IEC 61162-460

Edition 1.0 2015-08

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 61162-460:2015-08(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

IEC 61162-460

Edition 1.0 2015-08

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 978-2-8322-2850-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

FOREWORD

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

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

The text of this standard is based on the following documents:

FDIS	Report on voting
80/764/FDIS	80/769/RVD

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

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

This International Standard is to be used in conjunction with IEC 61162-450:2011.

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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

A bilingual version of this publication may be issued at a later date.

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

1 Scope

This part of IEC 61162 is an add-on to the IEC 61162-450 standard where higher safety and security standards are needed, e.g. due to higher exposure to external threats or to improve network integrity. This standard 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 standard also contains requirements for a redundant IEC 61162-460 compliant network.

This standard extends the informative guidance given in Annex D of IEC 61162-450:2011. It does not introduce new application level protocol requirements to those that are defined in IEC 61162-450.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 61162-450:2011, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talker and multiple listeners – Ethernet interconnection*

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

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

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

IEEE 802.1Q-2005, *Virtual Bridged Local Area Networks*

ISOC RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)*

ISOC RFC 1112, *Host Extensions for IP Multicasting*

ISOC RFC 2236, *Internet Group Management Protocol, Version 2*

ISOC RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

ISOC RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

ISOC RFC 5424, *The Syslog Protocol*

3 Terms and definitions

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

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

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

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

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

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 standard

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 standard

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 standard

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

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

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

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

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

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

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

3.14
caution
lowest priority of an alert

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

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

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

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

3.18
failure mode and effects analysis
FMEA
failure mode, effects and criticality analysis
FMECA
analytic method as specified in IEC 60812

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.

3.19
internet control message protocol
ICMP
protocol according to ISOC RFC 792

3.20
internet group management protocol
IGMP
protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and ISOC RFC 4604 (version 3)

3.21
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.

3.22
malware
malicious code
software used or created to disrupt computer operation

3.23
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).

3.24
maximum transmission rate
maximum number of bytes per second that can be transmitted by a network node or network infrastructure equipment

3.25
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)

3.26
network infrastructure components
devices that connect at least two nodes in a 460-Network and two different networks such as 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

3.27
nominal network capacity
network capacity as a bit 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.

3.28
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.

3.29
rapid spanning tree protocol
RSTP
protocol according to IEEE 802.1D

3.30
removable external data source
REDS
user removable non-network data source, including, but not limited to compact discs, memory sticks and Bluetooth[1] devices

3.31
ring topology
topology where each node is connected in series to two other nodes

3.32
RSA
public-key cryptosystem as described in IEEE 1363

3.33
safety
protection of networks from un-intentional threats such as system mal-functioning, mis-configuration and mis-operation

3.34
secure area
area with defined physical perimeters and barriers, with physical entry controls or access point protection or access point observation

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

3.35
security
protection of networks from intentional threats such as virus, worm, denial-of-service attacks, illicit access, etc.

3.36
simple network management protocol
SNMP
protocol according to ISOC RFC 3411

3.37
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

3.38
sniffing
monitoring and analysis of the network traffic

---

[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 standard and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

3.39
stream
combination of all flows from a device which use same protocol

3.40
syslog
protocol according to ISOC RFC 5424 which is used for an external logging in IEC 61162-450

3.41
system integrator
person or organisation responsible for the functionality of the integrated 460-network

3.42
threat
potential cause of an incident in computer security that may result in harm to the system

3.43
traffic
combination of all streams from a device

3.44
uncontrolled network
data network that is not an IEC 61162-450 compliant, IEC 61162-460 compliant or a controlled network

EXAMPLE: Wireless networks.

3.45
virtual local area network
VLAN
network according to IEEE 802.1Q

3.46
virtual private network
VPN
extension of a private network through encapsulated, encrypted, and authenticated links across shared or public networks

3.47
warning
announcing a situation or condition requiring attention but no immediate attention or action by the bridge team

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

3.48
wireless access point
wireless AP
device that connects wireless devices to wired devices through various wireless technologies such as Wi-Fi, Bluetooth

4 High-level requirements

4.1 Overview

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

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

4.2 Description

Figure 1 shows a network implementing the requirements of this standard on different parts and components of the network. The grey symbols represent equipment specified in this standard. The pentagons represent logical software functions specified in this standard.

