IEC 61162-460

Edition 3.0 2024-04

INTERNATIONAL STANDARD

colour inside

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

IEC 61162-460:2024-04(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC 61162-460

Edition 3.0 2024-04

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 978-2-8322-8275-5

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

CONTENTS

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

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

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

Annex C (informative) Guidance for testing 77
C.1 Methods of test 77
C.2 Observation 77
C.3 Inspection of documented evidence 77
C.4 Measurement 77
C.5 Analytical evaluation 78
Annex D (informative) Some examples to use this document 79
Annex E (normative) IEC 61162 interfaces for the network monitoring function 83
Annex F (informative) Distribution of functions around 460-Network 84
Annex G (normative) USB class codes 86
Annex H (informative) Cross reference between IACS UR E26/E27 and IEC 61162-460 87
Bibliography 90

Figure 1 – Functional overview of IEC 61162-460 applications 16
Figure 2 – 460-Network with 460-Gateway 30
Figure 3 – Example of redundancy 39
Figure 4 – Example of network status recording information 43
Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks 74
Figure D.1 – 460-Forwarder used between two networks 79
Figure D.2 – 460-Forwarder used between two networks 79
Figure D.3 – 460-Gateway used for e-Navigation services 80
Figure D.4 – 460-Gateway used for remote maintenance 80
Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices 81
Figure D.6 – 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices 82
Figure E.1 – Network monitoring function logical interfaces 83

Table 1 – Traffic prioritization with CoS and DSCP 22
Table 2 – Summary of alert of network monitoring 48
Table B.1 – Redundancy protocols and recovery times 76
Table E.1 – Sentences received by the network monitoring function 83
Table E.2 – Sentences transmitted by the network monitoring function 83
Table F.1 – Distribution of functions around 460-Network 84
Table F.2 – Equipment standards referencing IEC 61162-460 85
Table G.1 – USB class codes 86
Table H.1 – Cross reference between IACS UR E26/E27 and IEC 61162-460 87

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

FOREWORD

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

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

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

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

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

c) default time for escalation of a warning to an alarm has been changed from max 60 seconds to max 5 minutes as allowed by IMO BAM rules and escalation from caution to warning has been removed from the use of direct access;

d) recorded event size in network monitoring function has been changed from 1 000 bytes to 1 472 bytes (i.e. size of an ethernet datagram in the network);

e) requirements have been incorporated for cyber resilience given by the International Association of Classification Societies (IACS) in their documents UR E26 and UR E27. A new Annex H has been added giving a cross reference between the IACS documents and this document.

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

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

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

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

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

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

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

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

- reconfirmed,
- withdrawn, or
- revised.

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

1 Scope

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

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

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

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

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

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

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

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

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

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

3.9
alarm
high-priority alert, condition requiring immediate attention and action by the bridge team, to maintain the safe navigation and safe operation of the ship

[SOURCE: IEC 62923-1]

3.10
backdoor
installed program allowing access to a computer by providing a method of bypassing normal authentication

3.11
controlled network
any network that has been designed to operate such that authorities are satisfied by documented evidence that the network minimises the security risks to any connected network nodes

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

3.12
controlled shutdown
defined way to switch off equipment under normal operating conditions

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

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

[SOURCE: IEC 62923-1]

3.14
caution
lowest-priority alert, awareness of a condition which does not warrant an alarm or warning condition but still requires attention out of the ordinary consideration of the situation or of given information

[SOURCE: IEC 62923-1]

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

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

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

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

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

3.18
external data source
EDS
network or non-network data source, including, but not limited to REDS, excluding 460-Network for which the equipment belongs

3.19
failure mode and effects analysis
FMEA
method as specified in IEC 60812 for the analysis of a system to identify the potential failure modes, their causes and effects on system performance

3.20
failure mode, effects and criticality analysis
FMECA
analytic method as specified in IEC 60812 that includes a means of ranking the severity of the failure modes

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

3.21
firewall
logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules

[SOURCE: IACS UR E27]

3.22
internet control message protocol
ICMP
protocol according to ISOC RFC 792

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

3.23
internet group management protocol
IGMP
protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and ISOC RFC 4604 (version 3)

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

3.24
least privilege
security concept in which a user is given the minimum levels of access or permissions needed to perform their work

3.25
loss rate
amount of lost data by the receiving device of a flow as lost packets per total amount of packets, measured at the input port of a device

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

3.26
malware
malicious code
software used or created to compromise computer operation

3.27
maximum network load
cumulative maximum amount of all traffic from all network nodes and network infrastructure components of a single 460-Network

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

3.28
maximum transmission rate
maximum number of bytes per second that can be transmitted by a network node or network infrastructure equipment

3.29
multi-factor authentication
authentication using two or more distinct factors to achieve authentication

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

3.30
multiple spanning tree protocol
MSTP
protocol, according to IEEE 802.1Q, which is an extension of RSTP for VLANs

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

3.31
neighbour MAC address
MAC (media access control) address of connected 450-Node or 460-Node as seen by 460 Switch and as reported by SNMP (simple network management protocol)

3.32
network infrastructure component
device that connects at least two nodes in a 460-Network and two different networks, such as 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

3.33
nominal network capacity
network capacity as a byte rate which is based on the configuration

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

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

3.34
other network function
ONF
function block that interfaces to the network as specified in IEC 61162-450

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

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

3.35
privilege
authority to perform functions on a computer system

3.36
rapid spanning tree protocol
RSTP
protocol according to IEEE 802.1D for calculating and configuring the active topology of a network

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

3.37
removable external data source
REDS
user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth[1] devices

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

3.38
remote network monitoring
RMON
standard monitoring specification as described in ISOC RFC 3577

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

3.39
ring topology
topology where each node is connected in series to two other nodes

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

3.40
roll-back
restore the system to a previous known state

3.41
RSA
public-key cryptosystem as described in IEEE 1363

3.42
safety
protection of networks from unintentional threats such as system malfunctioning, misconfiguration and misoperation

3.43
secure area
area with defined physical perimeters and barriers, with physical entry controls or access point protection or access point supervision

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

3.44
security
protection of networks from intentional threats such as virus, worm, denial-of-service attacks, illicit access, etc.

3.45
security strength
number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system

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

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

3.46
simple network management protocol
SNMP
protocol according to ISOC RFC 3411 used to provide management information

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

3.47
SNMP-Trap
method to collect events and statistical information from SNMP enabled equipment such as switches, according to ISOC RFC 1157, ISOC RFC 2021 and ISOC RFC 2819

3.48
shipborne network
data network infrastructure on board a ship to exchange data between equipment on board

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

3.49
sniffing
monitoring and analysis of the network traffic

3.50
stream
combination of all flows from a device that use same protocol

3.51
syslog
protocol according to ISOC RFC 5424, which is used for an external logging in IEC 61162-450

3.52
system integrator
person or organisation responsible for the functionality of the integrated 460-network

3.53
threat
potential cause of an incident in computer security that may result in harm to the system

3.54
transport layer security
TLS
widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. The TLS protocol is described in the following RFCs; RFC2246 v1.0, RFC4346 v1.1, RFC5346 v1.2, and RFC8446 v1.3

3.55
traffic
combination of all streams from a device

3.56
uncontrolled network
any data network that is not a controlled network

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

3.57
virtual local area network
VLAN
network according to IEEE 802.1Q consisting of interconnected networks with bridges

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

3.58
virtual private network
VPN
VPN tunnel
extension of a private network through encapsulated, encrypted, and authenticated links across shared or public networks

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

3.59
warning
condition requiring immediate attention but no immediate action by the bridge team

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

[SOURCE: IEC 62923-1]

3.60
wireless access point
wireless AP
device that connects wireless devices to wired devices through various wireless technologies such as Wi-Fi, Bluetooth

