IEC 61162-450

Edition 1.1 2016-03

CONSOLIDATED VERSION

colour inside

Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

IEC 61162-450:2011-06+AMD1:2016-03 CSV(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 It also gives information on projects, replaced and withdrawn publications.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 20 000 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
65 000 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 61162-450

Edition 1.1 2016-03

CONSOLIDATED VERSION

colour inside

Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 47.020.70

ISBN 978-2-8322-3289-7

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

IEC 61162-450

Edition 1.1 2016-03

REDLINE VERSION

colour inside

Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

IEC 61162-450:2011-06+AMD1:2016-03 CSV(en)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

FOREWORD

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

This Consolidated version of IEC 61162-450 bears the edition number 1.1. It consists of the first edition (2011-06) [documents 80/615/FDIS and 80/621/RVD] and its amendment 1 (2016-03) [documents 80/795/FDIS and 80/796/RVD]. The technical content is identical to the base edition and its amendment.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

International Standard IEC 61162-450 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems.

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

The committee has decided that the contents of the base publication and its amendment 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 450: Multiple talkers and multiple listeners – Ethernet interconnection

1 Scope

This part of IEC 61162 specifies interface requirements and methods of test for high speed communication between shipboard navigation and radiocommunication equipment as well as between such systems and other ship systems that need to communicate with navigation and radio-communication equipment. This part of IEC 61162 is based on the application of an appropriate suite of existing international standards to provide a framework for implementing data transfer between devices on a shipboard Ethernet network.

This standard provides a higher speed and higher capacity alternative to the IEC 61162-1 and IEC 61162-2 standards while retaining these standards' basic data format. This standard provides a higher data capacity than IEC 61162-3.

This standard specifies an Ethernet based bus type network where any listener may receive messages from any sender with the following properties.

- This standard includes provisions for multicast distribution of information formatted according to IEC 61162-1, for example position fixes and other measurements, as well as provisions for transmission of general data blocks (binary image), for example between radar and VDR.
- This standard is limited to protocols for equipment (Network nodes) connected to a single Ethernet network consisting only of OSI level one or two devices and cables (Network infrastructure).
- This standard provides requirements only for equipment interfaces. By specifying protocols for transmission of IEC 61162-1 sentences and general binary image data these requirements will guarantee interoperability between equipment implementing this standard as well as a certain level of safe behaviour of the equipment itself.
- This standard permits equipment using other protocols than those specified in this standard to share a network infrastructure provided that it is supplied with interfaces which satisfy the requirements described for ONF (see 4.6).
- This standard does not contain any system requirements other than the ones that can be inferred from the sum of individual equipment requirements. Thus, to ascertain system properties that cannot be derived from equipment requirements alone, additional analysis or standards will be required. In particular, this applies to requirements to maintain system functionality in the face of a single point failure in equipment or networks. Informative Annex D contains guidance on how to address such issues.

2 Normative references

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

IEC 60825-2, *Safety of laser products – Part 2: Safety of optical fibre communication systems (OFCS)*

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

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

IEC 61996-1, *Maritime navigation and radiocommunication equipment and systems – Shipborne voyage data recorder (VDR) – Part 1: Performance requirements, methods of testing and required test results*

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

ISOC RFC 768, *User Datagram Protocol, Standard STD0006*

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

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

ISOC RFC 826, *An ethernet Address Resolution Protocol*

ISOC RFC 1918, *Address Allocation for Private Internets, Best Current Practice BCP0005*

ISOC RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

ISOC RFC 5000, *Internet Official Protocol Standards, Standard 0001*

ISOC RFC 5227, *IPv4 Address Conflict Detection*

ISOC RFC 5424, *The Syslog Protocol*

NMEA 0183:2008, *Standard for interfacing marine electronic devices, Version 4.00*

NOTE The standards of the Internet Society (ISOC) are available on the IETF websites http://www.ietf.org. Later updates can be tracked at http://www.rfc-editor.org/rfcsearch.html

3 Terms and definitions

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

3.1
ASCII
printable 7 bit character encoded in one byte

3.2
binary image
data block without formatting known to this protocol, i.e., non IEC 61162-1 formatted data, that can be transmitted with the protocol defined in 7.3.

NOTE The term “binary image” is used to differentiate the general data transfer protocol (which may or may not be in ordinary text format) from the transmission of sentences that is always in 7 bit ASCII format.

3.3
byte
group of 8 bits treated as one unit; this corresponds to what is also sometimes called an octet

3.4
command-response pair
CRP
messages exchanged between parties that synchronize state changes on both sides through the exchange

NOTE 1 CRP are defined in Annex A.

NOTE 2 Both the command and the reply message may also be used as a sensor broadcast message in some cases. Thus, the implementation of the semantics of the message exchange is somewhat different between different users of the exchange.

3.5
datagram
one atomic UDP transmission unit on the Ethernet as defined in ISOC RFC 768 and as constrained elsewhere in this standard

3.6
Ethernet
a carrier sense, multiple access collision detect (CSMA/CD) local area network protocol standard as defined in IEEE 802.3 and later revisions and additions to IEEE 802

NOTE The types of Ethernet media that can be used for implementation of this standard are defined in Clause 5.

3.7
function block
specified functionality implemented by equipment

NOTE Equipment normally implements multiple function blocks. Requirements to equipment are the sum of requirements to the function blocks it implements. Function blocks are defined in Clause 4. Types of function blocks are System Function Block (SF), Other Network Function Block (ONF), Network Function Block (NF) and Serial to Network Gateway Function Block (SNGF).

3.8
internet assigned number authority
IANA
global coordination of the Domain Name Server (DNS) Root, IP addressing, and other Internet protocol resources, including UDP and TCP port numbers

NOTE The currently assigned numbers are listed in http://www.iana.org/assignments/port-numbers.

3.9
internet protocol
IP
used and defined in ISOC RFC 791 (and updates)

3.10
message
collection of one or more sentences that are grouped by mechanisms internal to the sentence, for instance by sequence numbers as in the TXT sentence, i.e. a stand alone sentence is a message

3.11
message type
classification of IEC 61162-1 sentence formatters into ~~SMB~~ SBM, MSM and CRP types

NOTE 1 ~~SMB~~ SBM, MSM and CRP types are defined in Annex A.

NOTE 2 This standard defines different requirements to the transmission of different message types.

3.12
multi-sentence messages
MSM
logical group of messages and/or sentences where the full meaning of the group is dependent on the receiver reading the full group

NOTE 1 Multi-sentence messages that are grouped together with a TAG construct is also a sentence group.

NOTE 2 MSM are defined in Annex A.

3.13
network
one physical Ethernet network with one Internet address space, consisting only of the network nodes, switches, cables and supporting equipment such as power supply units

3.14
network function block
NF
function block responsible for physical connectivity to the network and connectivity to the transport layer as described in 4.3

3.15
network infrastructure
the part of the Network that provides a transmission path between network nodes

NOTE The network nodes are not part of the network infrastructure.

3.16
network node
physical device connected to the network and which have an Internet address (also called an Internet host)

NOTE A network node will normally correspond to equipment as the latter term is used in this standard.

3.17
other network function block
ONF
function block that interfaces to the network, but which is not using the protocol definition in Clauses 5, 6 and 7 of this standard (for example real time streaming of Radar and CCTV image transfer, VDR sound transfer, etc.)

NOTE Requirements as defined in 4.6 ensure that an ONF can co-reside with SF network nodes and function blocks that make use of this standard's protocol.

3.18
sensor broadcast message
SBM
messages consisting of only one sentence

NOTE 1 SBM type messages are sent with a sufficiently high update rate to ensure that the receiver can maintain the correct status even in environments where some messages may be lost.

NOTE 2 SBM are defined in Annex A.

3.19
sentence
standard information carrying unit as defined in IEC 61162-1

3.20
sentence group
logical group of sentences (which may consist of only one) that need to be processed together to give full meaning to the information contained in the sentence(s)

NOTE 1 The grouping of sentences into sentence group is done by TAG block mechanisms. The sentences in a sentence group may or may not have the same formatter. A multi sentence message grouped by this mechanism is also a sentence group.

NOTE 2 This standard allows the explicit grouping of sentences by using coding in a datagram. This standard does not enforce any relationship between datagram and sentence group. Thus a datagram may contain more than one sentence group or a sentence group may be split over two or more datagrams.

3.21
serial to network gateway function block
SNGF
function block that enables transfer of sentences between the network and devices that are compliant with the IEC 61162-1 and IEC 61162-2 serial line interface

3.22
system function block
SF
function block, identified by a unique system function ID (SFI), that is the only function block that can send information in a datagram format as defined in clause 7

3.23
system function ID
SFI
parameter string as defined in 4.4.2

3.24
transmission group
a pair of a multicast address and a port number that are used by an SF to transmit sentences

NOTE The transmission groups are defined in Table 4 and Annex A defines default transmission groups for the SF.

3.25
transport annotate and group
TAG
formatted block of data, defined in NMEA 0183, that adds parameters to IEC 61162-1 sentences

NOTE Informative Annex B gives an overview of the TAG blocks used in this standard.

3.26
user datagram protocol
UDP
connection-less datagram protocol defined by ISOC RFC 768; it makes no provision for transport-layer acknowledgement of packets received

4 General network and equipment requirements

4.1 Network topology example

Figure 1 shows a possible IEC 61162-450 network topology consisting of one IP Local Area Network (LAN) and a number of different network nodes, each containing different function blocks. This diagram is informal and does not imply any requirements other than the ones defined in the following subclauses.

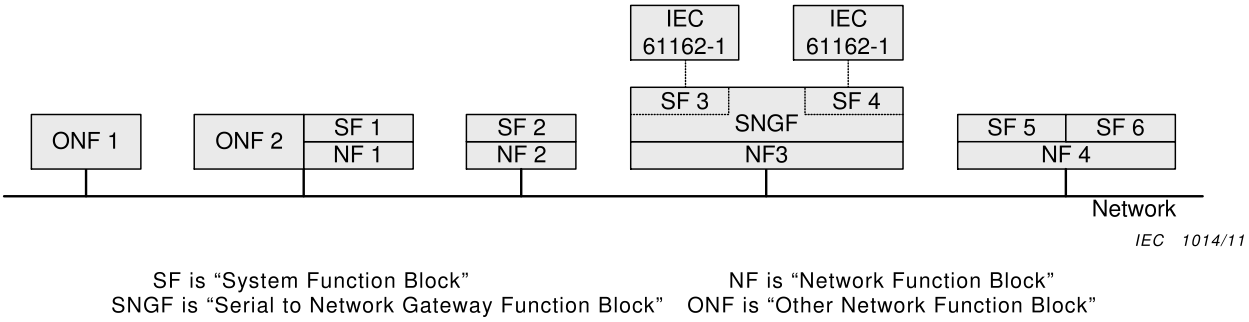

Figure 1 – Network topology example

Some examples of network nodes are (see Figure 1):

- a sensor, for example a GNSS receiver that is also a network node (SF2 and NF2).
- a device that sends or receives IEC 61162-450 compliant data (sentences and/or binary image) as well as other types of information onto the network, for example an ECDIS that can also load chart data from another device (SF1, ONF2 and NF1).
- two independent functions, such as a gyrocompass also approved as a rate of turn sensor that are implemented in one network node (SF5, SF6 and NF4).
- a system device function block represented by an IEC 61162-1 compliant equipment connected to a serial to network gateway function (SNGF). In this case, the SNGF will format outgoing sentences according to requirements in this standard (SF3, SF4, SNGF and NF3)
- a device that does not send or receive IEC 61162-450 compliant data (sentences and/or binary image), but which satisfies minimum requirements for compatible use of the same network (ONF1).

4.2 Basic requirements

4.2.1 Requirements for equipment to be connected to the network

(see 8.2.1)

The requirements for equipment connected to the network are as follows.

- All equipment connected to the network including network infrastructure equipment, shall satisfy the relevant physical and electrical requirements defined in 5.1.
- All equipment that implements one or more of SF and/or SNGF shall implement the NF. This equipment shall satisfy the requirements to the function blocks they implement as defined in 4.3 (NF), 4.4 (SF) and 4.5 (SNGF).
- All other equipment that is not network infrastructure equipment and that shares the network infrastructure shall comply with requirements to an ONF as defined in 4.6.
- Network infrastructure equipment, i.e., switches, shall satisfy requirements in 4.2.2.
- All equipment connected to a network shall satisfy the requirements of IEC 60945.

Any other equipment is not allowed to be connected to the network.

4.2.2 Additional requirements for network infrastructure equipment

(see 8.2.2)

The following requirements are included to avoid potential problems with certain network infrastructure equipment:

- routers and repeater hubs shall not be used to interconnect components of an IEC 61162-450 network;

- switches that are used to interconnect equipment compliant with IEC 61162-450 shall not implement multicast filtering techniques, such as IGMP snooping or CGMP.

NOTE 1 IGMP is Internet Group Management Protocol and CGMP is Cisco Group Management Protocol. If switches are capable of implementing multicast filtering techniques, then this functionality should be disabled.

NOTE 2 Routers are network infrastructure devices that can forward datagrams between networks. Repeater hubs are network infrastructure devices without internal storage that repeat incoming datagrams onto all outgoing connections. Switches are network infrastructure devices that based on forwarding tables can process, and forward *datagrams between nodes on the same network, using intermediate storage in the switch before retransmission.*

NOTE 3 Although multicast filtering techniques, such as IGMP snooping or CGMP, are not allowed to be activated, it is acceptable to manually configure individual ports of the switches to block unnecessary traffic flow (for example to isolate simple sensors from ECDIS and radar).

4.3 Network function (NF) requirements

4.3.1 General requirements

All equipment that implements a NF shall satisfy the requirements in Clauses 5 and 6.

4.3.2 Maximum data rate requirements

(see 8.3.1)

The manufacturer shall specify the maximum input rate under which the equipment can still perform all functions required by its performance standards.

Maximum input rate shall be specified as:

a) maximum number of datagrams per second received, intended for and processed by the equipment;

b) maximum number of datagrams per second received by but not intended for the equipment;

c) maximum number of datagrams per second received by, but not intended for, the equipment at 50 % of the maximum load for item a).

NOTE "Received by" means datagrams that are received on a transmission group that the equipment listens to. "Intended for" are datagrams that are processed by the equipment as part of its specified function.

The maximum data rates shall be the mean rate over a 10 s measurement period.

4.3.3 Error logging function

(see 8.3.2)

4.3.3.1 Internal logging

Means shall be provided in each NF to record errors that occur in the NF itself as well as SF and SNGF using it. Subclauses 4.5.2, 7.1.2, 7.2.5 and 7.3.9 give minimum requirements as to what shall be logged.