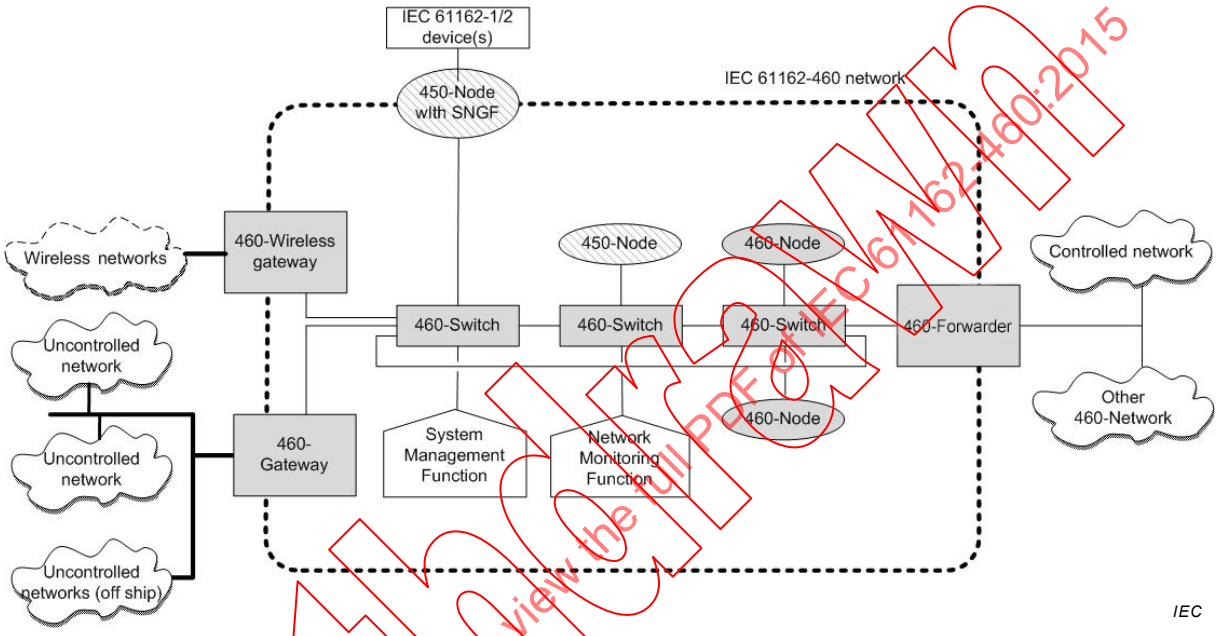

Figure 1 – Functional overview of IEC 61162-460 requirement applications

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

4.3 General requirements

4.3.1 Equipment and system requirements

(See 10.3)

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

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

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

All network nodes, network infrastructure components and cables shall satisfy the requirements in Clauses 4 and 5 of IEC 61162-450:2011.

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

4.3.2 Physical composition requirements

(See 10.12.3.1)

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

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

4.3.3 Logical composition requirements

(See 10.12.3.1)

A 460-Network shall also include the following logical system function components which are located at all nodes in a 460-Network:

- network monitoring function, 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, a SF or an ONF compliant with the requirements in 4.5.2.

4.4 Physical component requirements

4.4.1 450-Node

(See 10.4)

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

- no connection to external networks or REDS;
- syslog implemented as defined IEC 61162-450:2011, 4.3.3.2;
- data output bandwidth documented by the manufacturer as described in 6.2.2.1;
- implemented ONF services if provided specified by the manufacturer including the necessary protocol parameters, for instance for IP address and UDP/TCP 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 UDP/TCP port number received from an external controlled network shall be processed and checked by application level software in the 460-Node;

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

  - or if a connection with the controlled network is used to forward unmodified datagrams between the 460-Network and controlled networks or other 460-Networks, then this forwarding shall be handled by a 460-Forwarder;
- support for REDS as specified in 6.2.3;
- direct connection with uncontrolled networks as specified in 6.3.4;
- VLAN compatibility as specified in 5.1;
- implemented ONF services specified by the manufacturer including the necessary protocol parameters, for instance for IP address and UDP/TCP port number.

4.4.3 460-Switch

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

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

4.4.4 460-Forwarder

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

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

4.4.5 460-Gateway and 460-Wireless gateway

Connections to uncontrolled networks shall be protected by a gateway fulfilling the requirements for a 460-Gateway as specified in 6.3.5 or a 460-Wireless gateway as specified in 6.3.6. The following functions shall be implemented in a 460-Gateway and 460-Wireless gateway:

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

4.5 Logical component requirements

4.5.1 Network monitoring function

The network monitoring function shall perform the following functions:

- network load as specified in 8.2.2;
- network redundancy as specified in 8.2.3;
- network topology as specified in 8.2.4.