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

4 High-level requirements

4.1 Overview

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

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

4.2 Description

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

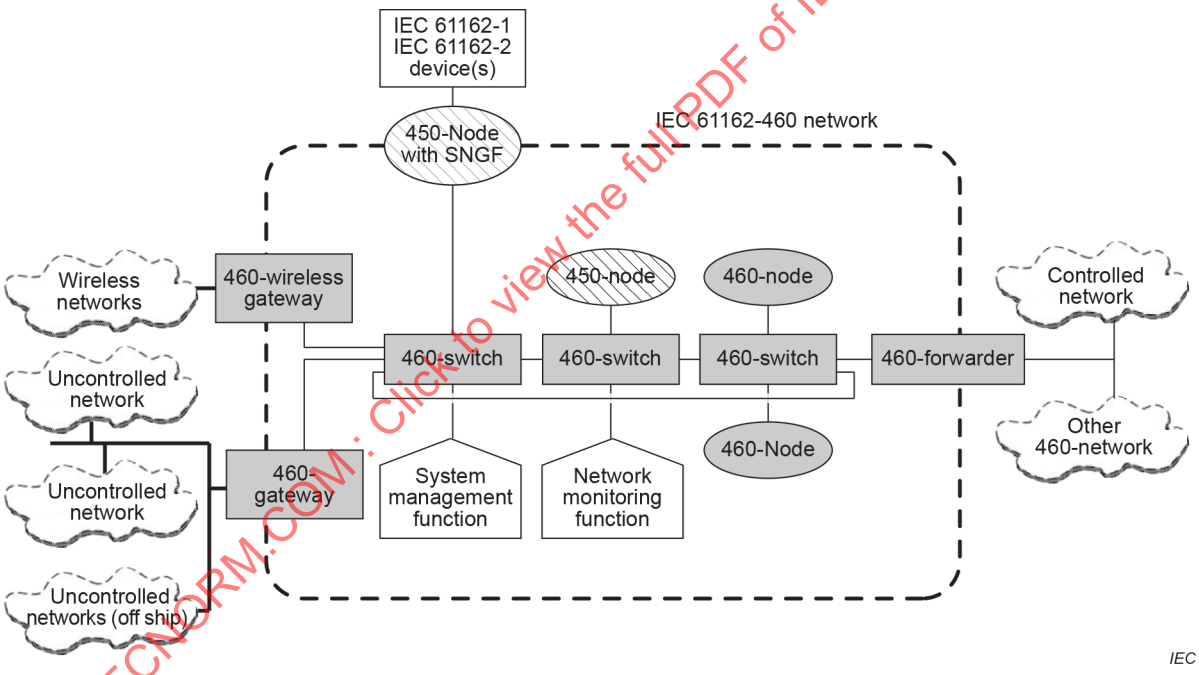

Figure 1 – Functional overview of IEC 61162-460 applications

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

4.3 General requirements

4.3.1 Equipment and system requirements

(See 10.3)

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

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

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

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

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

The list can be a label or list or equivalent.

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

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

4.3.2 Physical composition requirements

(See 10.12.3.1)

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

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

4.3.3 Logical composition requirements

(See 10.12.3.1)

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

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

4.4 Physical component requirements

4.4.1 450-Node

(See 10.4)

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

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

4.4.2 460-Node

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

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

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

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

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

4.4.3 460-Switch

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

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

4.4.4 460-Forwarder

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

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

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

4.4.5 460-Gateway and 460-Wireless gateway

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

4.5 Logical component requirements

4.5.1 Network monitoring function

The network monitoring function shall perform the following functions:

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

4.5.2 System management function

(See 10.12.2)

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

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

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

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

4.6 System documentation requirements

(See 10.12.3.1)

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

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

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

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

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

See also 5.4.

4.7 Secure area requirements

(See 10.12.3.1)

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

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

5 Network traffic management requirements

5.1 460-Node requirements

(See 10.5.1)

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

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

  NOTE 1 Chart update is an example of ONF.

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

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

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

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

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

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

5.2 460-Switch requirements

5.2.1 Resource allocation

(See 10.6.1)

The following are required for resource allocation:

a) means to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and port number or range of port numbers. The source may be from any source or range of sources or group of sources, etc. The destination may be to any destination or range of destinations or group of destinations, etc.;

b) a stream or network flow only to be permitted to interfaces with configured MAC or IP-addresses for specified protocols and ports where network bandwidth limits are applied (see bullet e)). All other traffic shall be blocked;

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

c) means to allocate network bandwidth resource for each stream or network flow;

d) the amount of bandwidth allocated at a 460-Switch shall be more than the sum of all normal traffic volumes of each traffic class allocated to the network connected to the switch;

e) the total amount of traffic per interface to a 450-Node or 460-Node shall be limited to the appropriate bandwidth as a proportion of the switch's or connected node's overall capacity so that the capacity of the switch or node is not exceeded by the traffic allocated to all ports;

f) if VLAN is provided, a means to configure virtual networks (VLAN) per interface shall be provided;

g) if VLAN is provided, VLAN protocol IEEE 802.1Q shall be supported;

h) means to filter multicast traffic by IGMP snooping as required by IEC 61162-450;

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

5.2.2 Loop prevention

(See 10.6.2)

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

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

The following are the RSTP requirements, if provided:

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

5.3 460-Forwarder requirements

5.3.1 Traffic separation

(See 10.7.1)

The following are required for traffic separation:

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

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

5.3.2 Resource allocation

(See 10.7.2)

The following are required for resource allocation:

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

5.3.3 Traffic prioritization

(See 10.7.3)

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

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

Table 1 – Traffic prioritization with CoS and DSCP

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

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

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

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

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

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

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

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

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

5.4 System design requirements

5.4.1 Documentation

(See 10.12.3.2)

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

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

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

See also 4.6.

5.4.2 Traffic

(See 10.12.3.3)

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

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

5.4.3 Connections between secure and non-secure areas

(See 10.12.3.9)

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

6 Security requirements

6.1 Security scenarios

6.1.1 Threat scenarios

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

6.1.2 Internal threats

The following are scenarios that can occur in networks:

- malware replication from other equipment in a 460-Network such as a notebook that is infected by the malware;
- infection from corrupted mass storage devices (e.g. USB flash drive) or removable media drives (CD/DVD) being used within the 460-Network, for example in connection with (authorised or unauthorised) maintenance and support;
- installation of a backdoor in one of the equipment to get system privilege through it; other equipment is then attacked;
- deletion of the system file(s) or change of the configuration file(s) by mistake (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 networks;
- infection of a piece of equipment in the 460-Network by a malware in other shipborne networks;
- remote log-in to equipment in a 460-Network by a user in a shipborne network, which deletes important files or changes the configuration by mistake (misoperation);
- installation of a backdoor by shipborne equipment to use it as an attack agent; direct attack to equipment through the network infrastructure such as switch or router;
- scanning attack – attacker finds a port for attack by scanning the ports first. If found, it scans the service with the port. For example, when port number 80 is open for the web service, the attacker collects the information of web server type and version;
- in-direct attack to the 460-Network via uncontrolled networks such as another shipborne network;
- data sniffing and modification attack during the communication with external equipment and systems – When equipment in a 460-Network communicates with off-ship network systems,

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

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

Requirements for security against external threats are described in 6.2.5.

6.2 Internal security requirements

6.2.1 General

(See 10.5.2.1, 10.6.3.1, 10.7.4.1)

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

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

6.2.2 Denial of service protection

6.2.2.1 460-Node

(See 10.5.2.2)

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

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

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

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

(See 10.6.3.2, 10.7.4.2, 10.8.1)

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

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

6.2.3 REDS security

(See 10.5.2.3)

6.2.3.1 General

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

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

6.2.3.2 Physical protection

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

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

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

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

6.2.3.3 Operational protection

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

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

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

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

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

6.2.3.4 Executable program file verification

See 6.2.5.2.

6.2.3.5 Non-executable data verification

See 6.2.5.3.

6.2.4 Access control

6.2.4.1 Device access control

(See 10.5.2.4, 10.6.3.3, 10.7.4.3, 10.8.2)

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

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

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

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

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

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

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

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

6.2.4.2 Network access control

(See 10.6.3.4, 10.7.4.4)

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

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

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.

450-Nodes and 460-Nodes installed outside of an area providing physical access control shall be authorised before being permitted to connect to a 460-Network and shall be connected to a 460-Switch or 460-Forwarder.

Permissible methods of authorization are:

- MAC Address filtering;
- IEEE 802.1X;
- MACSEC (IEEE 802.1AE).

If a connected node is intended to be installed in a secure area means may be provided to disable this authorisation.

The operator's manual shall include a warning about users adding, removing, replacing or changing configuration of any switch (independent of the type of switch) or node (i.e. any equipment connected to the network). The warning shall explain that all traffic in the cyber secure network is controlled by the 460-Gateways, 460-Wireless Gateways, 460-Switches and 460-Forwarders and that the cyber security of the whole network and all connected equipment may be compromised by any adding, removing, replacing or changing configuration of any equipment by other actors than the system integrator or manufacturer.

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).

6.2.5 Executable and non-executable file security

(See 10.5.2.6)

6.2.5.1 General

Executable and non-executable file security applies to executable and non-executable files from EDS.

Where source authentication and integrity checks are used to verify files, this may be performed by an equipment such as the 460-Gateway before being made available to other equipment within the 460-Network. When provided, the manufacturer's documentation shall describe the method.

6.2.5.2 Executable program file verification

Requirements for normal operation are:

1) all automatic execution at a 460-Node from EDS including auto-run and booting shall be prohibited;
2) manual execution of any type of files from EDS shall only be possible after passing source authentication and integrity check of the executable content of the EDS, for example by using digital signatures or secret keys (i.e., authentication);
3) in the event of a catastrophic equipment failure, cryptographically authenticated software may boot and run from the EDS as a reversionary measure;
4) if the execution of the executable will affect the normal operation of the device, sufficient indication shall be given before execution; the execution shall only be possible in case of

confirmation by the operator. The manufacturer shall provide a list of executables which are possible to execute during normal operation.

