

Pour les dispositifs à port USB, seule la classe de dispositif USB 08h (stockage de masse USB) est acceptable pour les REDS. Pour les autres dispositifs, le fabricant doit fournir des informations concernant la technologie utilisée et la manière dont le point de connexion satisfait aux exigences de sorte à limiter la connexion aux sources de données uniquement.

Les points de connexion USB utilisés pour les claviers, imprimantes, etc. doivent être bloqués contre tout accès facile par un utilisateur, par exemple au moyen d'un outil, d'une clé ou d'une protection par mot de passe (désactiver/activer) dans les réglages du dispositif.

6.2.3.3 Vérification des fichiers programmes exécutables

Toute exécution automatique au niveau d'un nœud-460 à partir de la REDS, y compris l'exécution automatique USB, doit être interdite.

L'exécution manuelle de tout type de fichier à partir de la REDS ne doit être possible qu'après s'être authentifié afin d'avoir accès au contenu exécutable de la REDS. L'exécution manuelle doit être possible uniquement pour les fichiers qui sont vérifiés avant l'exécution à l'aide d'une signature numérique ou de clés spéciales.

NOTE 1 Une méthode de signature numérique se base sur une paire clé privée/clé publique. En règle générale, une fonction de hachage est utilisée, par exemple, de la famille SHA-2 (l'utilisation de MD5 et SHA-1 est désormais déconseillée, voir l'ISO/IEC 10118-3).

NOTE 2 Les clés spéciales peuvent être des valeurs calculées à partir des données fournies à l'aide d'une fonction spécifiée et comparées à une valeur connue et prévue, la fonction et la valeur étant toutes les deux spécifiées par la source ou l'expéditeur fiable.

6.2.3.4 Vérification des données non exécutables

Toutes les données non exécutables dans les REDS doivent être vérifiées avant d'être utilisées dans les matériels.

6.2.4 Contrôle d'accès

6.2.4.1 Contrôle d'accès aux dispositifs

(Voir 10.5.2.4, 10.6.3.3, 10.7.4.3, 10.8.2)

L'accès permettant d'effectuer des modifications dans la configuration des matériels du nœud-460, du commutateur-460, du redirecteur-460, de la passerelle-460 et de la passerelle sans fil-460 doit faire l'objet d'une authentification de l'utilisateur.

L'authentification de l'utilisateur doit inclure les informations relatives à l'ouverture d'une session. Les exigences suivantes s'appliquent pour le processus de contrôle d'accès aux dispositifs:

- un mécanisme d'authentification de l'utilisateur doit être appliqué avant la modification des réglages du dispositif. Certains exemples d'authentification comprennent les mots de passe et les cartes-clés;
- si un mot de passe est exigé pour l'ouverture d'une session, il doit comporter au moins 8 caractères. Les mots de passe plus longs et les autres jetons d'authentification tels que les clés RSA, etc. peuvent être pris en charge dans la mesure du possible;
- le manuel d'utilisation doit comprendre des recommandations telles que:"il convient que les mots de passe ne contiennent pas le nom de l'utilisateur ou des parties du nom complet de l'utilisateur, telles que son prénom, sa raison sociale, le nom du produit, etc.", "il convient de ne pas utiliser les mots du dictionnaire", "il convient d'utiliser des mots de passe aléatoires et dénués de sens";
- les mots de passe doivent utiliser au moins trois des quatre types de caractères disponibles: lettres minuscules, lettres majuscules, nombres et caractères spéciaux.

6.2.4.2 Contrôle d'accès au réseau

(Voir 10.6.3.4, 10.7.4.4)

Le contrôle d'accès au réseau est destiné à autoriser ou à refuser l'accès aux ressources du réseau-460. Un commutateur-460 ou un redirecteur-460 doit refuser l'accès des matériels non autorisés et des trafics non autorisés par le biais du contrôle d'accès au réseau.

Chaque nœud-450 et nœud-460 connecté à un réseau-460, s'il est installé en dehors d'une zone protégée, doit être autorisé par son adresse MAC et être physiquement connecté à un port aux bornes d'un commutateur-460 ou d'un redirecteur-460. Si un nœud connecté est destiné à être installé dans une zone protégée, un moyen permettant d'activer ou de désactiver l'autorisation par l'adresse MAC doit être fourni.

Tout trafic de contournement et de départ aux bornes d'un commutateur-460 et d'un redirecteur-460 doit être autorisé par l'adresse IP et le numéro de port.