4.5.2 System management function

(See 10.12.2)

The system management function shall perform the following functions:

- maintain all network infrastructure configuration information and be able to restore this to the equipment when requested. The management function shall maintain a history of at least the previous configuration;
- functionality to save and to restore configuration information either automatically or manually from 460-Switches, 460-Forwarders, 460-Gateways and 460-Wireless gateways;
- functionality to change the infrastructure configuration.

NOTE This function is necessary to allow exchange of equipment with new MAC addresses as, e.g. 460-Switches which only allow a known MAC to be connected to a specific port.

The system management function shall be redundantly available.

4.6 System documentation requirements

(See 10.12.3.1)

A system integrator of a 460-Network shall provide documentation of the network structure.

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

See also 5.4.

4.7 Secure area requirements

(See 10.12.3.1)

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

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

5 Network traffic management requirements

5.1 460-Node requirements

(See 10.5.1)

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

- all traffic shall be specified as one of the IEC 61162-450 compliant data types for example IEC 61162-1 sentence transmission, binary image 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;
- device behaviour shall be specified by the manufacturer when its maximum input data rate is exceeded;
- only data specified for the node shall be processed by the node;
- devices shall continue normal operation with an input loss rate of packets up to 0,1 % for time period of 10 min.

If VLAN is provided, VLAN protocol version IEEE 802.1Q:2005 shall be supported. All VLAN traffic shall be included in the maximum transmission rate.

NOTE 2 For example VLAN is used to create a separate segment.

5.2 460-Switch requirements

5.2.1 Resource allocation

(See 10.6.1)

The following are required for resource allocation:

- means to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and TCP or UDP port number;
- means to allocate network bandwidth resource for each registered stream;
- all incoming and outgoing traffic shall be registered;
- all traffic not registered shall be prohibited;
- the amount of bandwidth allocated at a 460-Switch shall be more than the sum of all normal traffic volumes of each traffic class allocated to the network connected to the switch;
- the total amount of traffic per interface to a 450-Node and 460-Node shall be limited to the network design value of that interface. The network design value shall be selectable between 0 % to 50 % of the capacity of the switch;
- if VLAN provided, a means to configure virtual networks (VLAN) per interface shall be provided;
- if VLAN provided, VLAN protocol version IEEE 802.1Q:2005 shall be supported.

5.2.2 Loop prevention

(See 10.6.2)

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

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

The following are the RSTP requirements if provided:

- RSTP protocol version IEEE 802.1D-2004 shall be supported;
- a 460-Switch shall provide a capability to enable RSTP in all interfaces.

5.3 460-Forwarder requirements

5.3.1 Traffic separation

(See 10.7.1)

The following are required for traffic separation:

- means to configure transmitting all or a subset of the traffic;
- means to configure for a maximum traffic flow;
- if VLAN provided, a means to configure virtual networks (VLAN) per each interface;
- if VLAN provided, VLAN protocol version IEEE 802.1Q:2005 shall be supported.

5.3.2 Resource allocation

(See 10.7.2)

The following are required for resource allocation:

- the 460-Forwarder shall have a capacity more than the summation of all traffic volumes of each traffic class allocated to the network connected to the switch;
- the 460-Forwarder shall be configurable for a maximum traffic flow;
- a means shall be provided to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and TCP or UDP port number;
- a means shall be provided to allocate network resource for all registered streams;
- a means shall be provided to allocate resource for each virtual network if provided.

5.3.3 Traffic prioritization

(See 10.7.3)

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

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

Table 1 – Traffic prioritization with CoS and DSCP

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

The following are required for traffic prioritisation at a 460-Forwarder:

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

5.4 System design requirements

5.4.1 Documentation

(See 10.12.3.2)

Documents shall be provided which include the following information:

- 460-Network traffic flow analysis and network topology information;
- documents that specify the total amount of network traffic 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;
- the prioritization of each traffic type at each 460-Forwarder.

See also 4.6.