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.

NOTE 3 Firmware or application software can automatically authenticate executables without user intervention, provided that an informative indication is given when those executables are executed.

6.2.5.3 Non-executable data file verification

The equipment shall validate the syntax, length and content of any non-executable input data that is received from EDS.

NOTE The above requirements can be a part of an individual equipment standard.

The equipment shall employ cryptographic integrity protection to recognize changes to information from EDS.

The cryptographic integrity protection may be file based, for example encryption of the content, provision of digital signatures or the cryptographic integrity protection may be transport based, for example by using a secure transport method such as provided by SSH or TLS protocols.

The encryption of the content and the provision of digital signature methods may terminate at the DMZ of the 460-Gateway or at an equipment connected to the 460-Network i.e. the digital signature may be verified by the 460-Gateway or in a node within the 460-Network.

The secure transport method may terminate at the DMZ of the 460-Gateway.

Equipment connected to the same 460-Network as a 460-Gateway may access the non-executable files from this DMZ.

6.2.6 Recording of device management activities

(See 10.5.2.7)

Recording of device management activities is applicable for 460-Nodes, 460-Switches, 460-Forwarders, 460-Gateways and 460-Wireless gateways.

Device management activities means managing and controlling equipment connected in the network such as their:

a) configuration (as applicable, IP address, Port number, etc.);

b) user accounts (as applicable, creation and deletion, change of privileges, and login).

For 460-Nodes, 460-Gateways and 460-Wireless gateways device management activities means also as applicable:

c) resource allocation;

d) software management (updates or upgrades);

e) connections with other devices (interface setup for external devices, for example input interface to receive gyro heading, output interface to report GPS position, etc.)

The recording system may be separate for each device management activity.

Equipment shall record device management activities locally and/or send the records to an external device, for example via syslog to the network monitoring function. Each recording shall be timestamped.

Sensitive information shall not be sent in plain text over the network. Typically, this includes username in user accounts and password in user accounts.

The recording shall provide the capability to record at least the last 100 events.

6.3 External security requirements

6.3.1 Overview

All traffic from uncontrolled networks is passed or processed through a 460-Gateway or 460-Wireless gateway. A 460-Gateway consists of firewall(s) (see 6.3.2) and may include support for one or any combination of the following functions:

- direct communication (see 6.3.3);
- DMZ with application services (see 6.3.5.2);
- DMZ with interoperable access to file storage (see 6.3.5.3).

Firewall(s) provide network-access security for the uncontrolled network and the 460-Network. Firewalls for external and internal interfaces may be provided by the same application.

The 460-Gateway may be implemented in one device or in different devices. A DMZ is considered to be a part of a 460-Gateway. Figure 2 shows an example of a 460-Network with a 460-Gateway.

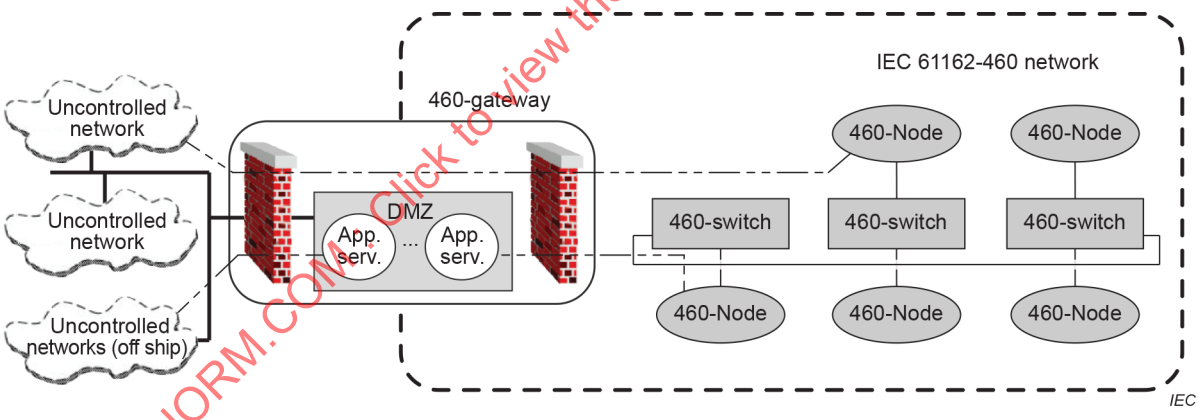

Figure 2 – 460-Network with 460-Gateway

6.3.2 Firewalls

6.3.2.1 External firewall

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

6.3.2.2 Internal firewall

An internal firewall blocks all traffic unless it is either destined to equipment in a 460-Network and it originates from equipment in the DMZ or it is destined to equipment in the DMZ and it originates from equipment in a 460-Network. All traffic passing through the internal firewall is registered (i.e. whitelisted) 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 permitted via a 460-Gateway or a 460-Wireless gateway. A VPN tunnel or equivalent secure connection is established by the 460-Gateway or 460-Wireless gateway and only activated from within the 460-Network i.e. it is protected from activation remotely via an external network.

Secure connections other than VPN tunnels may be used provided that the secure connections meet the same requirements as the VPN tunnel used for direct communication.

Once the VPN tunnel is established, a node can use this tunnel for direct communication with an uncontrolled network. If this functionality is provided the equipment shall comply with 6.3.4.

460-Nodes 460-Switches, 460-Forwarders, 460-Gateways or 460-Wireless gateways are permitted to use this direct connection for communication with devices outside of a 460-Network, for example for access by maintenance personnel.

NOTE 1 It is not permitted to access 450-Nodes from external networks, see 4.4.1.

It shall be possible to terminate the VPN tunnel of the 460-Gateway or 460 Wireless gateway at any time.

At the 460-Network side the endpoint of the VPN tunnel is a 460-Gateway or a 460-Wireless gateway. For the uncontrolled network side, the operator's manual shall describe how to establish a connection to the endpoint of the VPN tunnel on that side.

Both endpoints of the VPN tunnel shall be successfully authenticated before the VPN tunnel is established.

The VPN tunnel shall provide confidentiality and integrity for all traffic passing through the VPN tunnel using a secure encryption algorithm.

The secure encryption algorithm is typically a combination of different asymmetric and symmetric algorithms.

The secure encryption algorithm typically provides authorization, confidentiality, integrity and contains a means to prevent messages being replayed.

NOTE 2 Examples of such secure encryption algorithms include Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPsec). Use of SSH v1, SSL v1.0, v2.0 and v3.0 and TLS v1.0 and v1.1 protocols are now discouraged.

The secure encryption algorithm shall use asymmetric and/or symmetric algorithms with a security strength of at least 128 bits, for example:

- RSA, an asymmetric encryption algorithm, needs keys to be at least 3 072-bit key length (384 Bytes) for 128 bits of security strength;
- AES, a symmetric encryption algorithm, needs keys to be at least 128-bits in length (16 Bytes) for 128 bits of security strength.

Public keys may be delivered using a chain of trust. If private keys are involved, they need to be 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). The manufacturer's documentation shall describe the method.

6.3.4 Node requirements for direct communication

(See 10.5.2.5)

Node requirements for direct communication apply to 460-Node and network infrastructure components.

Equipment can exchange information with other equipment directly from uncontrolled networks only through a 460-Gateway bypassing the DMZ if it is required as described in 6.3.3.

Equipment using direct communication may need to use additional means to ensure secure end-to-end communication between nodes at the two ends of the VPN tunnel, for example use of TLS protected communication, SSH protocol, a nested VPN tunnel, application level digital signatures, application level encryption, etc. The manufacturer shall declare which methods are provided.

Access to equipment from or via uncontrolled networks shall only be granted after successful user authentication.

Confidentiality and integrity shall be provided using cryptographic methods for sensitive information, including the exchange of authenticators during user authentication.

Multi-factor authentication shall be required for any access by human users from an uncontrolled network to devices within the 460-Network. Where the means of remote access is available but not provided by the manufacturer themselves, the manufacturer shall document and demonstrate a system providing access to devices within the 460-Network which requires multi-factor authentication for human users.

NOTE 1 Typically this involves shore-based service engineers remotely accessing systems on the 460-Network for the purposes of maintenance but can also include connections from other networks on-board the ship.

Equipment may trigger a VPN tunnel to be established from a 460-Gateway or 460-Wireless gateway.

When the ability to trigger a VPN tunnel on a 460-Gateway from equipment is provided, the following requirements shall be satisfied:

- by manufacturing default, direct connection from an uncontrolled network shall be set to "not allowed" or "inactive", such that operator action is necessary to initiate a direct connection;
- the direct connection to equipment from an uncontrolled network shall only be activated by an operator from the equipment; a precondition is that a VPN tunnel between uncontrolled network and the 460-Network itself is already established within the 460-Gateway or the 460-Wireless gateway;
- the equipment shall have a permanent indication when direct connection with an uncontrolled network is activated;

  NOTE 2 Examples of indication are mechanical position, lamp, display, etc.