As a minimum, the manufacturer shall provide mechanisms by which error logs can be inspected by a human operator. It is allowed that the inspection is done through a simple network mechanism such as a terminal emulator, a datagram as defined in this standard or any other reasonable method.

The minimum requirements for the log are to count the number of each occurrence. The counter may reset itself by a manufacturer specified method.

4.3.3.2 External logging

A NF may be configured to support external logging, where non-trivial information is sent to a logging server. In this case a “syslog” message, as defined in ISOC RFC 5424, shall be used.

Syslog messages shall be formatted as ASCII text messages and sent as UDP packets on port 514 and the multicast address defined in Table 6. Error messages defined in this standard shall be reported through a simplified message as described in Table 1, where italicised words are place-holders for data explained in the right hand column. Other characters shall be transmitted as shown, including spaces.

Table 1 – Syslog message format

Element	Description
<pri>	The combined priority and facility code (number from 0 to 199 inclusive) enclosed in pointed brackets. For the errors defined in this standard, the value 131 shall be used (facility “local use 0” and priority “error condition”).
Version	The version code. The code 1 (one) shall be used for messages from this version of the standard.
Space	One space character.
Timestamp	Timestamp, containing date and time and optional UTC offset, in a valid format, for example 1985-04-12T23:20:50-03:00. The example shows date, followed by upper case “T”, then local time and finally offset from UTC (3 hours west – negative, east offsets shall be prefixed by a ‘+’. UTC offset can be abbreviated to a single upper case “Z”, without leading ‘-‘ or ‘+’). Alternatively, the timestamp field may be nil (‘-‘, a single dash character).
Space	One space character
Hostname	The host name of the network node, represented as the IP address in dotted decimal notation. Alternatively, this field may be nil (‘-‘, a single dash character).
Space	A space character
Appname	The application name. This shall be the string “450-“ followed by the configured SFI code if the error originates in the SF or SNGF, “NF” if the error originates from the network function block or “ONF” if it originates in the ONF function block.
Space	A space character
Procid	Normally, this field should be nil (‘-‘ a dash character). Other values as defined in the Syslog standard may be used.
Space	A space character
Msgid	For errors defined in this standard, this field shall be the error code as defined in Table 2.
Space	A space character
Structured	This field can be nil (‘-‘, a single dash character) or contain information as defined in ISOC RFC 5424.
Space	A space character
Msg	A free format message in ASCII format.

A ”syslog” packet shall not exceed 480 bytes and shall be sent as a single UDP datagram.

NOTE This standard does not specify requirements for equipment receiving syslog messages. This type of equipment would fall into the category of ONF. As the above specification is a subset of the full ISOC RFC 5424 specification, implementers of such equipment should refer to ISOC RFC 5424 and make sure that syslog messages from other ONF can be received and processed without problems.

To facilitate the use of the syslog protocol, the errors defined in this standard have been assigned a message identity as defined in Table 2.

Table 2 – Syslog error message codes

Message identity	Description	Sub-clause
101	SNGF buffer overflow	4.5.2
102	Datagram header error	7.1.2
103	TAG or sentence format error	7.2.5
104	Binary image error	7.3.9

Additional information can be given in the “Msg” field, if available.

4.4 System function (SF) requirements

4.4.1 General requirements

(see 8.4.1)

Equipment that implements an SF shall satisfy the following requirements:

- requirements in 6.2 shall be satisfied for all equipment implementing SF;
- requirements in 7.2 shall be satisfied for all equipment implementing IEC 61162-1 sentence transmitting or receiving function blocks;

  NOTE This also includes function blocks with the ability to send heartbeat (HBT) sentences.
- requirements in 7.3 shall be satisfied for equipment that implements an SF that can transmit or receive binary image data.

4.4.2 Assignment of unique system function ID (SFI)

(see 8.4.2)

The format of the SFI parameter string shall be “ccxxxx” where “cc” is two valid characters as defined in IEC 61162-1 and “xxxx” is four numeric characters.

An SF implementing the functionality of an equipment that has been given a talker mnemonic code in IEC 61162-1 shall use this talker mnemonic as the “cc” characters in the SFI.

NOTE Other SF may have their SFI string format defined in other standards or the manufacturer may have to choose a code. In the latter case, the already defined talker mnemonic codes should be avoided.

The numeric character string "xxxx" will be an instance number in the range "0000" to "9999" The numeric character string “9999” is reserved for an un-configured SF and shall not be used by any transmitting SF during normal operation. However, all receiving equipment shall accept the “9999” string.

During normal operation, the SFI parameter string shall be unique for all SF in an IEC 61162-450 network.

NOTE It is recommended that all SF on a ship, independent on whether they are residing on one common network or not, are given a ship unique SFI.

Means shall be provided by the manufacturer to configure the SFI for each SF (see 7.2.3.4).

4.4.3 Implementing configurable transmission groups

(see 8.4.3)

Each SF shall be assigned a single transmission group for all outgoing messages. The default for this transmission group is determined by the SFI as described in Annex A.

For each SF that the equipment implements, the manufacturer shall document the default transmission groups the SF listens to and what sentences it expects to receive on each group. The default transmission groups can be selected by the manufacturer from the list of groups in 6.2.2.

Means shall be provided to configure all transmission groups to another than the default. Only the transmission groups listed in 6.2.2 are allowed to be configured.

NOTE All transmission groups can be used for configuration, i.e., a system integrator may use, for instance the NAVD group also for non-navigational SFs, if desired. However, an overall load analysis of the network needs to take the actual configuration into consideration.

4.5 Serial to network gateway function (SNGF) requirements

4.5.1 General requirements

(see 8.5.1)

The SNGF shall implement all relevant functionality defined in 4.4 for each SF it supports.

Each serial port shall be implemented as a separate SF and assigned a separate SFI.

The default SFI shall use the talker mnemonic “SI”.

The SNGF may implement different types of filtering with regard to what serial line sentences are retransmitted as datagrams and what datagrams will result in a serial line sentence being sent. Any filtering methods shall be described in manufacturer’s documentation.

NOTE A typical filtering method would be to use the destination TAG ‘d' to determine what sentences in incoming datagrams are to be sent on the serial line.

4.5.2 Serial line output buffer management

(see 8.5.2)

An SNGF function block shall provide an independent buffer for each serial port it can send sentences onto. The manufacturer shall specify the maximum buffer capacity for each port. The maximum capacity may be configurable at installation.

The buffer shall be implemented as a FIFO (First In, First Out) buffer. In case of a full buffer, newly arrived sentences shall be discarded, unless these sentences are specified as prioritized (see below). Newly arrived sentences will be inserted into the buffer when buffer space is available. The method of treatment of sentences grouped by the TAG g (see 7.2.3.3) may be configurable or specified in the manufacturer’s documentation.

The SNGF may implement a priority-based functionality for some sentences with specified sentence formatters. The prioritised formatters may be configurable or specified in the manufacturer’s documentation.

Processing of prioritized sentences shall be as follows:

- only one sentence with identical talker ID and sentence formatter shall exist in the buffer;

NOTE When prioritizing AIS VDM and VDO sentences, the string beginning with the “!” character and ending with the 7th character of the encapsulation field should be used for comparison to identify identical sentences. A match of this string from a newly arrived sentence with one in the buffer means the sentence contains the same ITU-R M.1371 message from the same MMSI as the sentence already in the buffer, and can then replace the older sentence at its position in the queue.

- if a sentence, or a TAG block grouped sentences, with identical talker ID and sentence formatter exists in the buffer, the new sentence or sentences will replace the existing sentence at its position in the queue;

NOTE When prioritizing TAG block grouped sentences, several fields within the TAG block need to be compared as well as the sentence comparisons. All of the compared components should match those of the current TAG block group in order to the replace TAG block group in the queue. The components to compare are: The TAG block source parameter code value, the “number of lines” portion of the TAG block group parameter code, and the sentences within the TAG block group.

- otherwise, the new sentence shall follow the FIFO principle as described above.

If a sentence is discarded from the queue, this event shall be logged as an error internally in the equipment as defined in 4.3.3. The equipment shall have separate error counts for each serial port.

4.5.3 Datagram output requirements

(see 8.5.3)

The SNGF shall format outgoing datagrams as defined in 7.2.

The SNGF shall transmit one IEC 61162-1 sentence per outgoing IEC 61162-450 datagram to minimise delays.

4.6 Other network function (ONF) requirements

(see 8.6)

The ONF represents a function that is allowed to share the same network infrastructure as the network function blocks (NF) on an IEC 61162-450 network.

The ONF shall conform to the requirements given in 4.2.1.

The ONF equipment shall not use any IP multicast address reserved by this standard as defined in 5.4.

Documentation shall be provided describing the network protocols used by the ONF to send datagrams or byte steams for instance UDP, TCP/IP or other.

Documentation shall be provided demonstrating that the ONF cannot negatively impact the normal performance of the network or other equipment connected to the network.

5 Low level network requirements

5.1 Electrical and mechanical requirements

(see 8.7.1)

The cable and connectors used shall at least meet the specifications listed in Table 3 when used in protected environment as defined in IEC 60945.

The safety requirements and installation practices specified in IEEE 802.3, 14.7 and Clause 27 shall be followed. Also refer to IEEE 802.3, informative Annex 67.

Fibre optic interfaces shall comply with the laser safety requirements for Class 1 devices specified in IEC 60825-2.

Table 3 – Interfaces, connectors and cables

IEEE 802.3 Interface	Max network segment link distance	Mechanical device interface connector type (protected environment)	Pin assignment	Cable category, minimum
100BASE-TXS IEEE 802.3, 14.7 and Clauses 24 and 25	100 m	IEC 60603-7-3, 8-way shielded modular connector Refer to 802.3 Clause 3,IEC 60603-7 Figures 1 through 5 and IEEE 802.3/25	See b)	CAT5 STP Two shielded twisted pairs ANSI/ TIA/EIA-568-A:1995 and ISO/IEC 11801:1995 (Class D).
(not specified)	See a)	Terminal block	See b)	CAT5 STP Two shielded twisted pairs
100BASE-SX IEEE 802.3, Clauses 24 and 26	550 m	IEC 61754-20 LC type duplex optical connector. d)		Two multimode optical fibres Short wavelength 850 nm
1000BASE-T IEEE 802.3, Clause 40 (802.3ab)	100 m	IEC 60603-7-7, 8-way shielded modular connector Refer to 802.3 Clause 3 and IEC 60603-7 Figures 1 through 5. See IEEE 802.3/25	See c)	CAT5 STP Four shielded twisted pairs ANSI/ TIA/EIA-568-A:1995 and ISO/IEC 11801:1995 (Class D).
1000BASE-SX IEEE 802.3, Clause 38 (802.3z)	220 m (62/125 μm, low modal bw) 550 m (50/125 μm, high modal bw)	IEC 61754-20 LC type duplex optical connector. d)		Two multimode optical fibres Short wavelength 850 nm
For use in exposed environments, additional provisions are necessary. Consideration should be given to the M12-type specified in IEC 61076-2-101, Amendment 1 for copper network cable. And similar rugged connector for external fibre optic connectorization.				

a) In this case, the maximum operating distance should be specified by the manufacturer.

b) The 8-way modular connector specified in IEC 60603-7 is the “8P8C” type that has commonly been used in desktop computer LAN connections and incorrectly but widely referred to as “RJ45”. Wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack; the same at each end of a cable. The color-order from wire 1 to 7 shall be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown; the same at both ends of the cable. Refer to IEEE 802.3, 25.4.3 and IEC 60603-7-3.

c) The 8-way modular connector specified in IEC 60603-7 is the “8P8C” type that has commonly been used in desktop computer LAN connections and incorrectly but widely referred to as “RJ45”. Wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack; the same at each end of a cable. The color-order from wire 1 to 7 shall be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown; the same at both ends of the cable. Refer to IEEE 802.3, 40.8.1 and IEC 60603-7-7.

d) See TIA/EIA-604-10-A:2002.

5.2 Network protocol requirements

(see 8.7.2)

Equipment shall implement IP v4 as generally described in ISOC RFC 5000 with a minimum requirement of support for the following specific network protocols:

- ARP – Address Resolution Protocol as described in ISOC RFC 826 and as updated in ISOC RFC 5227;
- IP – Internet Protocol as described in ISOC RFC 791 and as updated in ISOC RFC 2474;
- UDP – User datagram Protocol as described in ISOC RFC 768;
- ICMP – Internet Control Message Protocol as described in ISOC RFC 792.

5.3 IP Address assignment for equipment

(see 8.7.3)

Means shall be provided to configure the equipment to an address in the range 172.16.0.1 to 172.31.255.254 (B type private addresses as described in ISOC RFC 1918) with a 16 bit network address mask. The assigned IP address shall remain fixed during normal operation of the equipment, including powering the equipment down and up.

5.4 Multicast address range

(see 8.7.4)

The range 239.192.0.1 to 239.192.0.64 is reserved for current and future use in the application layer protocols (see 6.2.2).

ONF equipment shall not use multicast addresses in the range 239.192.0.1 to 239.192.0.64.

NOTE ISOC RFC 2365 defines the multicast address range 239.192.0.0 to 239.192.63.255 as the IPv4 Organization Local Scope, and is the space from which an organization should allocate sub-ranges when defining scopes for private use. The specified range of IP multicast addresses map to Ethernet MAC addresses 01005E400001 to 01005E400040 (Hexadecimal).

6 Transport layer specification

(see 8.8)

6.1 General

This Clause specifies how UDP multicast messages are used to communicate between equipment over an Ethernet network.

Equipment may implement functionality for sending, receiving or both. The provisions in this Clause applies to both, but shall be tested independently as described in Clause 8.

An example of the structure of an Ethernet frame with a IEC 61162-450 sentence is given in Figure 2. The uppermost block shows the full Ethernet frame with the UDP user available data block shown in white. The IP and UDP headers are included in the grey blocks. The lower block shows the UDP user available data block with an IEC 61162-450 formatted sentence included. The numbers above the Ethernet frame gives the size of each block. The numbers in front of the UDP user data block gives the offset from the start of the block (0 – zero).