5.4.2 Traffic

(See 10.12.3.3)

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

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

6 Security requirements

6.1 Security scenarios

6.1.1 Threat scenarios

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

6.1.2 Internal threats

The following are scenarios that can occur in 460-Networks:

- malware replication from other equipment in a 460-Network such as a notebook that is infected by the malware;
- infection from corrupted mass storage devices (e.g. USB flash drive) or removable media drives (CD/DVD) being used within the 460-Network, e.g. in connection with (authorised or unauthorised) maintenance and support;
- attacker installs a backdoor in one of the equipment and gets system privilege through it. Then he attacks other equipment;
- user deletes the system file or changes the configuration file by mistake (mis-operation);
- illicit access that prohibits the normal operation of equipment;
- false data generation that prohibits the normal operation of equipment;
- security threats in controlled networks which are easily propagated into 460-Networks;
- security threats in other 460-Networks which are easily propagated into 460-Networks;

- interruption of network service due to the heavy volume of broadcasting traffic and of ICMP and IGMP packets.

Requirements for security against internal threats are described in 6.2.

6.1.3 External threats

The following are scenarios that are caused from external networks:

- threats from un-secure wireless networks;
- a malware in other shipborne networks infects equipment in the 460-Network;
- user in a shipborne network logs in remotely to equipment in a 460-Network, and deletes an important file or changes the configuration by mistake (mis-operation);
- shipborne equipment has installed a backdoor that is used as an attack agent. Direct attack to equipment through the network infrastructure such as switch or router;
- scanning attack. Attacker finds a port for attack by scanning the ports first. If found, it scans the service with the port. For example, when port number 80 is open for the web service, the attacker collects the information of web server type and version;
- in-direct attack to the 460-Network via uncontrolled networks such as another shipborne network;
- data sniffing and modification attack during the communication with external equipment and systems. When equipment in a 460-Network communicates with off-ship network systems, the attack extracts and modifies data by sniffing. For example, the navigational route information may be exposed to and be modified by pirates and terrorists;
- incoming excessive data traffic to 460-Networks and protocol features attack including SYN flooding attack.

Requirements for security against external threats are described in 6.3.

6.2 Internal security requirements

6.2.1 General

(See 10.5.1, 10.6.3.1, 10.7.4.1)

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

All VLAN tunnelling protocol shall be disabled in a 460-Node, 460-Switch and 460-Forwarder.

6.2.2 Denial of service protection

6.2.2.1 460-Node

(See 10.5.2.2)

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

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

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

(See 10.6.3.2, 10.7.4.2, 10.8.1)

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

6.2.3 REDS security

(See 10.5.2.3)

6.2.3.1 Physical protection

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

6.2.3.2 Operational protection

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

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

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

6.2.3.3 Executable program file verification

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

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

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

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

6.2.3.4 Non-executable data verification

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

6.2.4 Access control

6.2.4.1 Device access control

(See 10.5.2.4, 10.6.3.3, 10.7.4.3, 10.8.2)

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

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

- a user authentication mechanism shall be provided before changing the device settings. Some examples of authentication includes passwords and key cards;
- if a password is required at login, it shall be provided with at least 8 characters. Longer passwords and other authentication tokens like RSA keys, etc. may be supported where possible;

- the operator's manual shall include guidance such as: passwords should not contain the user name or parts of the user's full name, such as his first name, company name, product name, etc. Dictionary words should not be used. Random and meaningless passwords should be used;
- passwords shall use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and special characters.

6.2.4.2 Network access control

(See 10.6.3.4, 10.7.4.4)