NOTE En règle générale, les fonctions de contrôle d'accès au réseau sont fournies par le fabricant du matériel sous l'appellation "liste de contrôle d'accès".

6.3 Exigences relatives à la sécurité externe

6.3.1 Vue d'ensemble

Tout trafic provenant de réseaux non contrôlés est effectué ou traité par la passerelle-460 ou la passerelle sans fil-460. La Figure 2 donne un exemple de réseau-460 avec une passerelle-460. Comme représenté à la Figure 2, une passerelle-460 est constituée de pare-feu et de DMZ avec différents serveurs. La DMZ se situe entre le réseau-460 interne et le réseau non contrôlé. Deux pare-feu sont mis en œuvre, un pour le réseau non contrôlé et l'autre pour le réseau-460. Ces pare-feu sont classés comme étant des pare-feu internes et externes.

Les composants de la passerelle-460 peuvent être mis en œuvre dans un dispositif ou dans différents dispositifs.

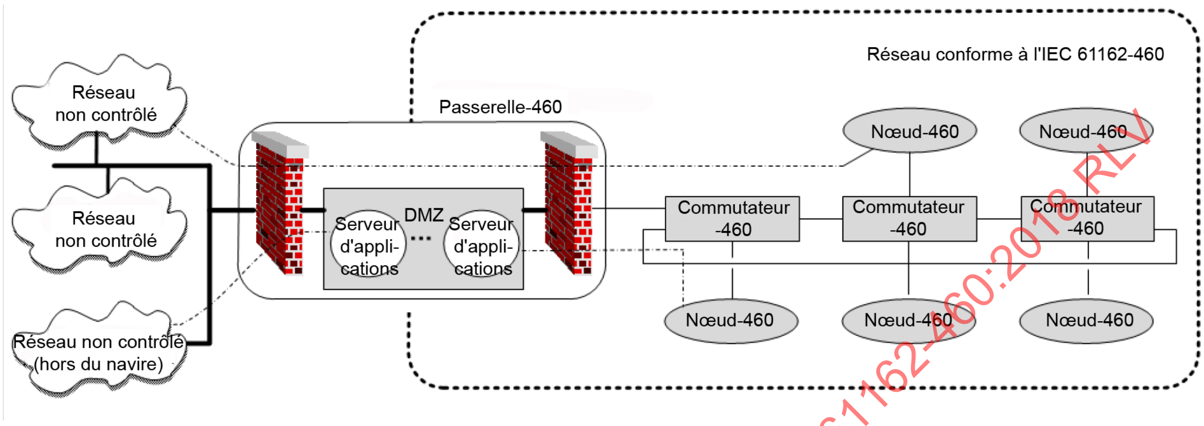


Figure 2 – Réseau-460 avec passerelle-460

6.3.2 Pare-feu

6.3.2.1 Pare-feu externe

Un pare-feu externe bloque tous les trafics, sauf les trafics enregistrés et destinés uniquement aux matériels dans la DMZ. Ceci signifie, en principe, qu'aucune communication directe avec un réseau-460 n'est admise.

6.3.2.2 Pare-feu interne

Un pare-feu interne bloque tous les trafics, sauf les trafics destinés aux matériels dans un réseau-460 et qui proviennent des matériels dans la DMZ. Tous les trafics qui traversent le pare-feu interne sont enregistrés à l'avance.

6.3.3 Communication directe

(Voir 10.8.3)

Lorsque la communication directe est exigée avec les matériels dans un réseau-460, il est exigé d'obtenir la permission de la part d'un administrateur ou d'un superviseur et de surveiller la communication pendant la totalité de la période de communication (voir 6.3.5 et l'Annexe A).

Une connexion directe entre les réseaux non contrôlés et un réseau-460 est uniquement activée à partir d'une passerelle-460 ou d'une passerelle sans fil-460. La connexion directe est protégée contre toute activation à distance via un réseau externe. Une fois la connexion directe établie, un nœud-460 peut utiliser cette connexion pour la communication avec un réseau non contrôlé. Pour de plus amples informations, voir 6.3.4.