- a caution (alert title = "Unct. connection", alert description (optional) = "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.

6.3.5 460-Gateway

6.3.5.1 General

(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";
- firewall(s) shall be provided which are configured with the combination of source and destination IP address, protocol and destination port number (see 6.3.2);
- all connections between uncontrolled networks and a 460-Network shall be registered (i.e. all network traffic that does not match a set firewall rule shall be blocked by the firewall);
- all connections from uncontrolled networks to a 460-Network, or from controlled 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 (alert title = "Unct. connection", alert description (optional) = "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 services

(See 10.8.5)

An application service may be built inside the same physical device as the 460-Gateway or may be in a separate device connected logically to the 460-Gateway. Application services are any applications in the DMZ that provide more functionality than the file storage of DMZ (see 6.3.5.3).

When not being used in the direct connection mode or as a file storage of DMZ, all communication between uncontrolled networks and the 460-Network is provided by application services.

An application service, for example, allows a common data access to be seen by the uncontrolled networks and the 460-Network. Application services do not apply when the related part of the data within the equipment is accessible only from the 460-Network. For example, application services are not applicable to a web interface used to access the equipment which is accessible only from the 460-Network.

If provided, application services shall provide an endpoint application-level authentication mechanism, such as password, smartcard, digital signature, dongle, etc., of clients, from uncontrolled networks, and provide cryptographic integrity protection. Confidentiality shall be

ensured for information that is subject to read or write authorisation, e.g., sensitive/secret information.

The following are requirements for a 460-Gateway providing one of more application services that are located at the DMZ:

– no routing of packets is allowed from uncontrolled network to 460-network;
– the 460-Network connection side shall comply with the following 460-Node requirements;
  - 5.1 – Network traffic management requirements;
  - 6.2.2.1 – Denial of service protection;
  - 6.2.3 – REDS;
  - 6.2.4.1 – Device access control;
  - 7.2 – Redundancy;
  - 8.1.2 – Network Monitoring.
– 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 via an application service (see 6.3.5.2).

Means may be provided to download/upload files between the DMZ and controlled network. 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) to provide cryptographic integrity protection and access control. Confidentiality shall be ensured for information that is subject to read or write authorisation, e.g., sensitive/secret information. Read or write authorization can be implemented using user authentication and access controls to the files in the DMZ. 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:

- a wireless gateway shall meet all the requirements of a 460-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;
- 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.

---

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.

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.

The following network management functions are required:

NOTE 1 This list of network management functions is based on IACS UR E26 and IACS UR E27. When these functions are supported, an IEC 61162-460 compliant equipment is assumed to be compliant with IACS UR E26 and IACS UR E27.

- use of firewalls for communication between secure networks, including protection from excessive data flow and application of principle of "Least Functionality" (restrict/prohibit non-essential functions/ports/protocols/services) (see 3.4, 3.7, 6.3.2, 6.3.5.1 and 6.3.6);

  NOTE 2 To support IACS UR E26, sections 4.2.1 and 4.2.2.

- possibility to interrupt and abort remote maintenance (direct connections) at all times and roll back to a previous safe configuration (see 6.5.5 and 6.5.2);

  NOTE 3 To support IACS UR E26, section 4.2.6.3.2.

- diagnostic functions, verification and testing of security functions (see 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.6 and 8.2.7);

  NOTE 4 To support IACS UR E26, section 4.3.2.

- backup and restore capability including roll-back to safe state to support Incident response (see 6.5.2);

  NOTE 5 To support IACS UR E26, sections 4.4 and 4.5.

- network topology monitoring to support for asset inventory for HW and SW used in systems and networks (see 8.2.4);

  NOTE 6 To support IACS UR E26, section 4.1.1.

- secure software development lifecycle (SSDLC) (see 6.6).

  NOTE 7 To support IACS UR E27, section 5.

IMO has specified for navigation and radiocommunication equipment and systems what to do in each case of inability to perform required functionality. These are understood as "fall back to a condition in which a reasonable safe state can be achieved" and as required "fall-back actions". The following are required for fallback to a minimal risk condition:

a) when applicable IMO Performance Standards exist, the equipment shall comply with the applicable related technical standard which refer to applicable IMO Performance Standards;

b) when no applicable IMO Performance Standards exist, the operator's manual shall describe effects of lack of input data and effects of inability of the equipment to continue its functionality and any appropriate action the operator may take on such cases. Fall-back actions may include:

   1) bringing the system to a complete stop;

   2) disengaging the system;

   3) transferring control to another system or human operator;

4) set outputs to a predetermined state if normal operation cannot be maintained as a result of a cyber attack. The predetermined state could be:
   - unpowered state (for example, dry contact);
   - last-known value;
   - fixed value;
   - flagging the value as not available or invalid;
5) other compensating actions.

6.5 Onboard software maintenance

6.5.1 General

(See 10.6.3.6.1)

This subclause, 6.5, applies during normal operation, during remote maintenance and in maintenance mode.

NOTE 1 Equipment can change in build standard during its life cycle. For example, new features can be added, existing features can be amended or design mistakes – often known as bugs – can be fixed. The type approval certificate is valid for an identified version of the product. Therefore, a new test of compliance and resulting new certificate can be required when the software is changed.

NOTE 2 The local conformity assessment laws, for example within the European Union, can require reporting of any modification to the conformity assessment authority.

Security related updates to software are an important part of protecting a system against attack, whilst bug fixes and new functionality are often important in maintaining equipment. It is important however to ensure that changes to software do not adversely impact the intended functionality of the equipment or its compliance to applicable regulations, prior to their deployment.

If provided, software maintenance shall be performed by any of the following methods:

– authorized persons local to the equipment, in maintenance mode;
– the crew in normal operation, where semi-automated means are provided;
– authorized persons remote from the equipment in maintenance mode for remote access.

Maintenance mode is intended to be available only to personnel authorized by the manufacturer.

Facilities or procedures, either external or internal to the equipment, shall be provided for restoring the equipment to a known good state, for example to recover from corruption or malware infection. This shall be described in the installation manual and may, for example, involve restoration from a backup or replacing and re-configuring affected equipment (see 6.5.2).

6.5.2 Roll back to previous safe configuration

(See 10.6.3.6.2)

The equipment shall support roll back to a previous safe configuration. As a minimum, the roll back shall be available at least for the manufacturer's working configuration.

Roll back procedures may include storing of the manufacturer's previous configuration (i.e. software and setup) in another shipboard equipment or REDS. If this method is provided, the operator's manual shall include instructions on how to execute the roll back procedure including the storage of the manufacturer's previous configuration and shall include instructions for storing the copy of the manufacturer's previous configuration for future use (for example, mark

and store the used USB memory stick in a safe place from where it is available for the future roll back). All data files or executables of this method including the manufacturer's previous configuration shall be subject to source authentication and integrity check.

6.5.3 Software maintenance in maintenance mode

(See 10.6.3.6.3)

The installation manual shall describe the means available to update the software in maintenance mode.

The manufacturer shall ensure that, where updates to software have the potential to impact the intended functionality of the equipment, the service documentation describes any limitations to the application of the updates.

6.5.4 Semi-automatic software maintenance by the crew onboard the vessel

6.5.4.1 General

Semi-automatic software maintenance may be provided by the equipment.

Semi-automatic software maintenance may be performed by authorised persons on board the vessel including members of the crew or other users authorised by the manufacturer.

This kind of software maintenance may be based on files classified as data files or as executables. Such files are subject to source authentication and integrity check.

The software maintenance related files may arrive to a remote system (for example by post, email attachment) from which the files are required to be moved to the equipment (for example by using REDS) or the software maintenance related files may arrive to be readily available for the equipment (i.e. no additional manual transfer of the files by the user is required, for example though 460-Gateway).

6.5.4.2 Requirements

(See 10.6.3.6.4)

The operator's manual shall describe instructions for semi-automatic software maintenance.

The files associated with the semi-automatic software maintenance shall be source authenticated and integrity checked as applicable (see 6.2.5).

The execution of a software update shall begin only after successful user authentication.

Access to semi-automatic software maintenance shall not lead to access to maintenance mode.

Semi-automatic software maintenance can be launched from the maintenance mode.

The equipment shall request and receive positive user confirmation prior to commencing the software update.

Two steps are required before execution of an update, user authentication and obtaining express permission to begin installing the update. Both of these steps may be performed at the same time.

Where maintenance to software has the potential to impact the intended functionality of the equipment, the impact and/or any limitations to the application(s) shall be indicated to the

operator and the equipment shall request and receive positive user confirmation prior to commencing the software update.

The user shall be notified if, once initiated, the software update fails to successfully complete.

After completion of the update, the authenticated user shall be able to roll back to the manufacturer's previous configuration (see 6.5.2). This capability to roll back shall be possible also after power off/power on sequence.

The equipment may inform the user about a software update readily available or the user may initiate the process of software update.