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

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

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

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

6.3 External security requirements

6.3.1 Overview

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

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

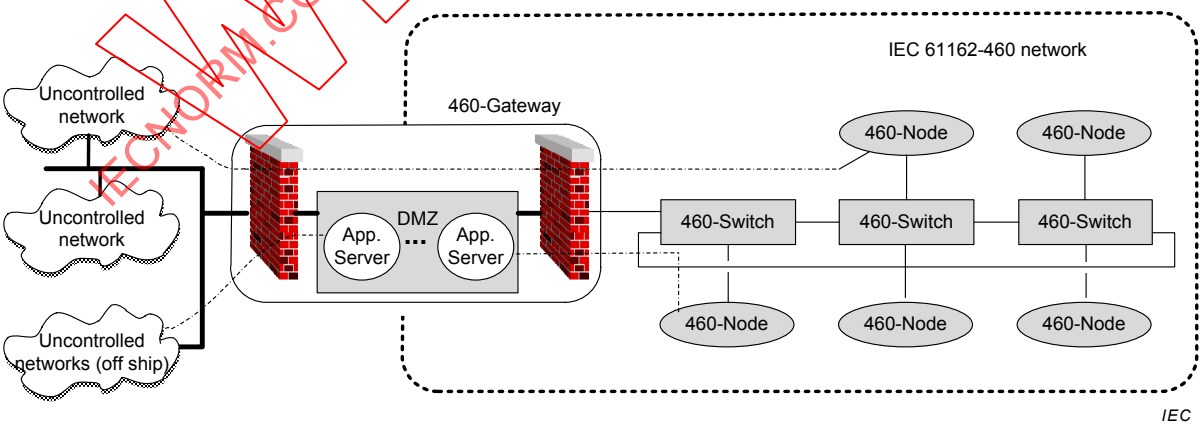

Figure 2 – 460-Network with 460-Gateway

6.3.2 Firewalls

6.3.2.1 External firewall

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

6.3.2.2 Internal firewall

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

6.3.2.3 Direct communication

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

6.3.3 Communication security

(See 10.8.3)

All connections between uncontrolled networks and a 460-Network shall use VPN through a 460-Gateway or 460-Wireless gateway. All data exchanged with an uncontrolled network shall be encrypted to protect from security attacks.

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

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

6.3.4 460-Node

(See 10.5.2.5)

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

- by manufacturing default, direct connection from an uncontrolled network shall be set to “not allowed”;
- the direct connection from an uncontrolled network shall only be activated by an operator from a 460-Node. It shall be protected from activation remotely via an external network;
- a 460-Node shall have a permanent indication when direct connection with an uncontrolled network is activated;
- a caution shall be generated after a pre-defined time period;
- the caution may be replaced with a warning after another pre-defined time period;
- all connections between uncontrolled networks and a 460-Node shall satisfy external communication security requirements (see 6.3.3).

6.3.5 460-Gateway

6.3.5.1 Firewall

(See 10.8.4)

The following are requirements for a 460-Gateway:

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

  NOTE Indication may be based on mechanical position, lamp, display, etc.
- a 460-Gateway shall provide a list of all activated direct connections between 460–Networks and uncontrolled networks. This list shall be recorded by the gateway or an external device including changes over the past 12 months. Means to view the list shall be provided. At least the following information, if available, shall be recorded for each activated direct connection: source IP address, destination IP address, starting time and end time of the connection, protocol, and TCP port number;
- the direct connection with a 460-Node from an uncontrolled network shall only be activated by an operation on the installation site or the 460-Network side of the firewall. It shall not be 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 time period of 10 min of no traffic on the connection.

6.3.5.2 Application server

(See 10.8.5)

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

The application server shall provide an application level authentication mechanism such as password to client from uncontrolled networks.

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

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

6.3.5.3 Interoperable access to file storage of DMZ

(See 10.8.6)

Means may be provided to download/upload files between the DMZ and uncontrolled networks or a 460-Network in order to access the file storage within the DMZ. If access to the file

storage within the DMZ is provided, then it shall implement a protocol such as SMB networking protocol (for example Samba [2]) or SFTP (Secure Shell (SSH) File Transfer Protocol).

6.3.6 460-Wireless gateway

(See 10.9.2)

The following are requirements for a 460-Wireless gateway:

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

6.4 Additional security issues

(See 10.6.3.5, 10.7.4.5, 10.8.7)

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

- the configuration shall be retained following a switch off or power failure and the equipment shall return to the normal operation upon restoration of power;
- when changes are made to the configuration, the previous configuration shall be stored. Means shall be provided to revert to the previous configuration;
- installation instruction shall advise that physical access to 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway shall be restricted.

7 Redundancy requirements

7.1 General requirements

(See 10.12.3.9)

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, 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.

---

2 www.samba.org

Samba is the trademark of a product supplied by Samba Organization.

This information is given for the convenience of users of this standard and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

The 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 standard.