Toutes les connexions directes entre des réseaux non contrôlés et un réseau-460 doivent utiliser un réseau privé virtuel (RPV) par le biais d'une passerelle-460 ou d'une passerelle sans fil-460. Toutes les données échangées avec le réseau non contrôlé doivent être chiffrées afin d'être protégées des attaques contre la sécurité. Le RPV peut être utilisé par la passerelle-460 ou la passerelle sans fil-460 pour connecter les réseaux-460 aux réseaux non contrôlés. Une passerelle-460 ou une passerelle sans fil-460 peut également permettre à un nœud-460 de communiquer via le RPV directement avec une autre destination. Dans ce cas, une passerelle-460 ou une passerelle sans fil-460 doit établir la connexion au RPV et la passerelle-460 ou la passerelle sans fil-460 doit fournir les fonctions du réseau pour les connexions dans le réseau-460 interne.

NOTE Le chiffrement protège contre les lectures non autorisées, la signature/l'authentification protège contre les modifications non autorisées et identifie l'expéditeur. Une combinaison des deux est possible.

L'algorithme de chiffrement sécurisé doit utiliser des algorithmes asymétriques ou des algorithmes symétriques avec la longueur de clé suivante:

- un algorithme de chiffrement asymétrique doit fournir une longueur de clé d'au moins 2 048 bits (256 octets) avec un niveau de chiffrement au moins aussi élevé que RSA;
- un algorithme de chiffrement symétrique doit fournir une longueur de clé d'au moins 256 bits (32 octets) avec un niveau de chiffrement au moins aussi élevé que AES.

La clé doit être saisie à l'aide d'une chaîne d'approbation, ou, en cas de clé privée, échangée de manière manuelle et sécurisée ou en utilisant une combinaison de méthode manuelle (par exemple, par appel téléphonique) et de messages (par exemple, par transfert de courriel sécurisé/chiffré).

6.3.4 Nœud-460

(Voir 10.5.2.5)

Un nœud-460 peut échanger des informations avec d'autres matériels directement à partir de réseaux non contrôlés uniquement par le biais d'une passerelle-460 contournant la DMZ si cela est exigé. Lorsque la connexion directe est fournie, les exigences suivantes doivent être satisfaites:

- par défaut à la fabrication, la connexion directe à partir d'un réseau non contrôlé doit être définie comme "non autorisée";
- la connexion directe à un nœud-460 à partir d'un réseau non contrôlé doit uniquement être activée par un opérateur à partir d'un nœud-460; la condition préalable est qu'une connexion directe entre un réseau non contrôlé et le réseau-460 proprement dit soit déjà activée à partir de la passerelle-460 ou à partir de la passerelle sans fil-460.
- un nœud-460 doit porter une indication permanente lorsque la connexion directe avec un réseau non contrôlé est activée;

  NOTE Exemples d'indications: position mécanique, lampe, affichage, etc.

- une mise en garde "Connecté à un réseau non contrôlé" doit être produite, et l'interface décrite en 8.2.7 doit être utilisée lorsqu'une connexion directe est activée;
- la mise en garde peut être remplacée par un avertissement après une période de temps prédéfinie;
- toutes les connexions entre les réseaux non contrôlés et un nœud-460 doivent satisfaire aux exigences relatives à la sécurité de la communication (voir 6.3.3).

6.3.5 Passerelle-460

6.3.5.1 Pare-feu

(Voir 10.8.4)

Les exigences suivantes s'appliquent aux passerelles-460:

- par défaut à la fabrication, la connexion directe à partir d'un réseau non contrôlé doit être définie comme "non autorisée";
- des pare-feu externes et internes configurés avec la combinaison adresse IP source/destination, protocole et numéro de port doivent être fournis;

- toutes les connexions entre les réseaux non contrôlés et un réseau-460 doivent être enregistrées;
- toutes les connexions partant de réseaux non contrôlés jusqu'à un réseau-460 doivent satisfaire aux exigences relatives à la sécurité des communications externes (voir 6.3.3);
- une passerelle-460 doit indiquer la connexion directe activée entre les réseaux-460 et des réseaux non contrôlés ou produire une mise en garde "Connecté à un réseau non contrôlé"; le cas échant, la mise en garde doit utiliser une interface telle que celle décrite en 8.2.7;
- une passerelle-460 doit fournir une liste de toutes les connexions directes activées entre des réseaux-460 et des réseaux non contrôlés; cette liste doit être enregistrée par la passerelle ou par un dispositif externe, y compris les modifications effectuées lors des 12 derniers mois; un moyen d'accéder à la liste doit être fourni; au minimum, les informations suivantes, si elles sont disponibles, doivent être enregistrées pour chaque connexion directe activée: adresse IP source, adresse IP de destination, heure de début et heure de fin de la connexion, protocole et numéro de port;
- la connexion directe avec un nœud-460 à partir d'un réseau non contrôlé doit uniquement être activée par une manœuvre sur le site d'installation ou du côté du réseau-460 du pare-feu; il ne doit pas être possible de l'activer à partir de réseaux non contrôlés; un moyen d'assurer que la manœuvre peut uniquement être effectuée avec la permission d'un administrateur ou d'un superviseur doit être fourni;
- toutes les connexions directes doivent être automatiquement interrompues après une période de temps prédéfinie inférieure ou égale à 4 h, sauf en cas d'intervention de l'utilisateur afin de prolonger cette période de temps;
- aucun trafic de connexion directe ne doit être redirigé automatiquement après une période de temps de 10 min sans trafic sur la connexion.