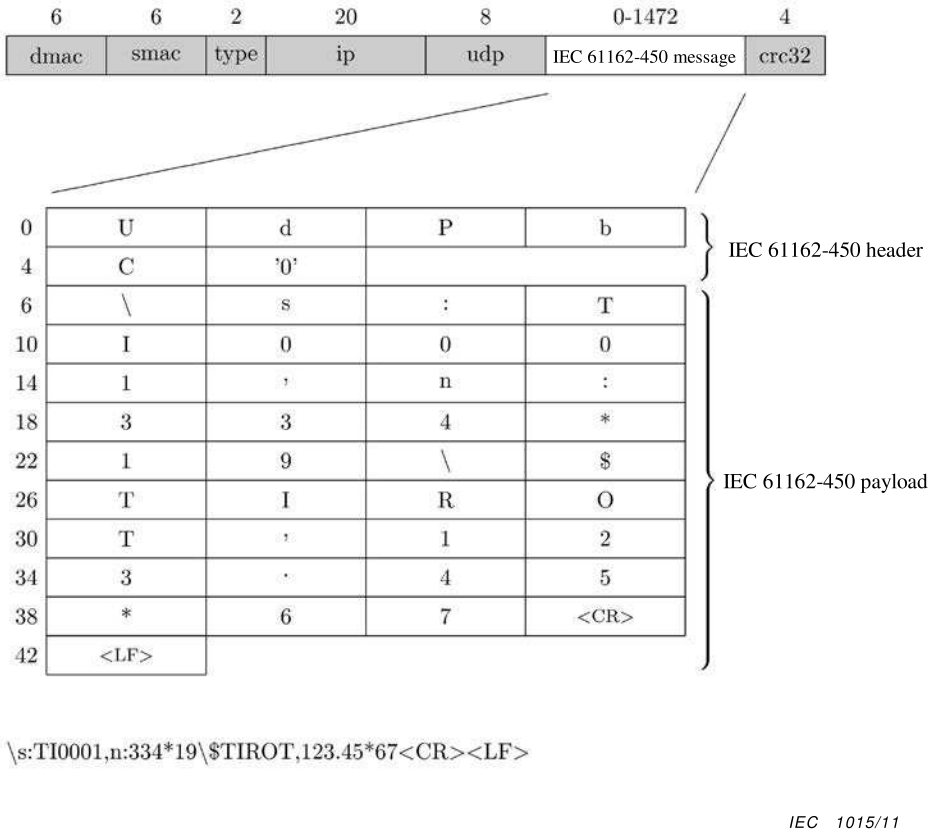

Figure 2 – Ethernet frame example for a SBM from a rate of turn sensor

6.2 UDP messages

6.2.1 UDP multicast protocol

Senders and receivers shall as a minimum be able to use the UDP protocol as defined by ISOC RFC 768 and as further specified in this standard.

6.2.2 Use of multicast addresses and port numbers

Port numbers shall be allocated from the Dynamic Port range that IANA has reserved for dynamic and/or private port numbers (range 49152 to 65535, inclusive).

Table 4 defines multicast addresses and destination port numbers that shall be used when transmitting sentences from a system function block. The mapping of SFI to default transmission group is described in Annex A.

NOTE The purpose of the port differentiation is to provide a mechanism that allows a certain level of load reduction for the receiving equipment.

Table 4 – Destination multicast addresses and port numbers

Transmission group	Category	Multicast address	Destination port
MISC	SF not explicitly listed below	239.192.0.1	60001
TGTD	Target data (AIS), tracked target messages (Radar)	239.192.0.2	60002
SATD	High update rate, for example ship heading, attitude data.	239.192.0.3	60003
NAVD	Navigational output other than that of TGTD and SATD groups	239.192.0.4	60004
VDRD	Data required for the VDR according to IEC 61996	239.192.0.5	60005
RCOM	Radio communication equipment	239.192.0.6	60006
TIME	Time transmitting equipment	239.192.0.7	60007
PROP	Proprietary and user specified SFs	239.192.0.8	60008
USR1 to USR8	User defined transmission group 1 to 8	239.192.0.9 to 239.192.0.16	60009 to 60016

NOTE The USR1 to USR8 transmission groups can be used, for example, for proprietary data in binary format.

Table 5 defines multicast addresses and destination port numbers that shall be used when transmitting binary image data.

Table 5 – Destination multicast addresses and port numbers for binary data transfer

Category	Multicast address	Destination port
Simple Binary image transfer [a]	239.192.0.21 to 239.192.0.25	60021 to 60025
Re-transmittable binary image transfer [b]	239.192.0.26 to 239.192.0.30	60026 to 60030

[a] Address 239.192.0.25, port 60025 is the recommended default for ECDIS route transfer (see IEC 61174).

[b] Address 239.192.0.26, port 60026 is the recommended default for VDR image transfer (see IEC 61996-1).

Address 239.192.0.30, port 60030 is the recommended default for ECDIS re-transmittable data blocks for route transfer (see IEC 61174).

Table 6 lists other multicast addresses and ports reserved by this standard.

Table 6 – Destination multicast addresses and port numbers for other services

Category	Multicast address	Destination port
Syslog	239.192.0.254	514

The addresses 239.192.0.17 to 239.192.0.20 and 239.192.0.31 to 239.192.0.64 are reserved for future expansion.

6.2.3 UDP checksum

All devices shall calculate and check the UDP checksum as defined by ISOC RFC 768. It is not permitted to set the checksum field to zero (no checksum).

A datagram that has an incorrect or missing checksum shall be discarded by the receiver.

6.2.4 Datagram size

The network function block shall not transmit more than 1 472 bytes of data in each datagram, including header as defined in Clause 7.

Receiving equipment is allowed to discard datagrams that have a size larger than the maximum specified size.

NOTE UDP datagrams can be up to 64 kByte in size when they are sent as a number of IP fragments.

7 Application layer specification

7.1 Datagram header

(see 8.9.2)

7.1.1 Valid header

All UDP multicast datagram shall contain one of the following strings, followed by a null character (all bits set to zero) as the first six bytes of the datagram:

- "`UdPbC`" for transmission of IEC 61162-1 formatted sentences as described in 7.2;
- "`RaUdP`" for transmission of binary images as described in 7.3;
- "`RrUdP`" for transmission of re-transmittable binary images as described in 7.3.

Incoming datagrams with an unknown header should be discarded without processing the content beyond the header.

NOTE Future editions of this standard may define other header codes. Any such header code will be different from the ones already in use and will at least contain six bytes, possibly including a trailing null character.

7.1.2 Error logging

The equipment shall maintain a count of received datagrams that do not have a valid header and make this available as defined in 4.3.3.

7.2 General IEC 61162-1 sentence transmissions

7.2.1 Application of this protocol

(see 8.9.1)

This protocol provides a mechanism by which IEC 61162-1 sentences can be sent to one or more receivers on the network. The protocol allows several sentences to be merged into one datagram.

7.2.2 Types of messages for which this protocol can be used

(see 8.9.3)

This protocol shall be used for SBM and MSM (see Annex A) type messages. The protocol shall also be used for CRP message exchanges with provisions specified in Annex C.

7.2.3 TAG block parameters for sentences transmitted in the datagram

(see 8.9.4)

7.2.3.1 Valid TAG block

Each sentence shall be preceded with one or more TAG blocks as defined in NMEA 0183 Section 7 (see also Annex B), containing the parameter codes described in the following

subclauses. If a parameter code is assigned a value more than once in the TAG blocks and only one value is expected, the last parameter value shall be used.

In this standard all identities are set at the time of installation and shall not be dynamically configurable during normal operation. The control sentences for changing parameter codes in NMEA 0183 shall not be used during normal operation.

7.2.3.2 TAG block checking

Only sentences preceded by valid TAG blocks as defined in 7.2.3.1 shall be processed by the receiver.

NOTE Receivers need to parse all TAG blocks and should ignore parameters that are not understood by the receiver. For the processing specified in this standard, only the last TAG block should be used.

7.2.3.3 Grouping control – g

The g parameter code shall be used by talkers to group TAG blocks and/or sentences. As a minimum it shall be used to group sentences that are classified as belonging to message type "MSM" in Table A.2, when the multi-sentence group consists of more than one message. It is not required to include the “g” parameter-code for single line sentences.

Receivers shall accept the g parameter code for all message types.

A valid MSM type sentence where internal data fields specifies that it belongs to a group of more than one message shall be discarded if the g group is missing or contains inconsistent information.

The group code is determined by the sending device. The initial group code value shall be one ("1") and the group code increment value shall be one ("1"). The group code shall be reset to one ("1") after it reaches 100, i.e., the valid range is 1-99, inclusive.

The following example shows the g parameter code used to group sentences in two different groups, each consisting of two sentences:

```
\g:1-2-34*59\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*2504
\g:2-2-34*5A\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*3014
\g:1-2-46*5C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*0C2D
\g:2-2-46*5F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*0420
```

7.2.3.4 Source identification – s

The s parameter code is mandatory for talkers and shall contain the system function ID (SFI see 4.4.2) corresponding to the function block from where the sentence originates.

7.2.3.5 Destination identification – d

The d parameter code is optional and shall, if used, contain the system function ID (SFI see 4.4.2) corresponding to the intended recipient of the sentence.

Multiple d parameters may be specified, if more than one receiver exists.

NOTE This may be the case for redundant control functions.

For CRP type sentences, the destination code shall be read and processed to ensure that only the intended recipients take action on the content of the sentence. Other receivers may also read the message, for example for voyage data recording purposes, but shall not take any further action on the contents.

7.2.3.6 Line-count parameter – n

The n parameter code shall be used to assign a sequence number to each sentence transmitted from a system function block. The format of the parameter value is a positive integer. The value shall start at one ("1") and shall be incremented by one ("1") for each sentence or TAG block transmitted from this system function block. The parameter value shall be reset to one ("1") when it reaches 1000, i.e., the valid range is 1-999, inclusive.

For function blocks that transmit datagram to more than one transmission group destination, separate line counters shall be maintained for each transmission group (see 6.2.2).

7.2.3.7 Text string parameter – t (Proprietary data)

The t parameter code is a free text field. This standard reserves coding for proprietary TAG-codes with the fields defined below where the leading p and the three letter manufacturer mnemonic code is required for this type of text string.

```
t:p<manufacturer mnemonic code in lower case><proprietary data>
```

An example used for proprietary authentication of lines using grouping and source for manufacturer “mmm” might be

```
\g:1-2-34,s:TI0001,n:333*68B\$TIROT,123.45*6B7
\g:2-2-34,n:334,t:pmmma;MD5;0x12345678*hh74\
```

7.2.4 Requirements for processing incoming datagrams

Any syntax error in a TAG block or a sentence shall make the receiving equipment discard the complete datagram without any further processing.

7.2.5 Error logging

(see 8.10)

The equipment shall maintain counts of errors detected in processing datagrams containing IEC 61162-1 sentences or binary images. As a minimum, the following errors shall be counted and made available as defined in 4.3.3:

- any TAG block formatting errors as defined in 7.2.3.1;
- TAG checksum error;
- TAG syntax error (line length, use of delimiters, invalid characters);
- TAG framing error (incorrect start or termination of TAG block);
- any sentence syntax errors, including formatting, length or checksum as defined in 7.2.4.

7.3 Binary image transfer using UDP multicast

(see 8.11)

7.3.1 Application of this protocol

This protocol provides a mechanism by which non IEC 61162-1 formatted data, for instance radar images, can be transmitted to one or more receivers. This protocol supports the transmission of images from zero bytes up to 4 billion image blocks.

Equipment using this mechanism shall be able to use one or both of the following two forms of image transfer:

- non re-transmittable transfers where sender sends the complete binary image without any feed-back from receiver;

- re-transmittable transfers where limited feed-back from receiver can be used to re-transmit certain parts of the image.

~~NOTE The two transmission forms use the same protocol. If any party to the transmission does not use the re-transmittable features, the protocol will automatically revert to non re-transmittable transfer mode.~~

Table 7 gives a description of terms used in this application.

Table 7 – Description of terms

Term	Description
DWORD	Double Word. One unsigned 32-bit integer (in range 0 to 4294967295). The DWORD is constructed from four consecutively transmitted BYTE, where the transmission order on the network is most significant BYTE first followed by next most significant BYTE till the least significant BYTE.
Null character	A BYTE with the value zero
Reserved bytes	A number of bytes in the datagram that may be ignored by the receiver. The reserved bytes may be additional header information that only has meaning for newer versions of the protocol or they may also be used for manufacturer specific purposes.
WORD	One unsigned 16-bit integer (in range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTE, where the transmission order on the network is the most significant BYTE followed by the least significant BYTE.
STRING[n]	A sequence of exactly n BYTE, interpreted as a string of characters. The transmission order on the network is left-most character first. If the string is shorter than n, additional trailing bytes shall be set to null character All strings in the header are encoded in ISO 18859-1 (ISO Latin 1).

7.3.2 Binary image structure

The binary images are transmitted over the network in one or more datagrams. The binary image structure is a sequential and unpadded stream of bytes divided into three main groups: Header; Binary image descriptor and Binary image data, see Table 8. The Header is needed for synchronisation and data integrity validation. The binary image descriptor is needed for the description of the binary image data and is only used in the first datagram for each image transfer.

Table 8 – Binary image structure

Header
Binary image descriptor (Only in first datagram)
Binary image data fragment
Header (zero or more)
Binary image data fragment (zero or more)

A minimum binary image transmission will consist of the three first blocks where the Binary image fragment may have zero length.

The Header shall be repeated as the first element of any datagram that contains Binary image data fragments.

7.3.3 Header

7.3.3.1 Header format

The purpose of the Header is to provide the data transfer status to receivers. This allows a receiver to identify if there is any data loss during image transfers, and how much data loss

occurs. In addition, the Header is used to provide a re-transmission mechanism for re-transmittable image transfer.

The Header format is defined in the Table 9.

Table 9 – Header format

Data item	TYPE	Description
Token	STRING[6]	Identifier as ASCII string with a length of 5 bytes followed by a null character, see 7.1.1.
Version	WORD	Defines the header version. The header version with value 1 is defined in this standard. Extensions and/or modified versions may update this value
SrcID	STRING[6]	Define the source system identifier in format ”ccxxxx”, see 4.4.2.
DestID	STRING[6]	Define the destination system identifier In format “ccxxxx”, see 4.4.2. When Destid = ”XXXXXX”, then any device can be a destination.
Type	WORD	Identifies the information in the Header.
BlockID	DWORD	Binary image block identifier. The initial value is randomly generated within a range 0 to (2^{32} – 1 = 42949672950) and is incremented by 1 after a whole block is transmitted.
SequenceNum	DWORD	Defines the sequnce number of the binary image block. In ACK, this is used to inform the sender what block was last received.
MaxSequence	DWORD	The number of datagrams needed for the transmission of this image data block. When SequenceNum is equal to MaxSequence, it means that this datagram is the last datagram of the data block. The Maxseq is used only for DATA type message. For other messages (QUERY,ACK), this field shall be 0.