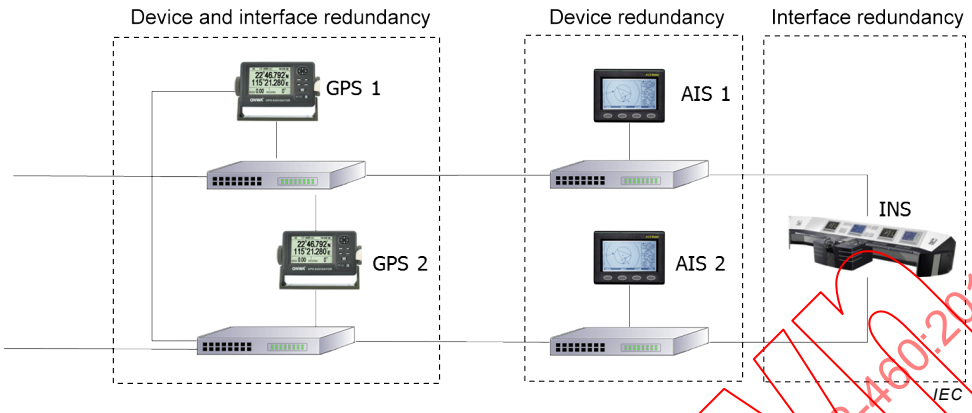

Figure 3 – An example of redundancy

7.1.2 Interface redundancy

Interface redundancy means that there are more than one IEC 61162-450 interfaces 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.

- 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 1 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 2 The implementation of interface redundancy depends on the local area network (LAN) topology.

7.1.3 Device redundancy

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

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

7.2 460-Node requirements

(See 10.5.3)

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

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

Documentation shall be provided describing the redundancy capability.

7.3 460-Switch requirements

(See 10.5.3)

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

7.4 460-Forwarder requirements

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

7.5 460-Gateway and 460-Wireless gateway requirements

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

7.6 Network monitoring function requirements

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

7.7 System design requirements

(See 10.12.3.9)

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

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

8 Network monitoring requirements

8.1 Network status monitoring

8.1.1 460-Network

The configuration of the 460-Network and the traffic flows shall be reported and monitored as described in 8.1.2 to 8.1.5.

8.1.2 460-Node

(See 10.5.4)

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

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

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

8.1.3 460-Switch

(See 10.6.4)

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

- interface information;
- 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 request message (see 8.2.4). Also, the information shall be logged whenever changes in the configuration occur such as changes of a neighbour MAC address. The configuration information shall not be reported more often than once per minute.

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

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

8.1.4 460-Forwarder

(See 10.7.5)

The 460-Forwarder shall provide the configuration information which is required for the switch (see 8.1.3) periodically each 30 min using SNMP. If VLAN is provided, current VLAN configuration information shall be provided. Also, the information shall be reported whenever changes have been made. The configuration information shall not be reported more often than once per minute.

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

8.1.5 460-Gateway and 460-Wireless gateway

(See 10.8.8, 10.9.3)

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

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

8.2 Network monitoring function

8.2.1 General

(See 10.11.1)

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

The network monitoring function shall provide either a local human machine interface (HMI) or an interface for the alerts (see 8.2.7).

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

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

- any alert from the network monitoring function;
- any event or reports from 460-Switches using SNMP.

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 of the maximum network load based on the manufacturer's declarations of total maximum traffic rates for all flows the system generates to the 460-Network.

The network monitoring function shall request SNMP responses from the 460-Switches as specified in 8.1.3 periodically every 30 s.

The network load monitoring function shall generate the following alerts.

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

8.2.3 Redundancy monitoring function

(See 10.11.3)

The system documentation shall include a list of data sources which are redundantly available either by interface redundancy (see 7.1.2) or device redundancy (see 7.1.3). For interface redundancy the list shall contain the MAC address, interface number and interface available in a 460-Switch. For device redundancy, the list shall contain the MAC address of each redundantly available device.

The network monitoring function shall request SNMP responses from the 460-Switches as specified in 8.1.3 periodically every 30 s.

The list shall include the following information:

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

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

Caution: Network redundancy lost for xxxx.

Where xxxx is a name of the data source.

8.2.4 Network topology monitoring function

(See 10.11.4)

System documentation shall include the list of accepted devices for a 460-Network with their MAC addresses.

Maintaining the network topology requires network topology monitoring and generating alerts based on detected additional devices not available in the list of accepted devices. The network monitoring function shall request network configuration information from the 460-Switches as specified in 8.1.3 using SNMP periodically every 30 min.

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

Caution: New device is detected in the network.

8.2.5 Syslog recording function

(See 10.11.5)

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

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

8.2.6 Redundancy of network monitoring function

(See 10.12.7.3)

The network monitoring function shall be redundantly available.

8.2.7 Alert management

8.2.7.1 Alerts and indication

(See 10.11.6.1)

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

8.2.7.2 Alert management interface

(See 10.11.6.2)

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

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

Alert management requires:

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

8.2.7.3 Unacknowledged warnings

(See 10.11.6.3)

An unacknowledged warning shall be:

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

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

8.2.7.4 Remote acknowledgments and silencing of alerts

(See 10.11.6.4)

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

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

9 Controlled network requirements

(See 10.10)

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

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

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

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

10 Methods of testing and required test results

10.1 Subject of tests

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

10.2 Test site

A network protocol analyser is required (for example wireshark[3]).