If provided, informing the user about a readily available software update:

a) shall not obscure or prevent normal functionality of the equipment;

NOTE An indicator, small icon or small dialog can comply with above.

b) may provide the possibility to accept initiation of the procedure to update software;

c) shall include the possibility to acknowledge the information without initiation of the procedure to update software.

d) may include a repeated reminder, but this shall comply with the above requirements from a) to c);

6.5.5 Remote software maintenance

(See 10.6.3.6.5)

Remote software maintenance happens remotely, for example through a 460-Gateway (see 6.3.3) or for example from another node connected in the same segment of the 460-Network.

The operator's manual shall describe instructions for remote software maintenance.

The establishment of direct communication though a 460-Gateway may enable remote monitoring of equipment but does not enable commencing of the remote software maintenance, The commencing of a remote software maintenance shall begin only after enabled by successfully authenticated user onboard.

Where maintenance to software has the potential to impact the intended functionality of the equipment, the impact and/or any limitations to the application(s) shall be indicated to the operator and the equipment shall request and receive positive user confirmation prior to commencing the software update.

The files associated with the remote software maintenance shall be source authenticated and integrity checked as applicable (see 6.2.5).

The onboard user shall be notified, if once initiated, the remote software maintenance fails to successfully complete (for example due to termination of remote connection, etc.).

The authenticated onboard user shall be able to terminate the remote software maintenance at any time, this termination shall be available at the Human Machine Interface of the equipment and may be available at the Human Machine Interface of an equipment related to the communication path of the remote maintenance, for example 460-Gateway.

After completion, failure or termination of the remote software maintenance, the authenticated onboard user shall be able to roll back to the previous configuration (see 6.5.2). This capability to roll back shall be possible also after power off/power on sequence.

6.6 Secure software lifecycle management

(See 10.6.3.7)

The requirements related to onboard software maintenance part are given in 6.5,

Where applicable, the documented evidence on the applied secure software lifecycle management (e.g. software testing, version control, software/firmware upgrade procedures) shall be included into the conformity assessment.

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.

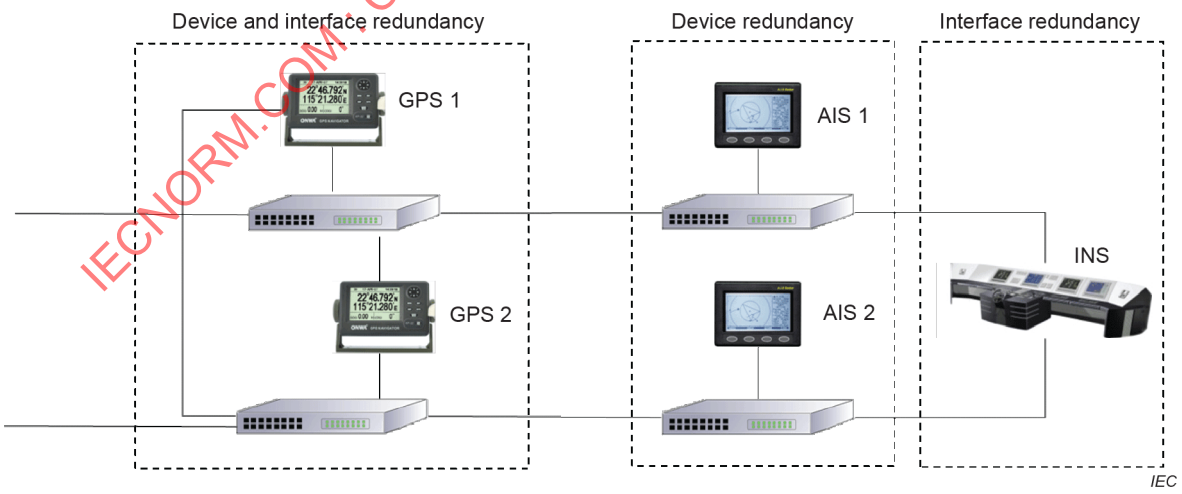

Figure 3 – Example of redundancy

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 10.5.2.6)

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, see 7.7.

Documentation shall be provided describing the redundancy capability.

7.3 460-Switch requirements

(See 10.5.2.6)

For critical nodes the network architecture shall avoid single points of failure for network paths.

NOTE 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 is 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 FMECA for its redundancy capability and criticality.

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 information 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 all outbound TCP and UDP connections and their designed maximum traffic rate;
- the change of any outbound TCP and UDP connections – add, delete or modify;
- the list of all outbound TCP and UDP connections 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.

NOTE Periodical sending facilitates that the configuration is recorded by the syslog even if the syslog was not able to receive and record at the time of configuration change.

Consideration should be made to avoid excessive syslog messages, such as representing ephemeral source ports by a "wildcard".

8.1.3 460-Switch

(See 10.6.3.6)

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

- the interface information (interface input and output link utilization);
- 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 information for monitoring at a 460-Switch is the interface input and output link utilization, for example, 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, for example, in a 0 % to 100 % scale of network capacity) have been made, the changes shall be reported using SNMP-Traps and/or syslog. The traffic 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 function 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.

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). The HMI of the network monitoring function may be provided on a Central Alert Management HMI, or on the alert HMI of other equipment on the 460-Network.

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 local timestamped recording of any device management activities including adding of new devices, removing of existing devices and

changes of details of existing devices in the setup of network topology monitoring including who performed the management activity, for example the identifier of the authorized user. If these recordings are sent over a network they shall be in encrypted form.

The network monitoring function shall keep a timestamped recording of events listed below which are available on demand. The recording shall be capable of storing events for at least the last 90 days or the last 10 000 events, whichever is smaller. At least the first 1 472 bytes of 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 syslog (see 8.2.2, 8.2.3 and 8.2.4).

NOTE This recording is different from the generic syslog recording storing all syslog messages (see 8.2.5).

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

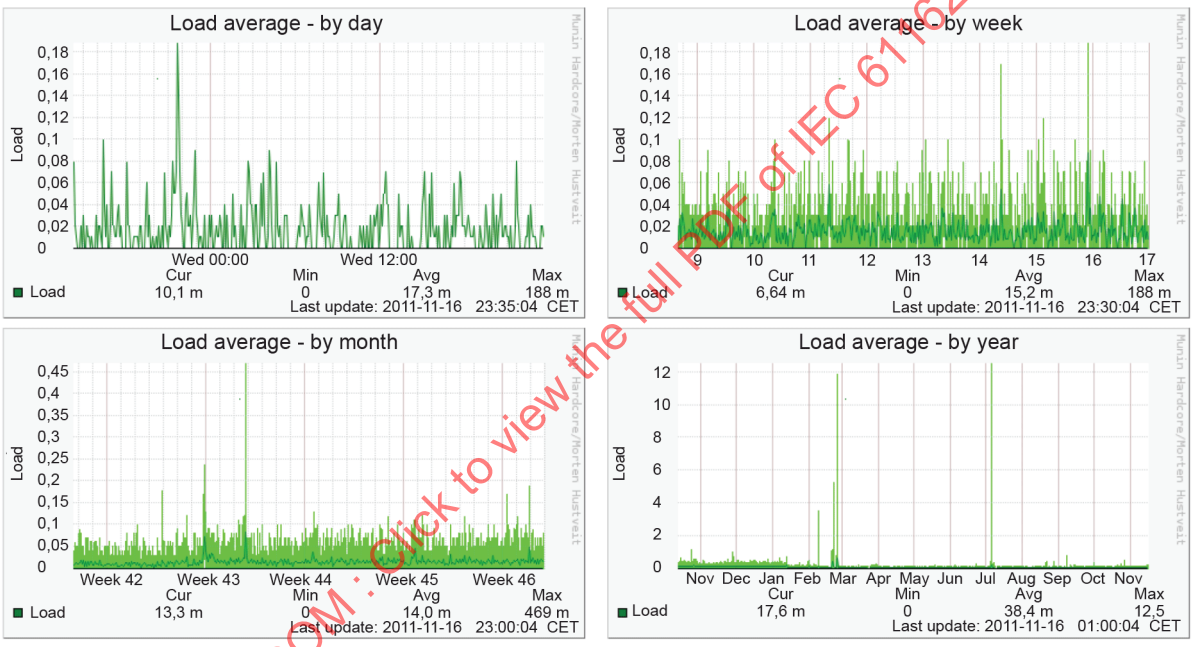

Figure 4 – Example of network status recording information

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 support all 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.

NOTE For each 460-Switch or 460-Forwarder one of the listed methods or a combination of the listed methods can be used.

The network load monitoring function shall generate the following alerts.

- Caution: Alert title "Network load", Alert description (optional) "Network traffic capacity may be exceeded" – when the observed network load has exceeded the 90 % 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. A lower percentage threshold may be used where equipment performance is adversely impacted at lower network traffic levels;
- Warning: Alert title "Network load", Alert description (optional) "Network traffic capacity exceeded" – when the observed network load has exceeded the 90 % 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. A lower percentage threshold may be used where equipment performance is adversely impacted at lower network traffic levels.