7.3.3.2 Use of header token

Header token is used to identify both the type of data block and transfer mode but shall not be used to accept or reject transmissions. Two tokens are defined in 7.1.1:

- “RaUdP” – Simple binary image transfer service with UDP;
- “RrUdP” – Re-transmittable binary image transfer service with UDP.

7.3.3.3 Version

Defines the header version. It shall be set to one for this edition of the standard.

7.3.3.4 ~~Source and~~ Destination identifier

For transmissions to one specific receiver, the field shall contain the destination SFI. The field shall be “XXXXXX” otherwise.

7.3.3.5 Message type

Message type gives the information about which information is contained in the datagram:

- DATA (0x01) This type is used for transmission of binary image data including image descriptor.
- QUERY (0x02) This type is used by the sender to query the reception status from the receiver. The length of this message payload is always zero (0). It is recommended that an image sender sends a QUERY message if there is no ACK message for 1 s after a last datagram of the image block is sent or after a QUERY message is sent.
- ACK (0x03) This message is used as an acknowledgement from the receiver. This message is transmitted by the receiver either when a whole binary image is received without any error or when errors occurred during the binary image reception, for example one sequence number is skipped. Also, when a receiver receives a QUERY message from the sender, it also responds with an ACK message.

Non re-transmittable transfer makes use of only DATA message but re-transmittable transfer uses all messages.

7.3.3.6 Image block identifier

Block identifier is used to identify each image block. Since an image block is fragmented into several datagrams, the block identifier is used to assemble one or more datagrams into an image block in a receiver.

7.3.3.7 Sequence number and maximum sequence number

Sequence number (SequenceNum) and maximum sequence number (MaxSequence) is used for segmentation and re-assembly purposes. When a receiver gets a datagram, it checks the sequence number and maximum sequence number to determine if any errors have occurred or if it has received a whole message.

The sequence number is also used in ACK messages. In ACK messages, the sequence number identifies the last message the receiver receives without any error. The maximum sequence number is not used for control (Query) messages.

7.3.4 Binary image descriptor structure

The binary image descriptor format is defined in the Table 10.

Table 10 – Binary image descriptor format

Data item	TYPE	Description
Length	DWORD	Defines the binary image descriptor length in bytes. This is the length of the header as defined in this clause including the reserved bytes.
imageLength	DWORD	Defines the length of the full image content in bytes, excluding headers and descriptor.
Status of acquisition	WORD	The status for the data return. A zero is returned for normal operation. Non-zero value is used to indicate an error condition. A descriptive text may be put in the status and information text field
Device	BYTE	Data source (device) as binary value, 1 => equipment 1, 2 => equipment 2, etc. The value can be between 1 and 255
Channel	BYTE	Subdivision according to data source (device), values from 1 to 255, default = 1
TypeLength	BYTE	The length of the DataType field.
DataType	STRING[n]	This string defines the data block encoding by assigning a MIME content type to the data block for the server followed by null character. For example, “image/jpeg” is used for JPEG image type. The image quality shall comply with the image test of IEC 61996-1
Status and information text	STRING[n]	Status information (e.g. successful operation or error codes). This may be one or more strings, each terminated by a binary null
NOTE 1 There is no error check for the binary image header contents as this is handled by the UDP layer. In this specification, UDP header checksum is mandatory. NOTE 2 MIME is Multipart Internet Mail Extensions. The MIME content type was originally used for email services but is widely used for many other applications including Web. Also, it has flexibility to support new media types. The specification of the MIME content type and registration is defined in ISOC RFC 4288 and 4289.		

The Device and Channel fields are defined by the application and may be used by receivers to determine how to process the image data.

DataType shall be encoded by the MIME content-type which is “type/sub-type”, and is defined by IANA. Table 11 illustrates some examples of MIME content type for image and compressed

data. More updated information is available on the IANA web site, http://www.iana.org/assignments/media-types/.

Table 11 – Examples of MIME content type for DataType codes

Content type	File extension	MIME type/sub-type
GIF	gif	Image/gif
Microsoft Windows bitmap	bmp	image/x-ms-bmp
Gnu tar format	gtar	application/x-gtar
4.3BSD tar format	tar	application/x-tar
DOS/PC – Pkzipped archive	zip	application/zip

7.3.5 Binary image data fragment

The package data format is defined in Table 12.

Table 12 – Binary image data fragment format

Data item	TYPE	Description
Datablock	BYTE[datalength]	This item is the data either split into pieces or in one block.

The length of the image fragment is the length of the UDP datagram (as obtained from the UDP header) minus any headers that are inserted in front of the image fragment. All datagrams except the first datagram of the image which requires two headers (Header + Image Descriptor), carry only one header (Header).

The image fragment length is allowed to be zero for one or more datagrams.

NOTE There is no error check for the data contents as this is handled by the UDP layer.

7.3.6 Sender process for binary image transfer

7.3.6.3 General

Each single binary image transfer shall be identified by a unique combination of SrcID and BlockID (see Table 9). Within the same SrcID, the Device and Channel (see Table 10) shall be used to distinguish between different data sources of binary image transfers.

NOTE If a single SrcID has multiple needs to send binary images (e.g. ECDIS sending screen image, chart source information and Route exchange), then each single binary image transfer is identified, for example: ECDIS number 1 send screen image as Device = 1 and Channel = 1, and Chart source information as Device = 1 and Channel = 2.

7.3.6.1 Non re-transmittable sender process

The following steps are performed for the basic sending process:

a) a sender process waits until it gets an image block including image descriptor;

b) a block identifier is assigned for the image block (if this is the first image, then it is assigned randomly. Otherwise, the instance identifier of the previous image block + 1 is used). The BlockID shall be unique for each binary image transfer from the same SrcID;

c) an image block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer;

d) get the first datagram of the image block;

e) assign a sequence number, which is assigned ~~by zero~~ to one initially ~~and incremented by one~~;

f) compose a header including token, source id, destination id and maximum sequence number;

g) send a datagram to the network;

h) if all datagrams of the image block are not transmitted, get a next datagram and go to Step (e);

i) otherwise, then go to Step (a).

7.3.6.2 Re-transmittable sender process

The sender processing steps for re-transmittable binary image transfer is as follows:

a) a sender process waits until it gets an image block including image descriptor;

b) a block identifier is assigned for the image block (if this is the first image, then it is assigned randomly. Otherwise, the block identifier of the previous image block + 1 is used). The BlockID shall be unique for each binary image transfer from the same SrcID;

c) an image block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer;

d) get the first datagram of the image block;

e) assign a sequence number, which is assigned ~~by zero~~ to one initially ~~and incremented by one~~;

f) set re-transmission counter zero(0);

g) compose a header including token, source id, destination id and maximum sequence number;

h) send a datagram to the network;

i) if the sender receives an ACK message, whose sequence number is less than the maximum sequence number,

- get a datagram whose sequence number is sequence number in ACK message plus one,
- increase re-transmission count by one,
- go to Step (~~e~~ g);

j) if all datagram of the image block is not transmitted,

- get a next datagram,
- go to Step (~~e~~ g);

k) otherwise,

- set a ACK timer,
- wait for an ACK message;

l) if the sender receives an ACK message whose sequence number is equal to the maximum sequence number, then go to Step (a);

m) if the sender receives an ACK message whose sequence number is less than the maximum sequence number, then go to Step (h);

n) if ACK Timer expires and re-transmission counter is less than three, then,

- increase the re-transmission counter,
- go to Step (j);

o) if ACK Timer expires and re-transmission counter is equal to three, then,

- clear the sending buffer,
- go to Step (a).

7.3.7 Receiver process for binary image transfer

7.3.7.3 General

Each single binary image transfer shall be identified by a unique combination of SrcID and BlockID (see Table 9). Within the same SrcID, the Device and Channel (see Table 10) shall be used to distinguish between different data sources of binary image transfers.

NOTE If a single SrcID has multiple needs to send binary images (e.g. ECDIS sending screen image, chart source information and Route exchange), then each single binary image transfer is identified, for example: ECDIS number 1 send screen image as Device = 1 and Channel = 1, and Chart source information as Device = 1 and Channel = 2.

7.3.7.1 Non re-transmittable receiver process

The receiver process steps of the non re-transmittable binary image transfer is as follows:

a) waits for receiving new datagram;

b) if the ~~block identifier~~ BlockID of the received datagram for same source identified by the combination of SrcID, Device and Channel is not equal to that of the previous datagram,

- if there is any data in the receiver buffer, it is delivered to the SF,
- the receiver buffer is cleared;

c) put a datagram into the receiver buffer;

d) if the sequence number is same as the maximum sequence number,

- the all data in the received buffer is delivered to the SF,
- the receiver buffer is cleared;

e) go to Step (a).

7.3.7.2 Re-transmittable receiver process

The re-transmittable receiver process steps are performed only by the receiver whose identifier is same as the DestID in the Header as follows:

a) waits for receiving new datagram;

b) if the received datagram is QUERY message then,

- compose a Header with the ~~block identifier~~ BlockID and sequence number of the previous datagram,
- send a datagram to the sender,
- go to Step (a);

c) if the ~~block identifier~~ BlockID of the received datagram for same source identified by the combination of SrcID, Device and Channel is not equal to that of the previous datagram,

- if there is any data in the receiver buffer, it is delivered to the SF,
- the receiver buffer is cleared;

d) if the sequence number is not same as the sequence number of the previous datagram plus one, then,

- compose a Header with the block identifier and sequence number of the previous datagram,
- send a datagram to the sender,
- go to Step (a);

e) put a datagram into the receiver buffer;

f) if the sequence number is same as the maximum sequence number,

- all the data in the received buffer is delivered to the SF,

- the receiver buffer is cleared;

g) go to Step (a).

7.3.8 Other requirements

7.3.8.1 Re-transmittable messages that cannot be processed

Both receiver and sender shall silently ignore messages that are related to the retransmit process that they cannot process themselves.

7.3.8.2 Multiple binary image blocks

A receiver that receives a binary image block more than once shall ignore all but one of the transmissions.

NOTE It is allowed both to ignore the first (overwrite buffer) or the last (ignore).

7.3.8.3 Retransmissions size

If a sender retransmits one or more binary image blocks, each of the blocks shall have the same size and same header information.

7.3.8.4 Maximum outgoing rate

The data volume for each binary image source shall not exceed 2 MBytes per second.

NOTE This provision is included to guarantee spare network capacity for other transmissions in between the blocks of a large binary image. When the image is transmitted as multicast it will flood the network and can inhibit transmissions of other data.

7.3.8.5 End of transmission

The receiver shall assume that a transmission has ended unsuccessfully when it gets a binary image block from same source identified by the combination of SrcID, Device and Channel (see Table 9 and Table 10) with a new BlockID. Then the receiver stops the current receiving process and becomes ready for the new image block receiving. The transmission shall also be considered finished when the last block is signalled by the SequenceNum from the sender. When a receiver gets the last block, then it sends an ACK message to the sender so as to start new image block transmission.

The sender shall assume that a transmission has ended unsuccessfully when it requires more than three re-transmissions of the binary image blocks including control messages. The sender assumes that the transmission is successfully finished only if it receives an ACK message with the SequenceNum which is equal to the MaxSequence. When a transmission is ended, a sender starts a new transmission if necessary.

7.3.8.6 Gaps between ACK messages

In general, a receiver shall, immediately after loss detection, transmit an ACK message to the sender if a binary image block has been lost either by having a gap in sequence numbers or by finding errors in the block. Since there is a time delay between the reception of the ACK message and re-transmission of lost data at the sender, a receiver waits for the sender's response. For this purpose, a receiver should wait at least 200 ms before it sends another ACK message. However, when a receiver receives all messages correctly, it shall send an ACK message immediately to the sender.

NOTE ACK message is used both for positive and negative acknowledge. See 7.3.3.5 for the description of the ACK message.

7.3.8.7 Maximum retransmissions

The maximum number of re-transmissions is limited for three times. If an image block requires more than three times re-transmission, the sender stops the transmission and starts a new image block transmission.

In addition to data message re-transmission, control messages can be re-transmitted in case the control message is lost. The re-transmission counter increases whenever the control message is transmitted.

7.3.8.8 Timer management

Re-transmission timer is managed at the sender. A sender sets the re-transmission timer when either a whole image block is transmitted and waits for an ACK message, or a control message (QUERY) message is transmitted. When the re-transmission timer expires, the sender (re-) transmits a QUERY message and sets the timer again unless the re-transmission counter reaches three.

7.3.8.9 UDP port and IP addresses

Multicast addresses and ports for the service type are given in Table 5. As a default, addresses for simple and re-transmittable imager transfer service shall be 239.192.0.21 and 239.192.0.26 respectively. As a default, the port for simple and re-transmittable binary transfer shall be 60021 and 60026 respectively.

The receiver shall reply with ACK to the sender using the incoming datagram's multicast address and destination port. Optionally a reply with ACK to the sender may use any multicast address within the range from 239.192.0.21 to 239.192.0.30 and corresponding port number within the range from 60021 to 60030. This option requires that the system supports separate multicast address and port assignment for binary Image transfer sending and for ACK messages of binary Image transfer. For this option the default is 239.192.0.22 and 60022.

~~NOTE The radar should support configuration of the VDR port number and IP address.~~

7.3.9 Error logging

Equipment shall maintain a count of the events of invalid binary image structures processed and make the count available. As a minimum, the following events shall be logged:

- the number of image blocks where errors occur;
- missing datagrams;
- unrecognized header.

8 Methods of test and required results

8.1 Test set-up and equipment

The following test methods require test equipment capable of transmitting and receiving UDP datagrams over the Ethernet interface and the use of a network protocol analyser. The test equipment shall be capable of supporting the Ethernet interface appropriate for the device under test. The equipment shall also be capable of generating invalid data.

The test equipment shall be configured to transmit UDP broadcast messages for the ports defined in 6.2.2.

Simulation equipment is required capable of

- generation of test UDP datagrams containing unique and numbered content, syntactically correct and incorrect sentences with datagram intensity that can be varied to exceed IEC 61162-1 and IEC 61162-2 channel capacity,
- generation of IEC 61162-1 test sentences containing unique and numbered content, syntactically correct and incorrect with variable length and correct, incorrect and missing checksum,
- generation of non re-transmittable and re-transmittable binary images.

8.2 Basic requirements

8.2.1 Equipment to be connected to the network

(see 4.2.1)

Verify through inspection of test documentation, that the network devices have been tested against the relevant requirements contained in IEC 60945.

For the purposes of IEC 60945 the following definitions apply.

- **Performance check**
  A performance check is the successful transmission and reception of data.
- **Performance test**
  A performance test consists of evaluating performance under different test scenarios.