A simulator arrangement with the following characteristics is required:

- capable of transmitting and receiving IEC 61162-450 compliant data and non IEC 61162-450 compliant data;
- 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 non IEC 61162-450 compliant data (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.

3 www.wireshark.org

Wireshark is the trademark of a product supplied by the Wireshark organization.

This information is given for the convenience of users of this standard 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.

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

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

Guidance on testing is given in Annex C.

10.3 General requirements

(See 4.3.1)

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

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

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

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

10.4 450-Node

(See 4.4.1)

Confirm by observation that there is no connection to external networks or REDS.

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

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

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

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.

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

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

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

Confirm by analytical evaluation of the 460-Node that it discards all other received data except data it supports.

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

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

10.5.2 Security

10.5.2.1 Security general

(See 6.2.1)

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

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

10.5.2.2 Denial of service behaviour

(See 6.2.2.1)

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

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

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

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

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

10.5.2.3 Security for REDS

(See 6.2.3)

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

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

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

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

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

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

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

10.5.2.4 Access control to configuration setup

(See 6.2.4.1)

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

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

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

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

10.5.2.5 Direct access to uncontrolled network

(See 6.3.4)

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

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

For each configured direct data exchange, confirm by analytical evaluation that only the operator of the 460-Node can activate it.

For each direct data exchange confirm by observation that:

- there is an permanent indication when direct data exchange is active;
- a caution is created after a pre-defined time period;
- the caution is replaced by a warning after another pre-defined time period.

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

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

10.5.3 Redundancy

(See 7.2, 7.3)

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

10.5.4 Monitoring

(See 8.1.2)

Confirm by observation that monitoring information to syslog is provided by the EUT periodically each 30 min and not more often than once per 1 min 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 interface identifier, the MAC address or IP address, protocol number and TCP or UDP port number.

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

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

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

Use a simulation arrangement to interface two 460-Nodes to the EUT and set the nodes to communicate with each other using the set maximum traffic. Confirm by analytical evaluation that all traffic pass 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 VLAN is provided, a means is provided to configure virtual networks (VLAN) for each interface.

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

10.6.2 Loop prevention

(See 5.2.2)

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

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

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

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

10.6.3 Security

10.6.3.1 Security general

(See 6.2.1)

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

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

10.6.3.2 Denial of service behaviour

(See 6.2.2.2)

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

10.6.3.3 Access control to configuration setup

(See 6.2.4.1)

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

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

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

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

10.6.3.4 Access control for network

(See 6.2.4.2)

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

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

10.6.3.5 Additional security issues

(See 6.4)

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

Confirm by analytical evaluation that means are provided to revert to the previous stored configuration.

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

10.6.4 Monitoring

(See 8.1.3)

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

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

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

Confirm by observation that the interface input and output link utilization in percent (average over 5 min) is provided by the EUT. Confirm by observation that the network status information is sent through SNMP periodically every 30 s by the EUT. Confirm by observation that the information is reported whenever significant changes (more than 10 % difference with the previous information in a 0 % to 100 % scale of network capacity) have been made. Confirm by observation that the status information is never reported more often than once per 3 s.

10.7 460-Forwarder

10.7.1 Traffic separation

(See 5.3.1)

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

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

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

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

10.7.2 Resource allocation

(See 5.3.2)

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

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

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

Confirm by inspection of the manufacturer's documentation that a means is provided to configure a stream or a network flow that is identified by the combination of interface identifier, the MAC address or IP address, protocol number and TCP or UDP port number. Confirm by observation that means are provided to allocate a network resource for all registered streams.

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

10.7.3 Traffic prioritisation

(See 5.3.3)

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

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

Create increased traffic higher than 50 % of the set maximum for 30 s and return to the set maximum. Confirm by analytical evaluation that there was a drop in lower priority traffic until the traffic is below 50 % of the set maximum.

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 after which also a part of highest priority traffic is dropped.

Confirm by analytical evaluation that the use of dropping is reported by syslog for each period of 30 s during which the dropping has been used.