8.2.3 Redundancy monitoring function

(See 10.11.3)

Redundancy monitoring is mandatory for redundantly available critical nodes and it is optional for redundantly available non-critical nodes.

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) and included into the redundancy monitoring function. 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 support all 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.

NOTE 1 For each 460-Switch or 460-Forwarder one of the listed methods or a combination of the listed methods can be used.

Where available, 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.

NOTE 2 Some of the means for providing redundancy cannot provide this information, e.g. a common MAC address being used by independent Ethernet interfaces or on ONF devices.

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:

Alert priority: Caution

Alert title: Net redundancy

Alert description (optional): 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

NOTE 1 This topology monitoring performs dynamic asset monitoring for the content of the asset inventory described in IACS UR E26. This can be useful for maintaining the asset inventory.

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 support all 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.

NOTE 2 For each 460-Switch or 460-Forwarder one of the listed methods or a combination of the listed methods can be used.

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.

Alert priority: Caution

Alert title: New dev.detected

Alert description (optional): 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:

a) 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;

b) 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;

c) SFI collision monitoring may provide reset of the SFI Table at boot up of SFI collision monitoring and shall provide reset of the SFI Table on demand. The entries of state "detected SFI collision" or "potential SFI collision" shall be removed at the reset of SFI Table;

d) based on the SFI Table, non-colliding SFI can be identified. Multiple entries with the same MAC address but with different SFIs are not defined as a collision of SFI. Similarly multiple entries with the same IP address but with different SFIs are not defined as a collision of SFI;

e) based on the SFI Table, redundantly available SFIs can be identified from differences in the "Instance number" fields of SRP sentences. Redundantly available SFIs do not cause collision of SFIs;

f) based on the SFI Table, a potential SFI collision or SFI collision is detected when all conditions below are met:

   – identical SFIs are present in multiple SRP sentences; and

   – "Instance number" field of at least one of the SRP sentences contains a null or two SRP sentences contain equal values; and

   – there are either differences in the "MAC address" field or differences in the "IP address" field of SRP sentences.

When a potential SFI collision is detected, the SFI collision monitoring function:

g) shall set the related SFI entries in the SFI Table to the state of "potential SFI collision";

h) shall send an SRP-sentence with all fields being null fields (i.e. request to refresh SRP by equipment connected to network) and TAG block with parameter-code "d:" set to the value of the related SFI;

i) shall wait for response SRP sentences from equipment connected to network for a timeout period determined by the manufacturer, for example 10 s;

j) if the received SRP sentences do not indicate SFI collision (see criteria for detection in bullet f); the network monitoring function shall update the SFI Table from the received SRP sentences related to the potential SFI collision and shall remove the state of "potential SFI collision" from the related SFIs in the SFI Table;

k) SFI Table entries may be deleted from the SFI Table if they are not updated after an SRP request and timeout, see bullets h) and i);

l) if received SRP sentences indicate an SFI collision, the network monitoring function shall set the related SFIs in the SFI Table to the state of "detected SFI collision" and shall generate the following alert.

   Alert priority: Caution

   Alert title: SFI collision

   Alert description (optional): SFI ccxxxx collision in the network.

   Where ccxxxx is the identifier string of the SFI.

NOTE SFI collision monitoring function as source can aggregate or group multiple instances of Cautions.

The SFI collision related caution shall remain as long as the SFI related entry in the SFI Table is in state "detected SFI collision".

The SFI collision monitoring may periodically, for example every 60 s, check if an already detected state "detected SFI collision" is still valid. This is performed:

- by sending an SRP-sentence with all fields being null fields and TAG block with parameter-code "d:" set to the value of the SFI set as "SFI collision detected" in the SFI Table;
- if received SRP sentences do not indicate SFI collision (see criteria for detection in bullet f), update SFI Table from the received SRP sentences related to the detected SFI collision and remove the state of "detected SFI conflict" from the related SFI in the SFI Table.

Where an SFI entry exists in the SFI table and an SRP sentence has not been received for this SFI entry for some time, the SFI collision monitoring function may mark the SFI state entry as "stale" and send one or more SRP sentences with all fields being null fields and TAG block with parameter-code "d:" set to the value of the SFI. Stale entries in the SFI table may be periodically removed after a period determined by the manufacturer. This method may avoid the need for the SFI table to be manually reset.

Example 1

There are 2 entries in collision in the SFI Table:

SFI	Instance number	IP	MAC
GP0001	1	192.168.0.12	A7-98-12-0C-28-31
GP0001	1	192.168.0.13	A7-98-12-0C-28-32

A service engineer reconfigures the second device to use a different SFI GP0002. After reconfiguration the second device sent SRP with SFI set to GP0002:

GP0002	1	192.168.0.13	A7-98-12-0C-28-32

Which result an SFI Table

GP0001	1	192.168.0.12	A7-98-12-0C-28-31
GP0001	1	192.168.0.13	A7-98-12-0C-28-32
GP0002	1	192.168.0.13	A7-98-12-0C-28-32

The SFI collision monitoring function may request a SRP sentence refresh from connected equipment by sending a SRP sentence with all fields being null fields and TAG block with parameter-code "d:" set as GP0001. Within the timeout there is only one SRP response:

GP0001	1	192.168.0.12	A7-98-12-0C-28-31

Which means that SFI collision monitoring function can remove the non-responded SFI entry for GP0001. This result an SFI Table

GP0001	1	192.168.0.12	A7-98-12-0C-28-31
GP0002	1	192.168.0.13	A7-98-12-0C-28-32

Example 2

The SFI collision monitoring function may detect multiple potential SFI collisions. Each potential SFI collision may be requested by separate SRP sentences or combined into one SRP sentence using TAG block parameter-code "d:"

Two separate SRP

SRP sent to /d:GP0001*hh/

SRP sent to /d:EI0001*hh/

A single combined SRP

SRP sent to /d:GP0001,d:EI0001*hh/

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-Switches, 460-Forwarders, 460-Gateways and 460-Wireless gateways have provided.

The syslog shall be capable of storing messages for at least the last 90 days or last 20 000 messages, whichever is smaller.

8.2.6 Redundancy of network monitoring function

(See 10.12.7.3)

The network monitoring function shall be redundantly available using device redundancy. It shall be available at least in two devices out of the following list:

- 460-Node;
- 460-Gateway;
- 460-Switch.

8.2.7 Alert management

8.2.7.1 Alerts and indication

(See 10.11.6.1)

Where the physical local HMI is provided, alerts and indications shall comply with the presentation requirements specified in IEC 62923-1.

NOTE An equipment will not necessarily provide a local HMI for its own alerts. In such case there is an arrangement to communicate with another piece of equipment, for example CAM of BAM, which provides the HMI service for these alerts (see IEC 62923-1 for systems failures, redundancies, back-up and fallback arrangements).

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

Table 2 – Summary of alert of network monitoring

Source	Purpose	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	3159
460-Node	Direct connection to uncontrolled network as a warning (see 6.3.4)		x			x	3158
460-Gateway	Connected to uncontrolled network (see 6.3.5.1)			x		x	3163
Network monitoring function	Network traffic capacity may be exceeded (see 8.2.2)			x		x	3166
Network monitoring function	Network traffic capacity exceeded (see 8.2.2)		x			x	3168
Network monitoring function	Network redundancy lost for xxxx (see 8.2.3)			x		x	3173
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 sentences of Annex E and comply with the communication requirements of IEC 62923-1 and IEC 62923-2. In the BAM concept, the network components act as alert sources.

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 5 min.

NOTE If many devices have short escalation periods, it makes the bridge's CAM-HMI difficult to use.

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.

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 security risks to any of its connected network nodes have been minimized. This shall, as a minimum, satisfy the following requirements in normal operation:

- the controlled network, any associated infrastructure and the environment in which it is installed shall physically and/or logically prevent unauthorized devices from making connections to the controlled network through physical or wireless interfaces;
- network nodes shall not allow unauthorised users direct access to operating systems or functions that can be used to insert non-authorised traffic into the network;

- the nodes and infrastructure components in a controlled network shall provide means to prevent the transfer or execution of potentially malicious content from REDS, see 6.2.3.

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 all or a subset of 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.

[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.

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 61162-450:2023 as far as applicable.

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.

Use manufacture's documentation to identify equipment or network connection points which can be disconnected manually or automatically in order to isolate the 460-Network from other networks or network segments (see 4.6) and confirm by observation that such points are clearly marked.

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. Use multicast addresses and port numbers (either using multicast 239.192.0.254 port 514 or UDP unicast)

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 in total all IEC 61162-450 compliant data in each VLAN does not exceed the defined 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, but not over 90 % of the maximum available for the network interface, for a period of at least 10 min. Confirm by analytical evaluation that the functionality not dependent of the incoming traffic of the 460-Node is available as described by the manufacturer's documentation.