8.2.2 Network infrastructure equipment

(see 4.2.2)

If the device under test is an IGMP snooping or CGMP enabled switch, confirm that IGMP snooping or CGMP can be disabled and that the documentation describes how to disable it.

Confirm by inspection of manufacturer provided information that the device under test does not provide the functions of router or a repeater hub.

8.3 Network function (NF)

8.3.1 Maximum data rate

(see 4.3.2)

Confirm by inspection that the manufacturer has specified the maximum datagram ~~output~~ input rates as specified in items a) to c) in 4.3.2.

After activating all NF ports of the equipment under test with the specified maximum aggregate datagram rate as specified in 4.3.2, check that the performance of the equipment is not degraded in any way.

8.3.2 Error logging function

(see 4.3.3)

Confirm the manufacturer has provided means to inspect a log of detected errors.

NOTE Tests for the errors to be logged are given in 8.5.2, ~~8.8,~~ 8.9.2, 8.10 and 8.11.4.

Confirm that, if external data logging capability is provided, that the output of Syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

8.4 System function (SF)

8.4.1 General

(see 4.4.1)

For SFs that implement IEC 61162-1 and IEC 61162-1-2 interfaces, verify compliance in accordance with the test methods and required test results of IEC 61162-1, Annex B.

8.4.2 Assignment of unique system function ID (SFI)

(see 4.4.2)

Check that means are provided to assign and configure the SFI, as described in 4.4.2.

8.4.3 Implementing configurable transmission groups

(see 4.4.3)

Check that means are provided to assign and configure the transmission groups. Check that documentation has been provided describing the transmission groups supported by the device.

8.5 Serial to network gateway function (SNGF)

8.5.1 General

(see 4.5.1)

Check that it is possible to enter unique SFIs for all serial ports of the device and that the mapping of SFI to serial port is correctly implemented by analyzing the UDP datagrams.

Check that documentation is available describing any filtering used in the device.

8.5.2 Serial line output buffer management

(see 4.5.2)

Verify the output routing by feeding the network under test with datagrams containing sentences for all available serial outputs and check that sentences are routed to the output ports having the set SFIs.

Verify output buffer overflow handling by increasing the datagram data rate until possible capacity of the serial lines are exceeded and check that

- sentences are correctly discarded, maintaining the FIFO order and not affecting sentence integrity,
- the buffer overflow events are logged as required.

Verify required functionality for prioritized messages by repeating the test with the unit set for prioritized messages and check that behaviour is correct.

Verify message buffer integrity by repeating the test also with grouped messages and check that overflow handling maintains group integrity, meaning that whole groups are discarded, regardless of the prioritized message setting.

8.5.3 Datagram output

(see 4.5.3)

Verify datagram conversion by feeding the input ports of the network under test with sentences and check that these are transmitted in UDP datagrams with correct syntax and SFI.

The test sentences should include TAG blocks and grouped messages.

8.6 Other network function (ONF)

(see 4.6)

Verify by inspection of the manufacturer's documentation that information for the use of ONF is provided as described in 4.6.

Verify using the test equipment described in 8.1 that the ONF does not use any of the multicast IP addresses reserved in 5.4.

8.7 Low level network

8.7.1 Electrical and mechanical requirements

(see 5.1)

Verify by observation that one of the connectors specified in Table 3 is available on the equipment.

Verify by inspection of manufacturer documentation that one or more of these interfaces meets the requirements of Table 3.

Verify by inspection of manufacturer documentation that the laser safety requirements for Class 1 devices are met.

8.7.2 Network protocol

(see 5.2)

Confirm by inspection of documented evidence that the relevant IEEE 802.3 data link protocol is used.

Verify using the network protocol analyser that IP (Version 4) protocol is used and that no IP option is used.

Confirm using ping program that each device supports the network protocols specified.

8.7.3 IP address assignment for equipment

(see 5.3)

Confirm by observation that means are provided to configure an IP address for the device.

Confirm that an IP address for the device is configured with the range of 172.16.0.1 to 172.31.255.254.

Using the test equipment described in 8.1 and documentation provided by the manufacturer, verify by transmitting and receiving data that the equipment does not change its IP address and IP port settings after an OFF/ON power cycle.

8.7.4 Multicast address range

(see 5.4)

Verify using the network protocol analyser that each datagram is transmitted and received with the multicast address 239.192.0.1 to 239.192.0.64.

8.8 Transport layer

(see Clause 6)

Verify that UDP messages are transmitted and received at each of the appropriate port numbers as defined in Tables 4 and 5.

Verify that UDP are discarded if the received UDP checksum is invalid.

Verify that each datagram contains no more than 1 460 bytes.

~~Verify that UDP datagram can be logged if the received UDP checksum is invalid.~~

8.9 Application layer

8.9.1 Application

(see 7.2.1)

Using the test equipment described in 8.1 and documentation provided by the manufacturer verify by transmitting and receiving data that each SF and SNGF port of the equipment under test can send and receive IEC 61162-1 sentences and allows several sentences to be merged into one datagram if applicable.

8.9.2 Datagram header

(see 7.1)

Check that all UDP multicast datagrams are headed by:

- "UdPbC" for transmission of IEC 61162-1 formatted sentences;
- "RaUdP" for transmission of binary images;
- "RrUdP" for transmission of re-transmittable binary images;

followed by a null character (all bits set to zero) as the first six bytes of the datagram.

Check that incoming datagrams with an unknown header are discarded without processing the content beyond the header.

Verify that UDP datagram can be logged if UDP header is unrecognized or invalid, or has a UDP checksum error, including receiving datagrams with a zero checksum.

8.9.3 Types of messages

(see 7.2.2)

Using the test equipment described in 8.1, and documentation provided by the manufacturer, verify by transmitting and receiving data that each SF and SNGF port of the equipment under test can send and receive each of the message types specified by the manufacturer; one or more of SBM, MSM and CRP. For CRP messages, verify that the requirements of Clause C.4 are met by inspection of recorded datagrams and, in the case of timeout handling, the equipment's error log data.

8.9.4 TAG block parameters

(see 7.2.3)

8.9.4.1 Test of the transmitter

Verify using a receiving protocol analyzer that

- all members of group have same group code value,
- next group code value after 99 is 1,
- the device under test transmits the source identifier (two separate test cases – default and configured),
- if used, the device under test transmits valid destination code,
- line count value increments for each line and resets after 999 to 1,
- the heartbeat sentence (HBT) is transmitted at least once every 60 s,
- the device under test only feeds sentences preceded by a valid TAG block (for example "\s:II0001,n:23*31\$LCGLL,5420.123,N,01030.987,E,,A,A*~~7C~~58<CR><LF>") into the network.

8.9.4.2 Test of the receiver

Verify using a transmitting protocol analyzer that

- lines without a TAG block are not used as defined in 7.2.3.1,
- adding a TAG block containing syntactically correct parameter codes (for example "\z:Y23G81*56\") not defined in this standard is transparent to normal operation,
- only complete sentence groups are used,
- TAG block lines with the device under test as destination are processed.

8.9.4.3 Test for bidirectional communication

If the network under test supports CRP then using a bidirectional protocol analyzer verify that source and destination are correct in the CRP communication.

8.9.4.4 Configuration

Verify by inspection of documentation that it is not possible to dynamically configure any identities after installation.

8.10 Error logging

(see 7.2.5)

By feeding test sentences with variable contents into the network, verify that the network under test processes only sentences preceded by a valid TAG block as defined in 7.2.3.1 and verify that

- lines with TAG checksum errors increase the corresponding error log count as defined in 4.3.3,
- lines with TAG syntax errors increase the corresponding error log count as defined in 4.3.3,
- lines with TAG framing errors (i.e. missing \ character at start, stop and between adjacent TAG blocks) increase the corresponding error log count as defined in 4.3.3.

Check handling of incorrect messages by feeding the network under test with sentences having

- incorrect syntax,

- incorrect checksum,
- incorrect message length.

Verify that these sentences are discarded and that the network's error logs are updated.

8.11 Binary image transfer using UDP multicast

(see 7.3.)

8.11.1 Sender process test

8.11.1.1 Non re-transmittable image transfer

Using a test set-up with non re-transmittable binary images, verify that

- header tokens are set correctly,
- header version is one (=1),
- srcID is correctly set,
- destID is set by "XXXXXX",
- ~~BlockID is randomly generated whenever sender restarts,~~
- unique BlockID is correctly set,
- BlockID, SequenceNum and MaxSequence are correctly set,
- Device is correctly set,
- Channel is correctly set,
- the IP address and port numbers are assigned by one of the addresses for non re-transmittable binary image transfer,
- there is no response when a receiver sends any ACK messages.

8.11.1.2 Re-transmittable image transfer

Using a test set-up with re-transmittable binary images, verify that

- header tokens are set correctly,
- header version is one (=1),
- SrcID and DestID is correctly set by "ccxxxx",
- ~~BlockID is randomly generated whenever sender restarts,~~
- Unique BlockID is correctly set,
- BlockID, SequenceNum and MaxSequence are correctly set,
- Device is correctly set,
- Channel is correctly set,
- the IP address and port numbers are assigned by one of the addresses for re-transmittable binary image transfer,
- a new data transmission is started after an ACK message, whose SequenceNum is equal to the MaxSequence, after all data is transmitted,
- a QUERY message is sent when there is no ACK message after all data is transmitted,
- a QUERY message is sent when there is no ACK message after a QUERY message is transmitted,
- image data is re-transmitted when an ACK message, whose SequenceNum is less than the MaxSequence, is received,
- the number of re-transmissions including the number of QUERY message is always less than or equal to three,

- new data transmission is started when the number of re-transmission including the number of QUERY message is more than three,
- log messages are correct.

8.11.2 Receiver process test

8.11.2.1 Non-retransmittable image transfer

Using a test set-up with non re-transmittable binary images, verify that

- messages are received correctly on given IP and port address,
- each separate image transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- a new receiving process starts when a message with new BlockID is received for the combination of SrcID, Device and Channel,
- the received messages are the same as that of the transmitted data when there is ~~any~~ no loss,
- any log information is provided if there is any loss,
- log messages are correct.

8.11.2.2 Re-transmittable image transfer

Using a test set-up with re-transmittable binary images, verify that

- messages are received correctly on given IP and port address,
- each separate image transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- an ACK message is transmitted when the received SequenceNum is equal to the MaxSequence with the same instance identifier,
- an ACK message is transmitted when a receiver detects that there is a gap in the SequenceNum between two consecutive messages,
- a new receiving process starts when a message with new BlockID is received for the combination of SrcID, Device and Channel,
- the received messages are the same as that of the transmitted data,
- the receiver does not send any control message when a sender sends an image block with different DestID,
- log messages are correct.

8.11.3 Image descriptor test

Using a test set-up with binary images, verify that

- the device and channel is correctly set,
- image length in the descriptor is the same as the size of the received data,
- the received data format is the same as that of the data type in the descriptor.

8.11.4 Image transfer error logging

Using a test set-up with binary images, verify that the following events can be logged

- number of image blocks where errors occur,
- missing datagrams,
- unrecognized headers.

Annex A
(normative)

Classification of IEC 61162-1 talker identifier mnemonics and sentences

A.1 General

Table A.1 gives a mapping from talker identifier mnemonic to a default transmission group for an SF.

Table A.2 classifies each of the IEC 61162-1 sentence formatters as belonging to one of three types of message

- sensor broadcast message (SBM) see 3.18,
- multi-sentence message (MSM) see 3.12,
- command-response pair (CRP) see 3.4.

A.2 Talker identifier mnemonic to transmission group mapping

Table A.1 maps the two first characters of the SFI that is normally the IEC 61162-1 talker identifier mnemonic, to the default transmission group the SF shall use for transmitting sentences. For the two character codes listed in Table A.1, the transmission group is identified in column three. For two character codes not in this table, the SF shall use the MISC transmission group as default.

Proprietary sentences that do not use a talker identifier mnemonic can be given a default transmission group by the manufacturer.

Table A.1 – Classification of IEC 61162-1 talker identifier mnemonics

Type of equipment	Talker identifier	Transmission group
Heading/track controller (autopilot) general	AG	NAVD
magnetic	AP	NAVD
Automatic identification system	AI	TGTD
Bilge system	BI	MISC
Bridge navigational watch alarm system	BN	VDRD
Communications: digital selective calling (DSC)	CD	RCOM
data receiver	CR	RCOM
satellite	CS	RCOM
radio-telephone (MF/HF)	CT	RCOM
radio-telephone (VHF)	CV	RCOM
scanning receiver	CX	RCOM
Direction finder	DF	NAVD
Duplex repeater station	DU	MISC

Type of equipment	Talker identifier	Transmission group
Electronic chart system (ECS)	EC	NAVD
Electronic chart display and information system (ECDIS)	EI	NAVD
Emergency position indicating radio beacon (EPIRB)	EP	RCOM
Engine room monitoring system	ER	MISC
Fire door controller/monitoring system	FD	VDRD
Fire extinguisher system	FE	VDRD
Fire detection system	FR	VDRD
Fire sprinkler system	FS	VDRD
Galileo positioning system	GA	NAVD
Global positioning system (GPS)	GP	NAVD
GLONASS positioning system	GL	NAVD
Global navigation satellite system (GNSS)	GN	NAVD
Heading sensors: compass, magnetic	HC	NAVD
gyro, north seeking	HE	SATD
fluxgate	HF	NAVD
gyro, non-north seeking	HN	SATD
Hull door controller/monitoring system	HD	VDRD
Hull stress monitoring	HS	VDRD
Integrated instrumentation	II	MISC
Integrated navigation	IN	NAVD
LORAN: LORAN-C	LC	NAVD
Navigation light controller	NL	MISC
Radar and/or radar plotting	RA	TGTD
Propulsion machinery including remote control	RC	MISC
Sounder, depth	SD	NAVD
Steering gear/steering engine	SG	MISC
Electronic positioning system, other/general	SN	NAVD
Sounder, scanning	SS	MISC
Turn rate indicator	TI	SATD
Microprocessor controller	UP	MISC
(0<=#<=9) User configured talker identifier	U#	MISC
Velocity sensors: Doppler, other/general	VD	NAVD
speed log, water, magnetic	VM	NAVD
speed log, water, mechanical	VW	NAVD

Type of equipment	Talker identifier	Transmission group
Voyage data recorder	VR	MISC
Watertight door controller/monitoring system	WD	VDRD
Water level detection system	WL	VDRD
Transducer	YX	MISC
Timekeeper, time/date: atomic clock	ZA	TIME
chronometer	ZC	TIME
quartz	ZQ	TIME
radio update	ZV	TIME
Weather instrument	WI	NAVD
Serial to Network Gateway Function[a]	SI	MISC

[a] This talker is not defined in IEC 61162-1, but included here for use by SNGF function blocks.