6.3.5.2 Serveur d'applications

(Voir 10.8.5)

Un serveur d'applications autorise un accès commun aux données devant être perçues par les réseaux non contrôlés et le réseau-460.

Le cas échéant, le serveur d'applications doit fournir un mécanisme d'authentification du niveau d'application, tel qu'un mot de passe au client, à partir des réseaux non contrôlés.

Les exigences suivantes s'appliquent à tout serveur situé au niveau de la DMZ dans une passerelle-460:

- aucun routage des paquets n'est autorisé;
- doit satisfaire aux exigences relatives aux nœuds-460;
- un moyen approprié de protection contre les logiciels malveillants doit être fourni à la plateforme informatique.

6.3.5.3 Accès interopérable au stockage de fichiers de la DMZ

(Voir 10.8.6)

Un moyen de téléchargement/chargement de fichiers entre la DMZ et les réseaux non contrôlés ou un réseau-460 doit être fourni afin d'accéder au stockage de fichiers dans la DMZ. Si l'accès au stockage de fichiers dans la DMZ est fourni, il doit mettre en œuvre un protocole tel que le protocole réseau SMB (par exemple: Samba[2]) ou le protocole SSH de transfert de fichiers (SFTP – *Secure Shell (SSH) File Transfer Protocol*). Si le protocole

[2] Samba est l'appellation commerciale d'un produit distribué par Samba Organization (www.samba.org). Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il peut être démontré qu'ils conduisent aux mêmes résultats.

réseau SMB est employé, la version 1 ne doit pas être utilisée en raison de vulnérabilités sécuritaires.

6.3.6 Passerelle sans fil-460

(Voir 10.9.2)

Les exigences suivantes s'appliquent aux passerelles sans fil-460:

- les fonctions de point d'accès (AP) sans fil ne doivent pas être autorisées, c'est-à-dire qu'une passerelle sans fil doit être manœuvrée uniquement comme client;
- la redirection du trafic à partir du réseau sans fil vers le réseau-460 ne doit pas être autorisée;
- une SF ou ONF correspondante tel que définie dans l'IEC 61162-450 doit être fournie; une passerelle sans fil doit satisfaire à toutes les exigences applicables à une passerelle-460; toutes les données échangées par le biais d'une interface sans fil doivent satisfaire aux exigences de chiffrement de 6.3.3;
- une connexion sans fil doit être établie uniquement pour les points d'accès sans fil enregistrés avec authentification.

6.4 Enjeux sécuritaires supplémentaires

(Voir 10.6.3.5, 10.7.4.5, 10.8.7)

Les fonctions suivantes de gestion sont exigées pour un commutateur-460, un redirecteur-460, une passerelle-460 et une passerelle sans fil-460:

- la configuration doit être conservée après une mise hors tension ou une panne de l'alimentation et le matériel doit retourner en fonctionnement normal dès le rétablissement de l'alimentation;
- lorsque des modifications sont apportées à la configuration, la configuration précédente doit être stockée. Un moyen de rétablir la configuration précédente doit être fourni (voir 4.5.2);
- les instructions d'installation doivent mettre en garde sur le fait que l'accès physique au commutateur-460, au redirecteur-460, à la passerelle-460 et à la passerelle sans fil-460 doit être limité.

7 Exigences relatives à la redondance

7.1 Exigences générales

(Voir 10.12.3.10)

7.1.1 Généralités

La défaillance d'un composant unique (câble, commutateur-460, redirecteur-460, passerelle-460 ou passerelle sans fil-460) ne doit pas affecter la fonctionnalité des nœuds critiques du réseau-460.

La documentation relative à la configuration du système doit identifier les nœuds critiques.

NOTE 1 Trois types de défaillances sont définis dans l'IEC 62439-1: défaillance transitoire, défaillance de composant, défaillance systématique (voir l'Annexe B).