Use simulation arrangements to create traffics of 200 % of the maximum that is declared by the manufacturer, but not over 90 % of the maximum available for the network interface. 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)

10.5.2.3.1 Physical protection

Where physical protection is provided, refer to the manufacturer's documentation and confirm by inspection of the documented evidence that the number of connection points for REDS are limited to the minimum required for the operation of the system and its lifetime maintenance and support.

For all other connection points, either:

- confirm by observation that they are physically blocked from easy access without a tool or key, or that they can be used for charging only; or
- confirm by inspection of the manufacturer's documentation that there is an instruction in the manufacturer's installation manual that the equipment shall only be installed in a closed console or cabinet requiring additional tools or keys to open and that there is a notice of cyber security risk if not installed as described by the manufacturer.

10.5.2.3.2 Operational protection

Where operational protection is provided, for USB connection points, use the manufacturer's documentation and confirm by analytical evaluation that the EUT refuses to perform any other functionality than that specified in the manufacturer's documentation.

Refer to manufacturer's documentation and confirm by inspection that a declaration is included about which alternative of operational protection for each removable interface is provided.

If it is possible for a REDS technology to have functionality other than data storage (for example from keyboard to data storage), then attach one by one an example of such a non-data storage device to the connection point and confirm by analytical evaluation that the EUT only performs functions specified in the manufacturer's documentation.

If applicable, refer to the manufacturer's documentation and confirm by inspection that information is available as to how the interface is limited to its intended functionality and protected against misuse for any removable device which cannot practically be restricted using the options listed in 6.2.3.

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 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 or network infrastructure component provides direct connection for exchange of information with other equipment connected to an uncontrolled network.

If additional means to secure end-to-end communication between different equipment communicating via the VPN tunnel are provided, confirm by inspection of the manufacturer's documentation that such means are described.

Confirm by observation that access from or via uncontrolled networks into the equipment is only granted after successful user authentication.

Confirm by analytic evaluation that cryptographic methods are used to protect confidentiality of sensitive information.

Confirm by inspection of the documented evidence that multi-factor authentication is required for any access by human users from an uncontrolled network to devices within the 460-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 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;
- the caution is removed after closing of the direct connection.

10.5.2.6 Executable and non-executable file security

(See 6.2.5)

Use an executable in an EDS source that, when used in an unrestricted computer, would cause an automatic action.

- For REDS, one by one, attach a device to the connection points for REDS, which are accessible by the operator without using a tool or key, or insert a media into the REDS (disc drives, etc.) and confirm by observation that the executable file is not automatically executed.
- For network sources, if applicable, make executables available in the network source which is available to the EUT and confirm by observation that the executable file is not automatically executed.

If the EUT provides manual execution of any type of files from EDS, confirm by analytical evaluation that manual execution is only possible for files which have past source authentication and integrity check, for example by digital signatures or special keys.

If the EUT provides the possibility to boot and run from EDS in the event of catastrophic equipment failure, confirm by analytical evaluation that this is possible only for cryptographically authenticated executables.

If the EUT provides execution of executables during normal operation, use the list of such executables provided by the manufacturer and confirm by observation that either there is no recognizable effect on normal operation or that the EUT requested confirmation from the user to execute an executable.

Confirm by analytical evaluation that the equipment validates the syntax, length and content of any non-executable input data that is received from EDS sources.

Confirm by analytical evaluation that the equipment employs cryptographic integrity protection to recognize changes to information from EDS.

10.5.2.7 Recording of device management activities

(See 6.2.6)

Use manufacturer's documentation to locate places of recording of the device management activity and confirm by inspection of manufacturer's documentation that device management activity events are recorded either locally or are sent to an external device for recording.

View recorded device management activity events and confirm by observation that the events are timestamped.

If the equipment records device management events locally, confirm by analytical evaluation that the event recording(s) can store at least the last 100 events.

If the equipment sends device management activity events to an external device confirm by analytical evaluation that this transfer does either not contain any sensitive information, or that sensitive information is protected appropriately and that the recording capacity is at least the last 100 events and that it is possible to view the recorded events and that the events are timestamped.

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 (either using multicast 239.192.0.254 port 514 or UDP unicast) 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 registered 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 ring 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 ring 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 an 8 character long password, RSA keys, or another appropriate method.

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.

Confirm by inspection of the operator's manual that it includes a warning that all traffic in the cyber secure network is controlled by the 460-Switches and 460-Forwarders and that the cyber security of the whole network and all connected equipment may be compromised by any adding, removing, replacing or changing configuration of any equipment by other actors than the system integrator or manufacturer.

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.

10.6.3.6 Onboard software maintenance

10.6.3.6.1 General

(See 6.5.1)

If the equipment provides means for software maintenance, follow the procedure described in the operator's manual to perform initial steps prior to any software of configuration change to save the current state.

Confirm by analytic evaluation that software maintenance is only possible for the 3 cases described:

– authorized persons local to the equipment, in maintenance mode;
– the crew in normal operation, where semi-automated means are provided;
– authorized persons remote from the equipment in maintenance mode for remote access.

10.6.3.6.2 Roll back to previous working configuration

(See 6.5.2)

Follow the procedure described in the operator's manual to perform roll back and confirm by observation that it is possible to roll back to a working configuration.

After completion of roll back confirm by observation that EUT works as intended.

10.6.3.6.3 Software maintenance in maintenance mode

(See 6.5.3)

If the equipment provides a means to perform software maintenance in maintenance mode;

1) refer to manufacturer's documentation and confirm that the means to update the software in maintenance mode is described in the installation manual;
2) confirm by analytical evaluation that it is not possible to carry out the described software update procedure in normal operation;
3) refer to manufacturer's documentation and confirm that any limitations on application of the update that might affect normal operation of the equipment are clearly described.

10.6.3.6.4 Semi-automatic software maintenance by the crew onboard the vessel

(See 6.5.4)

Refer to the operator's manual and confirm by inspection that it contains instructions for software maintenance.

Confirm by analytical evaluation that only files with correct source authentication and integrity check are accepted for software maintenance (see 6.2.5).

Follow the procedure described in the operator's manual and confirm by observation that the EUT requires both of the following before the update is initiated:

– successful user authentication; and
– user confirmation to initiate the software update.

Confirm by observation that the identity used above cannot be used to access maintenance mode.

Confirm by observation that a software maintenance which has impact and/or any limitations to the application(s) generates an indication to the operator and the software maintenance only starts after the equipment has requested and received positive user confirmation from the operator prior to commencing the software maintenance.

Use a manufacturer provided test data set which will prevent software maintenance from successfully completing and confirm by observation that the software maintenance notifies the user that it was unsuccessful.

Use the manufacturer provided test data set and follow the procedure described in the operator's manual to perform a software maintenance. After completion confirm by observation that EUT works as intended. Then perform power off and power on. Perform roll back (see 10.6.3.6.2).

If the EUT provides the means to inform the user about software maintenance that is ready to install:

a) confirm by observation that it does not obscure or prevent normal functionality of the EUT;

b) if provided, confirm by observation that it is possible to initiate the procedure of software maintenance; it is still necessary to obtain the authenticated user's consent before initiation of any software maintenance, even if it has previously been delayed or scheduled for a different time;

c) confirm by observation that it is possible to acknowledge the information without initiation of the software maintenance;

d) if provided, confirm by observation that the repeated reminder complies with requirements from a) to c).

10.6.3.6.5 Remote software maintenance

(See 6.5.5)

Refer to the operator's manual and confirm by inspection that it contains instructions for remote software maintenance.

Confirm by observation that commencing of remote software maintenance begin only after enabled by successfully authenticated user onboard.

Confirm by observation that remote software maintenance which has impact and/or any limitations to the application(s) generates an indication to the operator and the remote software maintenance only starts after the equipment has requested and received positive user confirmation from the operator prior to commencing the remote software maintenance.

Confirm by analytical evaluation that only files with correct source authentication and integrity check are accepted for software maintenance, see 6.2.5.

Use the manufacturer provided test data set and follow the procedure described in the operator's manual to perform remote software maintenance. After completion confirm by observation that EUT works as intended. Then perform power off and power on. Perform roll back, see 10.6.3.6.2.

Use the manufacturer provided test data set and follow the procedure described in the operator's manual to perform remote software maintenance. Use the means provided for the onboard user to terminate the remote software maintenance. If instructed by the EUT, perform roll back, see 10.6.3.6.2, otherwise, confirm by observation that EUT works as intended.

Use the manufacturer provided test data set which will prevent remote software maintenance from successfully completing and confirm by observation that the remote software maintenance notifies the user that it was unsuccessful. If instructed by the EUT, perform roll back, see 10.6.3.6.2, otherwise, confirm by observation that EUT works as intended.

10.6.3.7 Secure software lifecycle management

(See 6.6)

Software development lifecycle management is part of secure software maintenance. The requirements related to onboard software maintenance part are given in 6.5.