A.3 List of all sentence formatters and the sentence type

Table A.2 classifies the existing IEC 61162-1 formatters. The rightmost column lists related sentence formatters for MSM and CPR sentences.

Table A.2 – Classification of IEC 61162-1 sentences

	Description	SBM	MSM	CRP	Related sentence formatters
Q	Query sentence			X	Any reply message
AAM	Waypoint arrival alarm	X			
ABK	AIS addressed and binary broadcast acknowledgement	X			ABK, ABM, AIR, BBM
ABM	AIS Addressed binary and safety related message		X		ABM
ACA	AIS channel assignment message		X		ACA, ACS
ACK	Acknowledge alarm			X	ALR, ACK
ACS	AIS Channel management information source		X		ACA, ACS
AIR	AIS Interrogation request.				ABK
AKD	Acknowledge detail alarm condition			X	ALA, AKD
ALA	Report detailed alarm condition			X	ALA, AKD
ALR	Set alarm state			X	ALR, ACK
APB	Heading/track controller (autopilot) sentence B	X			
BBM	AIS Broadcast binary message		X		BBM
BEC	Bearing and distance to waypoint – dead reckoning	X			
BOD	Bearing origin to destination	X			
BWC	Bearing and distance to waypoint – great circle	X			
BWR	Bearing and distance to waypoint – rhumb line	X			
BWW	Bearing waypoint to waypoint	X			

	Description	SBM	MSM	CRP	Related sentence formatters
CBR	Configure Broadcast Rates for AIS AtoN Station Message Command		X		MEB
CUR	Water current layer – Multi-layer water current data	X			
DBT	Depth below transducer	X			
DDC	Display Dimming Control	X			
DOR	Door status detection		X		DOR
DPT	Depth	X			
DSC	Digital selective calling information	X			
DSE	Expanded digital selective calling	X			
DTM	Datum reference	X			
ETL	Engine telegraph operation status	X			
EVE	General event message	X			
FIR	Fire detection		X		FIR
FSI	Frequency set information	X			
GBS	GNSS satellite fault detection	X			
GEN	Generic binary information	X			
GFA	GNSS fix accuracy and integrity	X			
GGA	Global positioning system (GPS) fix data	X			
GLL	Geographic position – latitude/longitude	X			
GNS	GNSS fix data	X			
GRS	GNSS range residuals	X			
GSA	GNSS DOP and active satellites	X			
GST	GNSS pseudorange noise statistics	X			
GSV	GNSS satellites in view	X			
HBT	Heartbeat supervision sentence	X			
HDG	Heading, deviation and variation	X			
HDT	Heading true	X			
HMR	Heading monitor receive			X	HMS
HMS	Heading monitor set			X	HMR
HSC	Heading steering command	X			
HSS	Hull stress surveillance systems	X			
HTC	Heading/track control command			X	HTD
HTD	Heading /track control data			X	HTC
LR1	AIS long-range reply sentence 1		X		LRF, LRI
LR2	AIS long-range reply sentence 2		X		LRF, LRI
LR3	AIS long-range reply sentence 3		X		LRF, LRI
LRF	AIS long-range function		X		LR1, LR2, LR3, LRF
LRI	AIS long-range interrogation		X		LR1, LR2, LR3, LRF
MEB	Message input for broadcast command		X		CBR
MSK	MSK receiver interface	X			

	Description	SBM	MSM	CRP	Related sentence formatters
MSS	MSK receiver signal status	X			
MTW	Water temperature	X			
MWD	Wind direction and speed	X			
MWV	Wind speed and angle	X			
NAK	Negative acknowledgment			X	ALR, NAK
NRM	NAVTEX receiver mask			X	NRX
NRX	NAVTEX received message		X		
OSD	Own ship data	X			
POS	Device position and ship dimensions report or configuration command			X	
PRC	Propulsion remote control status	X			
RMA	Recommended minimum specific LORAN-C data	X			
RMB	Recommended minimum navigation information	X			
RMC	Recommended minimum specific GNSS data	X			
ROR	Rudder order status	X			
ROT	Rate of turn	X			
RPM	Revolutions	X			
RSA	Rudder sensor angle	X			
RSD	Radar system data	X			
RTE	Routes	X			
SFI	Scanning frequency information	X			
SSD	AIS ship static data	X			
STN	Multiple data ID	X			
THS	True heading and status	X			
TLB	Target label	X			
TLL	Target latitude and longitude	X			
TRC	Thruster control data	X			TRD
TRD	Thruster response data	X			TRC
TTD	Tracked Target Data		X		
TTM	Tracked target message	X			
TUT	Transmission of multi-language text		X		
TXT	Text transmission		X		
UID	User identification code transmission	X			
VBW	Dual ground/water speed	X			
VDM	AIS VHF data-link message		X		Sometimes single
VDO	AIS VHF data-link own-vessel report	X			
VDR	Set and drift	X			
VER	Version		X		
VHW	Water speed and heading	X			
VLW	Dual ground/water distance	X			

	Description	SBM	MSM	CRP	Related sentence formatters
VPW	Speed measured parallel to wind	X			
VSD	AIS voyage static data	X			
VTG	Course over ground and ground speed	X			
WAT	Water level detection	X			
WCV	Waypoint closure velocity	X			
WNC	Distance waypoint to waypoint	X			
WPL	Waypoint location	X			
XDR	Transducer measurements	X			
XTE	Cross-track error, measured	X			
XTR	Cross-track error, dead reckoning	X			
ZDA	Time and date	X			
ZDL	Time and distance to variable point	X			
ZFO	UTC and time from origin waypoint	X			
ZTG	UTC and time to destination waypoint	X			

Annex B
(informative)

TAG block example

NOTE Abbreviations related to the IEC 61162 series of standards and NMEA 0183 series are not included in the below example. For their meaning refer to those standards.

B.1 Validity of this information

NMEA 0183 series defines the syntax and semantics of the TAG block. This Annex shows a few examples of how the TAG block can be used in relation to this standard and these examples are included for information only.

B.2 TAG Block structure in this standard

The TAG block structure examples provided are not intended to include all possible uses for the TAG block.

NMEA 0183 lists all the possible combinations of input lines, and settings for the listener destination-identification and listener source-identification data fields.

TAG block parameter codes that have specific meaning within the context of this standard in the TAG blocks are listed in Table B.1.

A TAG Block is able to associate or link data in the TAG block and IEC 61162-1 sentences and is intended to be used to facilitate transport of IEC 61162-1 sentences over a network.

One use of the source parameter to identify a System Function block (SF) or a Network Function block (NF) device is shown below.

```
\s:GP0002,d:SI0001,d:SI0005,n:23*21\$GNGNS,122310.2,3722.425671,N,
12258.856215,W,DA,14,0.9,1005.543,6.5,5.2,23*59<CR><LF>
```

In the example the source "s" identified is a system function block with implied talker identifier “GP” (Global Positioning System – GPS) that has been designated as equipment number "0002". The destination "d:" for the information is two SNGF serial ports with equipment numbers “0001” and “0005” . Other equipment listening on the same transmission group can also read and process this information. This sentence is line number "n:" 23, from this GNSS source.

```
\g:1-2-98,n:248,s:AI0002*76\
!AIVDM,2,1,9,A,54a5;h02=UWH?I=O8004pEA@D000000000000016BHQ,0*7B

\g:2-2-98,n:249,s:AI0002*74\
!AIVDM,2,2,9,A,?84bD0@URC0H13p0kkQ1@0000000,2*16
```

In the second example shown directly above, the "g" character is employed to group the sentences from an AIS source identified with SFI “AI0002”. The g code is divided into three fields where the use of each field (from left to right) are:

1. The line number for this particular TAG block and associated sentence.

2. The total number of lines.

3. The group code. Used to differentiate between different groups of TAG blocks and sentences.

```
\g:1-2-34,s:HE0003,n:23,d:VR0001*3C\$HETHS,181.3,A*26<CR><LF>
```

In this third example the gyro compass with SFI “HE0003” is providing its data to the destination device which is a voyage data recorder with SFI “VR0001”. In this case the destination code is strictly speaking superfluous as all devices listening on the transmission group can read and process the information.

Parameter codes and data for use in the IEC 61162-450 protocol can be located in different TAG blocks and the same parameter code may occur several times. In this case the last occurrence (reading from left to right) of the parameter code should be used.

```
\g:1-2-
98,s:sbAIS02*72\\n:248,s:AI0002*05\ !AIVDM,2,1,9,A,54a5;h02=UWH?I=O8004pEA@D00
0000000000016BHQ,0*7B
```

This is shown in the last example which is a variant of first line of the second example above. In this case the grouping information should be taken from the left most TAG block while the line number and source code should be taken from the right most. The source code in the left most TAG block is not in IEC 61162-450 format and does presumably contain information not intended for use in this protocol.

In general a TAG block will consist of a list of parameter code and value pairs. Each parameter code and associated value code is separated by a comma and the code and value pair is separated by a colon.

The maximum length of a TAG block is 80 characters. It is delineated by a back-slash at the start and the end of the TAG block.

B.3 TAG block parameter-code dictionary

Table B.1 lists the currently defined parameter-codes that are required when using TAG block within this standard. All codes are one lower case character.

NOTE Table B.1 is a subset of TAG Block parameters defined in NMEA 0183, section 7. NMEA 0183 defines for example additional TAG Blocks for UNIX time (c), Relative time (r), etc.

Table B.1 – Defined parameter-codes

Parameter-code	Description	Form of parameter value
d	Destination-identification	Alphanumeric string (15 char. maximum)
g	Sentence-grouping	Grouped numeric string (alphanumeric)
n	Line-count	Positive integer
s	Source-identification	Alphanumeric string (15 char. maximum)
t	Text	Free text, including proprietary information

Annex C
(normative)

Reliable transmission of command-response pair messages

C.1 Purpose

The rules that are listed below are included to promote reliable bidirectional exchanges of sentences classified as command-response pair (CRP) in Annex A. All equipment making use of CRP message exchanges shall follow these rules.

C.2 Information exchange examples

Examples of bidirectional communication where command-response pair typically occur include

- query for sentences,
- alarm and acknowledge,
- equipment initialisation with response success or fail,
- command followed by data or status as response.

Although the content differs, the information exchange is similar in structure.

C.3 Characteristics

Two parties exist in the communication, see Figure C.1. The Network device 1 (ND1) is transmitting the command and the ND2 is transmitting a response as a result of the processing of the command.

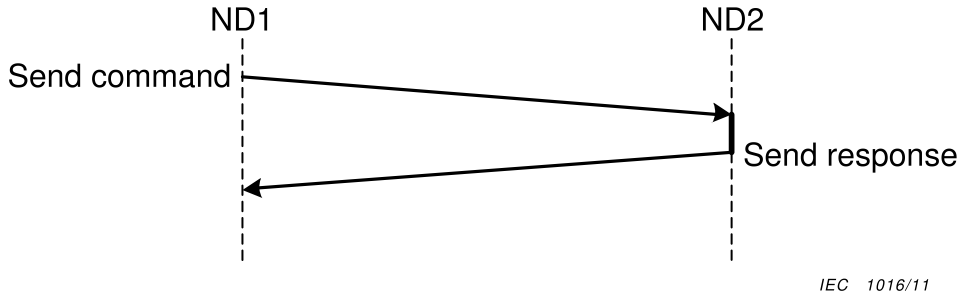

Figure C.1 – Command response communications

C.4 Requirements

The requirements for reliable communication include:

- TAG block parameter “s” shall be used to uniquely identify the source of the sentence;
- TAG block parameter “d” shall be used to uniquely identify the destination of the sentence;
- TAG block parameter “g” shall be used to group sentences if required;
- TAG block parameter “n” shall be used to assign a sequence number to each sentence transmitted from a system function block, if required;
- timeout handling to detect loss of messages;

- optional timestamp to limit the effect of time delays for transmission.

C.5 Data flow description

C.5.1 Heartbeat message

The heartbeat sentence (HBT) is intended to inform that the unit is in normal operation, if no other requirements specify other messages for this purpose, for example as done in C.5.4. It shall be sent at a stated interval. The example below transmits interval set to 60 s and shows the sequential sentence identifier incremented from 3 to 4 to distinguish sentences.

```
...
\s:YX0001,n:123*01\$YXHBT,60,A,3*2307<CR><LF>
...
\s:YX0001,n:231*01\$YXHBT,60,A,4*2400<CR><LF>
```

C.5.2 Command response pair

This example is for command-response to set NAVTEX receiver mask from an INS.

```
\s:IN0001,d:NR0001,n:123*68\$INNRM,2,1,00001E1F,00000023,C*1C38<CR><LF>
```

The response within timeout from the NAVTEX receiver is if operation is successful

```
\s:NR0001,d:IN0001,n:234*60D\$NRNRM,2,1,00001E1F,00000023,R*1632<CR><LF>
```

or if unsuccessful operation

```
\s:NR0001,d:IN0001,n:234*6D\$NRNAK,IN,NRM,NR0001,2,Unvalid
setting*3216<CR><LF>
```

or if a bad checksum in the TAG block or any TAG block in a grouped TAG block

```
\s:NR0001,d:IN0001,n:234*60D\$NRNAK,IN,NRM,NR0001,6,Checksum failure in TAG
Block*7C58<CR><LF>
```

or if a bad checksum in the sentence or any sentence in a TAG block group of sentences

```
\s:NR0001,d:IN0001,n:234*60D\$NRNAK,IN,NRM,NR0001,6,Checksum failure in
sentence*462<CR><LF>
```

C.5.3 Alert handling

Figure C.2 shows the two main states N and A that the sensor device can be in with respect to alerts.