10.7.4 Security

10.7.4.1 Security in general

(See 6.2.1)

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

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

10.7.4.2 Denial of service behaviour

(See 6.2.2.2)

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

10.7.4.3 Access control to configuration setup

(See 6.2.4.1)

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

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

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

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

10.7.4.4 Access control for network

(See 6.2.4.2)

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

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

10.7.4.5 Additional security

(See 6.4)

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

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

Confirm by inspection of the manufacturer's documentation that guidance is given to install the EUT in 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 neighbour MAC address per interface;
- the change of neighbour MAC address.

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

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

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

10.8 460-Gateway

10.8.1 Denial of service behaviour

(See 6.2.2.2)

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

10.8.2 Access control to configuration setup

(See 6.2.4.1)

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

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

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

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

10.8.3 Communication security

(See 6.3.3)

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

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

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

10.8.4 Firewall

(See 6.3.5.1)

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

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

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

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

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

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

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

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

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

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

10.8.5 Application server

(See 6.3.5.2)

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

Confirm by analytical evaluation that L3 forwarding or routing is disabled.

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 to revert to the previous stored configuration.

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

10.8.8 Monitoring

(See 8.1.5)

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

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

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

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

10.9 460-Wireless gateway

10.9.1 General

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

10.9.2 Security

(See 6.3.6)

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

Confirm by observation that the forwarding function is not allowed.

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

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

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

Confirm by observation that all connections to wireless AP are established only with authentication.

10.9.3 Monitoring

(See 8.1.5)

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

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

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

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

10.10 Controlled network

(See Clause 9)

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

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

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

10.11 Network monitoring function

10.11.1 General

(See 8.2.1)

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. Confirm by observation that all alerts, events and reports from 460-Switches are recorded in the EUT.

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

10.11.2 Network load monitoring function

(See 8.2.2)

Confirm by observation that the system documentation includes an analysis of the maximum network load.

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

Confirm by observation that the EUT generates cautions when the observed network load exceeds the 80 % limit of its maximum network capacity for a period of 30 s more than 3 times within a period of 10 min.

Confirm by observation that the EUT generates alerts when the observed network load has exceeded the 80 % limit of the maximum network capacity for a period of 30 s more than 10 times within a period of 10 min.

10.11.3 Redundancy monitoring function

(See 8.2.3)

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

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

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

10.11.4 Network topology monitoring function

(See 8.2.4)

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

Use the simulation arrangement and confirm by observation that the EUT requests the network topology information from all 460-Switches using SNMP request/response messages periodically every 30 min.

Use the simulation arrangement and confirm by observation that the EUT generates cautions when a MAC address, which is not included in the list of accepted devices, has been found.

10.11.5 Syslog recording function

(See 8.2.5)

Confirm by observation that the network monitoring function provides recording and viewing of the syslog information from the 450-Nodes, 460-Nodes, 460-Gateways and 460-Wireless gateways in 460-Network.

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

10.11.6 Alert management

10.11.6.1 Alerts and indications

(See 8.2.7.1)

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

10.11.6.2 Alert management interface

(See 8.2.7.2)

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

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

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

10.11.6.3 Unacknowledged warnings

(See 8.2.7.3)

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

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

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

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

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

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

10.11.6.4 Remote acknowledgements and silencing of alerts

(See 8.2.7.4)

Create 2 alerts, at least one of category B. Confirm by observation that ALF, ALC and HBT 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 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 sentences report correctly the new state of the alerts.

10.12 System level

10.12.1 General

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

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

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

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

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

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

The test site requirements are a network protocol analyser (for example wireshark[4]) 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,
- injecting DoS attack into the 460-Switches.

4 www.wireshark.org

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

Confirm by observation 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;
- the prioritization of each traffic type at each 460-Forwarder;
- an analysis of the maximum network load;
- a list of data sources which are redundantly available;
- a list of accepted devices.

10.12.3.3 Network traffic design

(See 5.4.2)

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

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

observation that the average load of all traffic in a 460-Network does not exceed 95 % of the nominal network capacity planned over a period of 1 s and does not exceed 80 % of the nominal network capacity planned over a period of 10 s.

10.12.3.4 Loop prevention

Use a network design document and select at least two 460-Switches for loop topology connect with at least one 460-Node at each switch for example using unicast. Confirm by analytical evaluation that the switch does not duplicate data at switches.

10.12.3.5 Resource allocation

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

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

10.12.3.6 Traffic prioritisation

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

10.12.3.7 Denial of service behaviour

Use a network design document and select three 460-Nodes to inject additional traffic flows up to line load for 1 h. 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 Redundancy

(See 7.1, 7.7)

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

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

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