Where applicable, confirm by inspection of documented evidence that there is a process for software development lifecycle management, e.g. software testing, version control, software/firmware upgrade procedures.

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 observation that the information is reported at least either by syslog (unsolicited sending, either using multicast 239.192.0.254 port 514 or UDP unicast) 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, either using multicast 239.192.0.254 port 514 or UDP unicast) 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 arrangements 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 through 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 (either using multicast 239.192.0.254 port 514 or UDP unicast) 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 an 8 character long password, RSA keys, or another appropriate method.

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 observation 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, either using multicast 239.192.0.254 port 514 or UDP unicast) 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, either using multicast 239.192.0.254 port 514 or UDP unicast) 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 for the 460-Network interfaces.

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 an 8 character long password, RSA keys, or another appropriate method.

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 permitted via a 460-Gateway or a 460-Wireless gateway and that a direct connection can only be established by 460-Gateway or 460-Wireless gateway and can only be activated from within the 460-Network.

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

Confirm by observation that it is possible to terminate the VPN tunnel or equivalent secure connection at any time.

Confirm by inspection of operator's manual that it includes instruction on how the direct connection using VPN tunnel or equivalent secure connection is established and terminated.

Confirm by analytic evaluation that both endpoints of the VPN tunnel are successfully authenticated before the VPN tunnel is established.

Confirm by analytic evaluation that the VPN tunnel provides confidentiality and integrity for all traffic passing through the VPN tunnel using a secure encryption algorithm.

Confirm by inspection of the documented evidence that the encryption algorithm used for VPN has a security strength of at least 128 bits.

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 in accordance with the manufacturer's instructions between a 460-Network and an uncontrolled network. Using a network scanner with port scan function, set it to scan the entire address range for the 460-Network and uncontrolled network. Use packet capture software running in promiscuous mode and confirm by analytical evaluation that packets do not pass through the EUT from the uncontrolled network to the 460-Network and vice-versa as follows:

- port scan UDP and TCP test for all ports 1-65535 to the internal address range of the 460-Network;
- port scan UDP and TCP test for all ports 1-65535 to the address range of the uncontrolled network.

Example test:

Using the Nmap®[4] network scanning tool with an address range for a 460-Network of 192.168.22.0/24 and for an uncontrolled network of 10.100.100.0/24.

- Port scan UDP and TCP test to the internal address range of the 460-Network:

  complete a ping test with TCP port scan with the command "nmap -p 1-65535 -sV -sS -T4 192.168.22.0/24";

  complete a ping test with UDP port scan with the command "nmap -p 1-65535 -sV -sU -T4 192.168.22.0/24".
- Port scan UDP and TCP test to the address range of the uncontrolled network;

  complete a ping test with TCP port scan with the command "nmap -p 1-65535 -sV -sS -T4 10.100.100.0/24";

  complete a ping test with UDP port scan with the command "nmap -p 1-65535 -sV -sU -T4 10.100.100.0/24".

4 Nmap® ("Network Mapper") is the trademark of a product supplied by the Nmap Project, a free and open source utility for network discovery and security auditing (https://nmap.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 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 inspection of the documented evidence 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 services

(See 6.3.5.2)

Confirm by inspection of the manufacturer's documentation that an application service 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.

Where applicable IMO Performance Standards exist, confirm by inspection of documented evidence that the equipment complies with the applicable related technical standard which refer to applicable IMO Performance Standards.

Otherwise, confirm by inspection of manufacturer's documentation that the operator's manual describes effects of lack of input data and effects of inability of the equipment to continue its functionality and any appropriate action the operator may take on such cases.

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 6.3.3, 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 uses asymmetric and/or symmetric algorithms with a security strength of at least 128 bits.

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, any associated infrastructure and the environment in which it is installed prevents unauthorised devices from connecting to the controlled network through physical or wireless interfaces.

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

Confirm by inspection of the documented evidence that the nodes and infrastructure in the controlled network provides a means to prevent transfer or execution of potentially malicious content from REDS.

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 provides a 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 the 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 (using multicast 239.192.0.254 port 514 and UDP unicast) or a combination of both for the following functionality:

a) generate cautions when the observed network load exceeds the 90 % limit or a lower limit as set in the EUT, 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 90 % limit or a lower limit as set in the EUT, 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 and intended for redundancy monitoring.

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 (using multicast 239.192.0.254 port 514 and UDP unicast) 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 (using multicast 239.192.0.254 port 514 and UDP unicast) 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", 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" 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" 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 after the internal processing time the EUT generates a caution.

Confirm by observation that the cautions comply with the requirements.

Confirm by observation that after resolving the SFI collision the caution is removed.

10.11.5 Syslog recording function

(See 8.2.5)

Set a simulation arrangement to cause syslog (either using multicast 239.192.0.254 port 514 or UDP unicast) messages. Confirm by observation that the network monitoring function provides recording and internal or external possibility to view the syslog information from the 460-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways in 460-Network.

Confirm by inspection of the documented evidence that the syslog has a capability to store messages for at least the last 90 days or last 20 000 messages, whichever is smaller.

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 62923-1.

In order to test the communication and presentation of the alerts, refer to the manufacturer's documentation to identify at least one of the available warnings, which may be chosen at random, and two 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 with the communication requirements of IEC 62923-1 and IEC 62923-2;
- 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 5 min.

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 two 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 two 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 two 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, 10.5, 10.6, 10.7, 10.8 and 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[5]) 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.

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;

---

5 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.

- 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 ring 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 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 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.

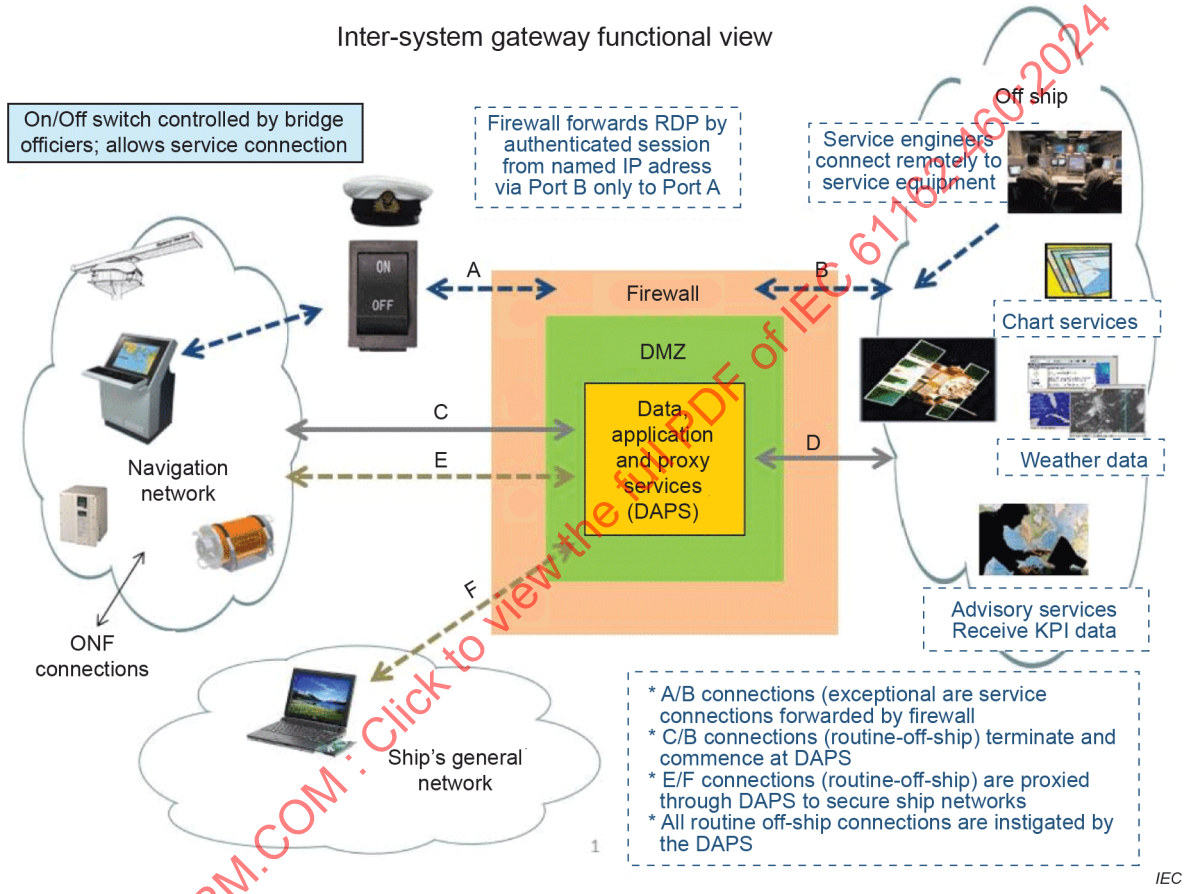

Figure A.1 – Usage model for communication between a IEC 61162-460 network and shore networks

A.2 Routine off-ship

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