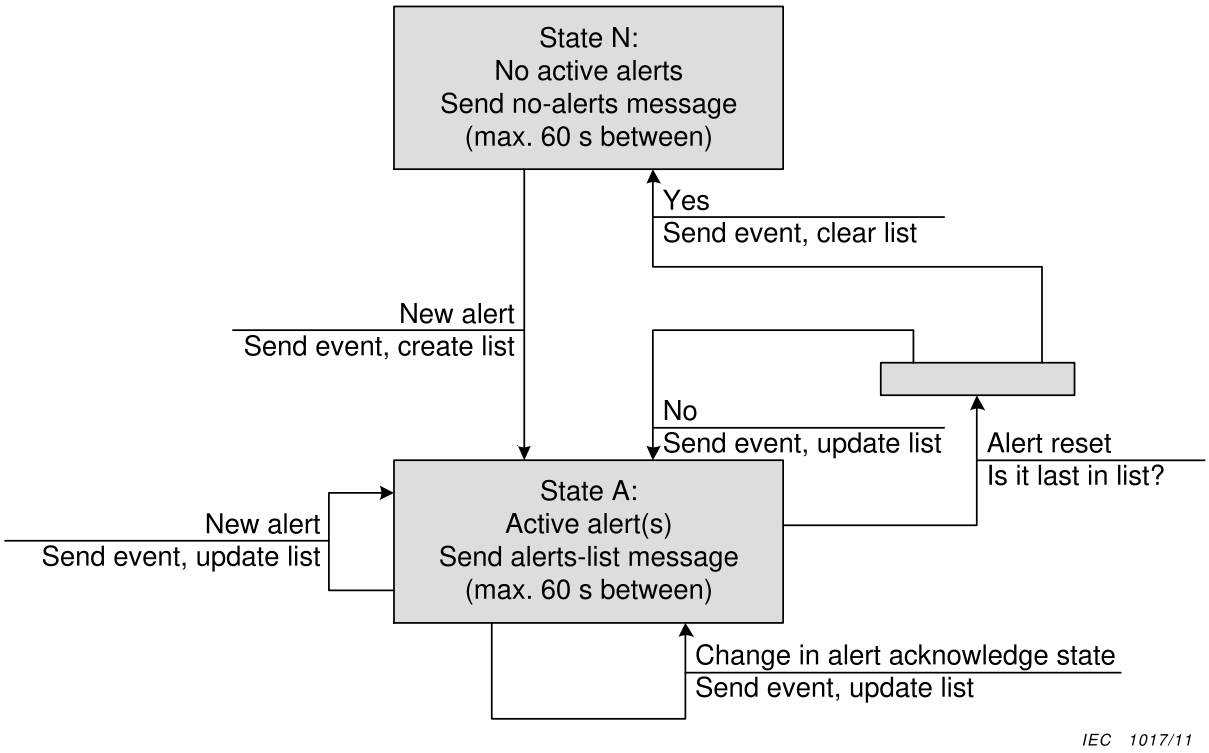

Figure C.2 – State diagram

The sensor device has two main states:

- *State N:* No active alerts. The device shall send a “no-alerts” message (see below) with a period not exceeding 60 s.
- *State A:* The device has one or more active alerts, of which zero or more may be acknowledged and the rest (possibly zero) are unacknowledged. In this state, the device shall send all active alerts with a period not exceeding 60 s. When multiple alerts are active in the device, it is recommended to transmit all active alerts as “a list” of alerts (alert-list message).

In addition to the periodic transmissions as mentioned above, the device shall immediately send an Alert message (ALR sentence), when (Values for alert condition and acknowledge state in parenthesis):

- a new alert is raised in the device – (A,V);
- an existing alert is acknowledged in the device (either on the device itself or by remote acknowledgement) – (A,A);
- an existing alert condition becomes non-active (V,V or V,A).

The alert message may include the time stamp when the alert last changed status (normally current time) and include the alert number, explanatory text as well as appropriate alert and acknowledgement flags. It may optionally be followed by a TXT message to give additional contextual information. The TXT message should be contiguous with its associated ALR. An example is included below.

```
\g:1-3-14,s:YX0001,d:BN0001,n:321*08\$YXALR,123456,906,A,V,Sensor
    fault*05<CR><LF>
\g:2-3-14,n:322*12\$YXTXT,02,01,06,Selftest error 17*2C<CR><LF>
\g:3-3-14,n:323*12\$YXTXT,02,02,06,See service manual*4F<CR><LF>
```

NOTE 1 This specification does not put any restrictions on the transitions that are reported through an event message. Thus, receivers should be prepared to receive and process all possible combinations and sequences of alert state events.

NOTE 2 The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.5.4 No-alerts message

The *no-alerts* message shall be sent to inform that the device has no active alerts. It shall be repeated with a period not exceeding 60 s. This message may be used to clear the receiver's alert list.

This message is sent as an ALR message, but without time stamp, and shall include a 'V' flag in both the alert condition and acknowledgement field. The *no-alerts* (list empty) message is included below.

```
\s:YX0001,d:BN0001,n:456*79\$YXALR,,,V,V,*5672
```

NOTE The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.5.5 Alerts-list message

The alert/alert-list message shall be sent to periodically refresh the alert list so that the listener can verify that it has the correct internal list of active alerts. This will, in turn, help to remedy problems that may occur due to lost datagrams at earlier stage, synchronization of recently added receivers, etc.

The alert/ alert-list message shall be repeated with a period not to exceed 60 s, if any alerts are active.

The alert/ alert-list message consists of the same message(s) sent when the corresponding event occurred, but all active alerts shall be reported, and preferably with no delay between messages. An example with two messages in the list is included below:

```
\s:YX0001,d:BN0001,n:567*7A\$YXALR,123456,123,A,A,Battery power in
    use*1733<CR><LF>
\s:YX0001,d:BN0001,n:568*75\$YXALR,130507,456,A,V,Self test
    failure*3C18<CR><LF>
```

NOTE 1 The time stamp will wrap around after 24 h. For alerts that are active longer than 24 h, the receivers will need to keep track of the original event time.

NOTE 2 The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.6 Alert acknowledgement

C.6.1 General principles

If the alert handling device has a bi-directional data link to the sensor device, it is possible to send remote acknowledgements to alerts (ACK sentence) based on user action, e.g., through an acknowledgement button. This means that one can leave the resolution of potentially lost acknowledgement or alert status messages to the user. The user should note that the acknowledgement was not effected and, if necessary, repeat the acknowledgement at the local or remote station.

C.6.2 Alert acknowledgement

If alert acknowledgement is implemented, exactly one acknowledgement message shall be sent each time the operator initiates an acknowledgement.

```
\s:BN0001,d:YX0001,n:123*7E\$BNACK,xxxx234*hh5C<CR><LF>
```

C.6.3 Alarm acknowledge capability

In some cases, the sensor device needs to know if the alert handling device is able to communicate with it. This may, for example be used to implement silent alerts on the sensor device.

In this case, it is necessary to send an empty alarm acknowledge message from the external alert handling device to the device at regular intervals. The message should be sent at an interval not to exceed 60 s.

```
\s:BN0001,d:YX0001,n:123*7E\$BNACK,*~~4D~~69<CR><LF>
```

The alert handling device shall not send any messages, including heartbeat, if the empty acknowledgement message from the sensor device has not been received in a period of maximum 130 s. This time shall be reduced appropriately if the specified repetition interval is shorter.

Annex D
(informative)

Network and system design guidance

D.1 General

This informative annex provides guidance on network and system design.

The purpose of this annex is to provide some guidelines as to how a ship system can be made safer and more maintainable. Safety does in particular address the needs of a system that should be continuously available or at least degrade in a manner that retains some minimum functionality for the operator.

D.2 Security

D.2.1 Connections to external networks and systems

D.2.1.1 General

In general one can look at the ship network as a black (here, white) box that has a number of interfaces to systems outside the network (hashed). The interfaces will normally have to be implemented so that they provide some form of “isolation” to avoid problems propagating from one system to another (dark gray boxes). This is illustrated in Figure D.1.

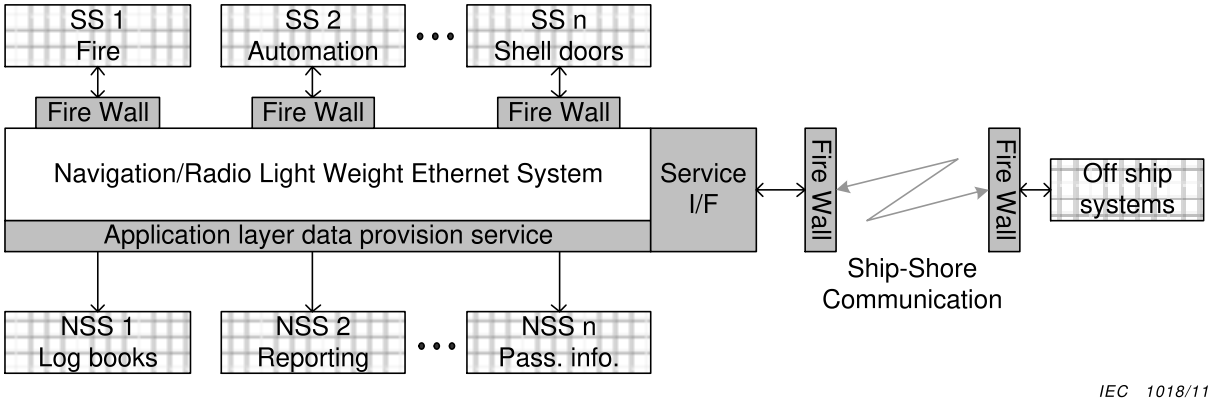

Figure D.1 – General system design architecture

One can define three different types of interfaces as follows.

a) Non-navigational data transfers in the navigational network (SS n), for example shell door status. These need some form of fire wall to be interfaced to the network.

b) Inter-system data transfers such as navigational data communications with other systems on the ship (NSS n). This may be interfaces for electronic log books, reporting systems or passenger information systems. One possibility here would be to define an application layer data provision service that also acts as a fire wall between external systems and the network.

c) Off-ship data transfers such as an interface to a ship management service or remote maintenance functions over a ship/shore data link. This is also a potential security and safety risk for the navigational services as it can change the functionality of the integrated bridge system. Thus, a number of fire walls will normally be needed.

D.2.1.2 Non-navigational data transfers

For the systems labelled SS in Figure D.1, an additional problem is that these systems have their own regulatory requirements that, in general, preclude direct connection between these systems and any other network on the ship.

D.2.1.3 Inter-system data transfers

For inter-system data transfers the easiest way to implement the required services is probably through an application layer firewall that connects the navigation network to a “public” on board network that also can provide a link to the satellite terminal. The details of the functions of this firewall depend on the general topology of ship networks and how different external systems can connect to the firewall.

D.2.1.4 Ship to shore data transfers

For connection to shore one could use VPN (Virtual Private Network) or similar technology to make sure that only authorized users get access to the system and that nobody can interfere when such access has been established. An example topology is shown below. Here, VPN is used in combination with application level fire walls.

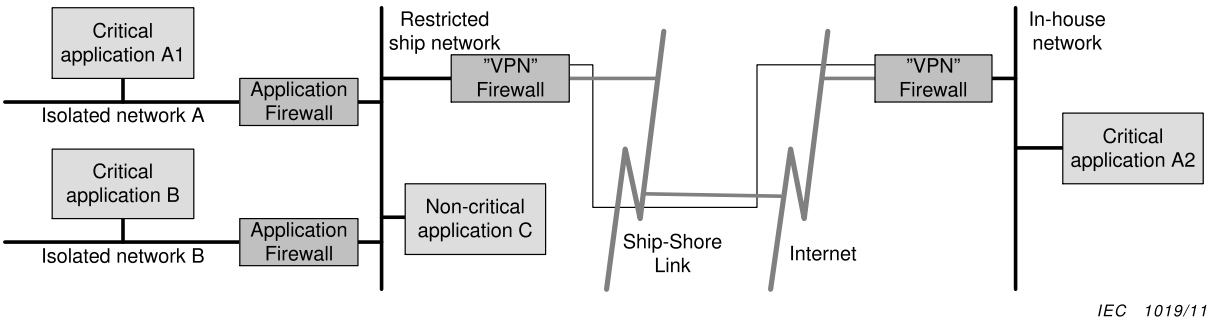

Figure D.2 – Example of ship-shore communication architecture

Ship operators are understandably concerned about security whenever the topic of internetworking ships navigation and control systems is raised. However, they tend to ignore the reality that bridge systems are often already connected by the “sneakernet” meaning that a memory stick or some other storage device is manually fitted into the bridge system to transfer data from a non-secured PC. This approach is extremely high-risk and potentially exposes the bridge system to all of the potential threats of the Internet and yet there are no protocols in place to protect these vulnerable systems from such threats.

A shipboard security architecture should comply with information security industry’s best practices, based on the following general principles:

- security and attack mitigation based on policy;
- security implementation throughout the infrastructure (not just on specialized devices);
- secure management and reporting;
- authentication and authorization of users and administrators to critical resources;
- intrusion detection for critical resources and subnets.

Implementation of these principles requires a layered approach to security “in-depth” which includes

- perimeter firewall(s) and intrusion detection,
- no Internet access permitted by any sensitive system,
- no non-encrypted Internet access by any Navigation System device (only VPN traffic),

- high security policy implementations on all sensitive nodes.

Figure D.3 shows how these principles can be realised onboard a ship.

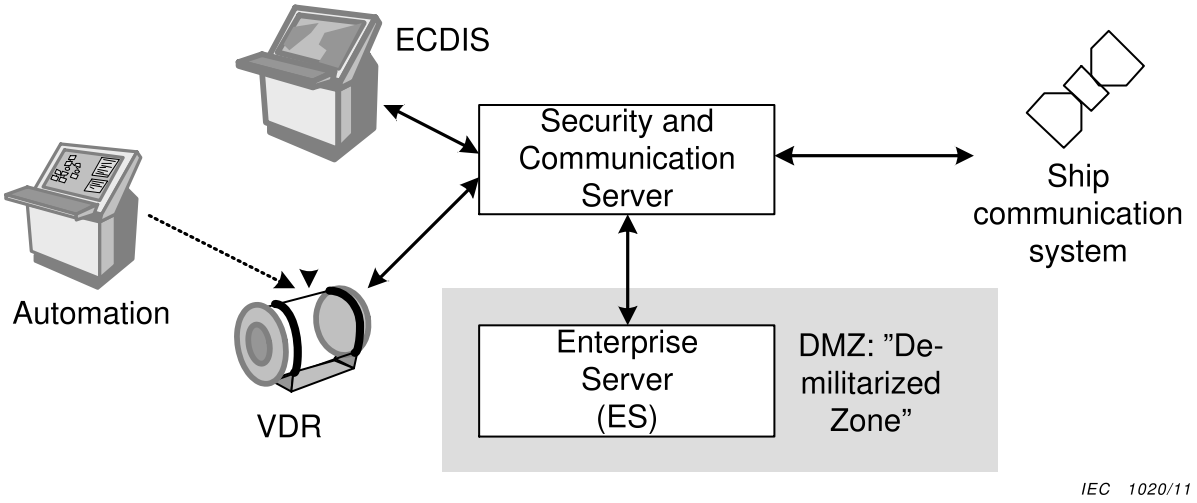

Figure D.3 – Security infrastructure

The Security and Communications Server isolates shipboard navigation and automation systems (safety dependent systems) from unsecured equipment. It also secures traffic from the shipboard enterprise server (trusted-software components) to the Internet and vice versa.