Lorsqu'un problème survient dans un réseau-460, le temps de récupération entre la défaillance et l'activation d'une méthode redondante ne doit pas dépasser 5 s.

NOTE 2 Pour les systèmes qui exigent un temps de récupération inférieur à 5 s, se référer à l'ISO 16425.

La redondance doit être fournie par la redondance d'interface (voir 7.1.2) ou la redondance de dispositif (voir 7.1.3). La Figure 3 donne un exemple de configuration de réseau avec la redondance spécifiée dans le présent document.

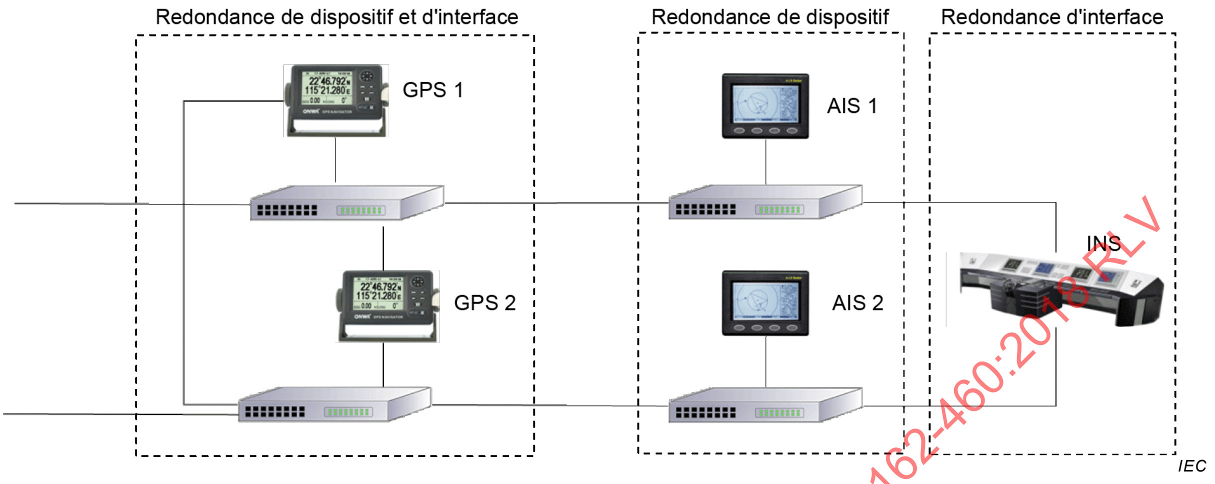


Figure 3 – Exemple de redondance

7.1.2 Redondance d'interface

La redondance d'interface signifie qu'il existe plus d'une interface IEC 61162-450 aux bornes du dispositif et que les interfaces sont connectées à au moins deux commutateurs-460 différents.

Les matériels doivent mettre en œuvre la redondance d'interface par l'une des méthodes décrites ci-dessous.

- Redondance des suites de données

  Les matériels à redondance des suites de données doivent émettre et recevoir les mêmes données de la part des deux interfaces. Lorsque les matériels reçoivent des messages en double, le message en double doit être traité au niveau de la couche réseau ou au-dessus de la couche transport.

  NOTE 1 Le traitement peut conduire à l'utilisation ou à la non-utilisation d'un message par le matériel de réception.

- Redondance établie sur la liaison

  Les matériels à redondance établie sur la liaison doivent émettre et recevoir des données uniquement sur la première interface, tandis que la deuxième interface est en veille. Si la première interface tombe en panne, la deuxième interface doit prendre le relais dans les 5 s qui suivent. Les deux interfaces peuvent être configurées avec deux adresses IP distinctes ou une adresse IP commune.

  NOTE 2 Cette technique est connue sous l'appellation switch fault tolerance (tolérance aux pannes du commutateur), backup bonding (liaison de secours) ou dual homing (double attachement). La commutation d'interface est gérée par le système d'exploitation. La couche d'application considère les deux interfaces comme une interface unique et ne nécessite pas de traitement des messages en double. Ceci permet l'utilisation de protocoles de redondance tels que le protocole de redondance d'adresse commune (CARP – *common address redundancy protocol*).

  NOTE 3 La mise en œuvre de la redondance d'interface dépend de la topologie du réseau local (LAN – *local area network*).

7.1.3 Redondance de dispositif

La redondance de dispositif signifie qu'au moins deux dispositifs ayant la même fonction sont activés en même temps.