D.2.2 Physical isolation of network and equipment

This standard assumes that the physical network is only available to authorised persons and that it is not possible to tamper with the network through direct access to it. The network designer needs to take special precautions where equipment is placed so that general crew or passengers do not have access to it. This will also mean that these persons should not get access to the network through the equipment or by removing the equipment and getting access directly to the network cable.

D.2.3 Security mechanisms

The security should be supported by all or some of the network nodes except hubs since these simply relay the physical signals and do not perform any processing. At least one of the following security functions should be provided in the network.

a) Device Authentication: Device authentication is a mechanism to verify that all devices connected to the network are authorized devices. If the device is not authorized, the device is not allowed to access network. So, all devices should be registered and pre-authorized before it starts the communication.

b) Rate Control: Rate control is the mechanism to control the incoming/outgoing traffic volume at the network nodes including devices. Each node can limit the incoming/outgoing traffic rate for each network interface. So, each node configures the incoming/outgoing traffic rate based on the estimation of the maximum network traffic. For example, when a switch configures an Ethernet interface with incoming traffic rate with 1 Mbps, it can receive at most a maximum of 1 Mbps with the interface. This is very useful to protect the network from the worm virus attacks or the malicious network attacks such as flooding attacks. Since those attacks generate huge volume of the network traffic, the network and devices can easily be saturated or malfunctioned.

c) Firewall: A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. Firewalls are frequently used to prevent unauthorized Internet users from accessing

private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

d) Intrusion protection system (IPS): Any connection to the internet can be subject to attack from outsiders in an attempt to gain unauthorized access to the systems. An Intrusion Protection System (IPS) goes beyond scanning for viruses or malware and looks directly at traffic behaviour. If an attacker is attempting to gain access to the network through known hacking behaviour, the IPS system will immediately shut them down while allowing legitimate traffic to pass uninterrupted.

The security functions and the locations that will provide these functions are summarised in Table D.1.

Table D.1 – Overview of possible security functions

Security functions	Location	Security level	Mechanisms
Device authentication	Switch and Gateway	Low	MAC/IP address filtering Smart card/ Hardware-based authentication Device certificate IEEE 802.1x
Rate control	Switch (and Gateway)	Low	Per interface Per traffic class Per traffic stream
Firewall	Switch and Gateway	Medium	Packet filtering Application gateway Circuit-level gateway Proxy server
Intrusion protection system	Gateway	High	

D.3 Safety and redundancy

D.3.1 Overview

Many ship systems, among them navigation, need a high degree of availability. The following objectives are defined.

- Redundancy: Functions that rely on communication between equipment will need more than one communication path.
- Fail to silent: Faults in a network should only affect connected equipment's ability to communicate with other equipment. Fault handling shall allow equipment that is not directly affected by the fault to continue to operate to the degree that lack of communication allows. This can be achieved by a switch rate control mechanism that can limit traffic from malfunctioning equipment.
- Avoid fault propagation: The network should, as far as possible, be designed to not propagate consequences of a failure from one part of the network to another. This also applies to faults occurring in one equipment that may threaten the whole system, for example equipment that transmits to other equipment with high volume garbage traffic. This can also be achieved by a switch rate control mechanism that can limit traffic from malfunctioning equipment.

D.3.2 IGMP snooping

For a network to work with IGMP snooping, all equipment in the network will need to incorporate the same version of IGMP. It is very unlikely that this can be achieved in a

shipborne network over the lifetime of a ship as equipment is changed and maintained. This standard requires therefore that IGMP snooping is disabled and the network documentation should provide this information.

D.3.3 Redundancy

For ships, the most common approach is to design the complete system so that no single fault or no likely combination of faults shall render critical functions unavailable. To achieve this, one will normally duplicate the necessary components and the communication paths between them or provide fall back modes of operation. A simple example of duplication is provided in Figure D.4.

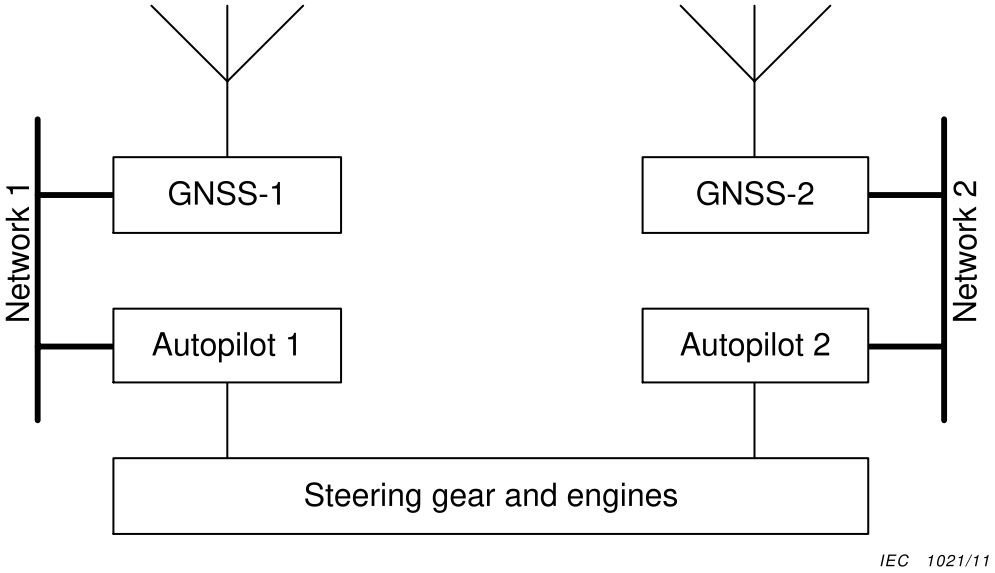

Figure D.4 – Decoupled system

This system will probably rely on some form of manual switch-over between the two autopilots so that the two networks are totally segregated and there is no possibility for any faults in one sub-system to propagate to the other.

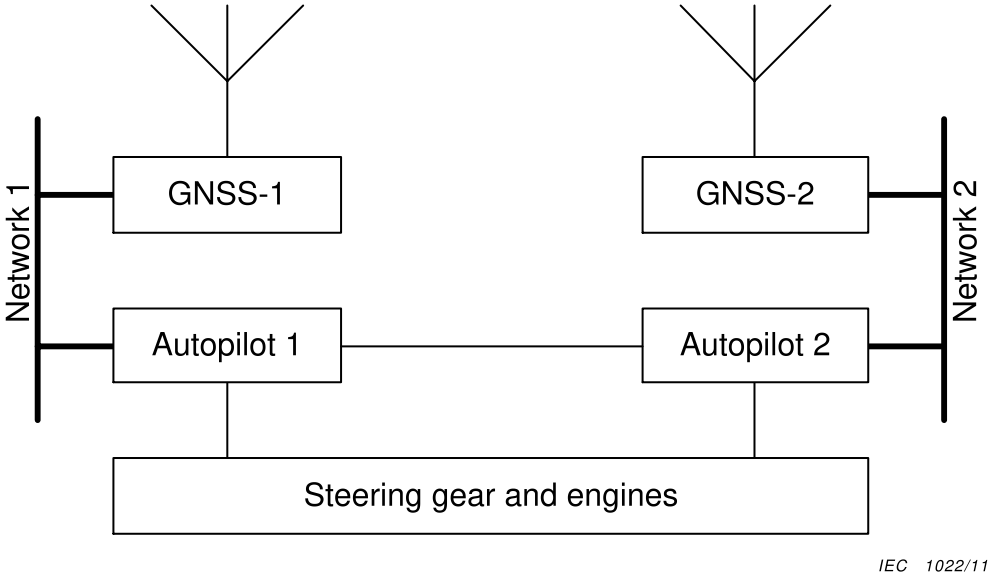

Figure D.5 – Loosely coupled system

A slightly more complex example is shown in Figure D.5 where an automatic coordination function via a digital communication link has been added. This has benefits in automatic, continuous and faster switch-over when problems are detected.

However, in this case there is a possibility that a failure mode in network 1 propagates to autopilot 2 through this data link. One may also conceivably get new common failure modes, triggered by the same event, in the two autopilots. These possibilities are normally low and can in most cases be disregarded if the two communicating devices have been properly designed.

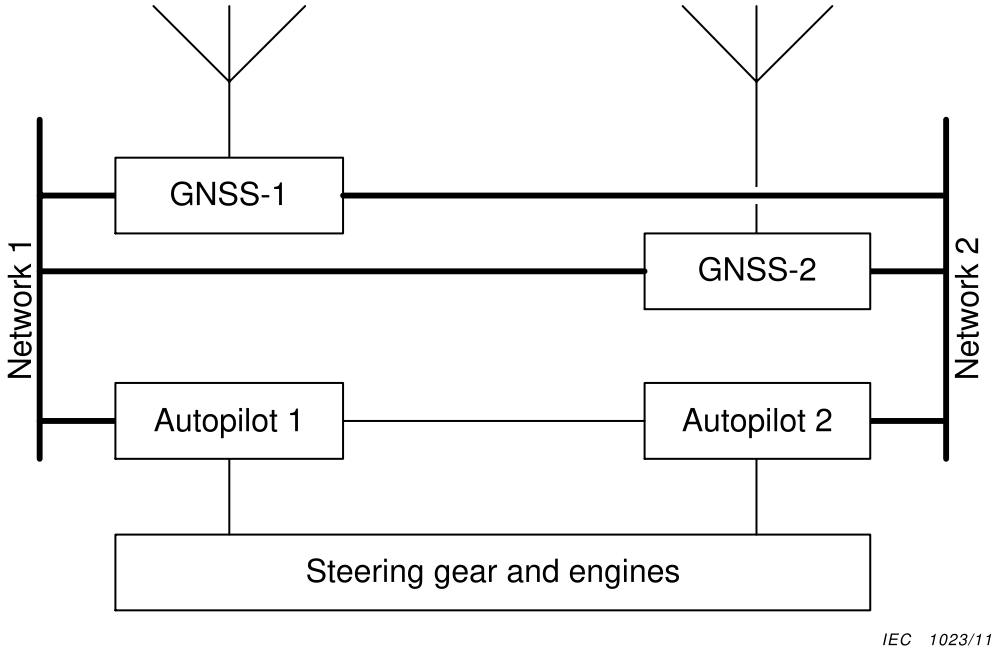

Figure D.6 – Strongly coupled system

One can consider the alternate system design in Figure D.6. At the cost of duplicated connections from each GNSS to both networks, this system provides much higher availability in that it can tolerate both a single general network fault as well as a fault in one of the GNSS receivers before functionality is degraded. Also, the coupling of sensor data allows new integrated navigation system functions to be implemented where one can increase the integrity of the position fix data.

However, this also adds new failure propagation possibilities, through each GNSS, from one network to the other. Also, a new common failure mode possibility is added in that each of the GNSS may have a failure mode where it overloads both networks, rendering the complete system without the autopilot function. On the other hand, failure modes associated with wrong data from each GNSS can be avoided as better integrity and data checks easily can be implemented.

As has been shown, there are important benefits to be had through coupling between the two networks, but this coupling provides the possibilities for new failure modes. The provisions of this standard allows for decoupled redundant systems to be designed with little or no system level analysis beyond that which is performed through equipment documentation and tests. This may also apply to loosely coupled systems, but in this case the designer of equipment that is connected together may need to prove that this coupling does not pose any problem in relationship to common mode failures in networks.

For strongly coupled systems, a system design review will normally have to be performed to identify any potential failure modes, their effects and criticality and measures to remedy any problems.

D.3.4 Failure propagation through a network

In addition to having some failure modes associated with its communication function, the network may also propagate failures from the network itself or other nodes. Table D.2 shows the most important types of such failure modes.

Table D.2 – Network failure propagation possibilities

Failure mode	Cause	Probability	Criticality
Network overload	General network traffic may overload listening nodes	Medium	High
Denial of service	One node may overload a single other node by excessive service requests or general garbage data.	Medium	High
Broadcast storms	Network devices fail in such a way as to overload nodes with garbage or duplicated real messages.	Low	High

An analysis of the traffic patterns and network load needs to be performed which may have various forms as follows.

- A receiver cannot process as many input messages as it gets, due, for example to too many senders being able to address this receiver. This can be analysed off-line by using equipment specifications and comparing these with each other. Note in particular that this standard uses multicast where several different senders can send messages to the same receiver.
- A network to serial line gateway has a special problem in that it is constrained to a maximum output rate given by the serial line capacity. This problem has been catered for in this standard in the equipment requirements for this type of device. Note however, that overload will make the gateway discard some messages.
- Hostile denial of service attacks may occur through an external gateway. This is discussed in D.2.3.
- Other forms of denial of service may occur due to equipment failures or errors in configuration. This has a relatively low probability and can normally be discarded for tested and approved equipment.

D.3.5 Non IEC 61162-450 equipment connected to a network

Other uses of the Ethernet network is allowed based on rules set for ONF (Other Network Function) specified in this standard (see 4.6).

D.4 Maintenance and manageability

D.4.1 Maintainability

One important aspect of safety is the time needed to repair a fault. The “single fault tolerance” principle is based on the ability to make corrective actions before a new fault occurs. Also, the issue of fault avoidance through problem detection and early repair is important.

D.4.2 System and management functionality

This standard contains no direct requirements to system management functions. However, early detection of problems and determining where the problems originate from is important for maintaining networked navigation systems.

Some of the possibilities that can be considered to simplify management of networked systems are the following.

- If the network has a firewall to outside networks, this node can also be used to collect statistics and error messages from the other nodes on the network. This can then be made

available to crew or to service personnel. Any other node can also be assigned this function, but the firewall function will also enable easy transfer to external systems.

- The heartbeat sentence can be used to collect some information from the nodes. One may also listen to other sentences when this gives system state information.
- Management protocols like SNMP (Simple Network Management Protocol) can be used to report additional information both from network nodes and network equipment like switches. This requires SNMP support in the relevant nodes.
- One may also use functionality in ICMP (Internet Control Message Protocol) to check if nodes are available. All nodes should be able to process, for example ping requests.

Finally, one should also consider the use of other protocols to facilitate for example time coordination in the system. The most common protocol for this is NTP (Network Time Protocol).

D.4.3 System and network integrator

In modern practice, after delivery of a ship from a shipyard, there is no system integrator or ship-board responsibility for network system, security and maintenance. This needs to be taken into account in network and system design.

Bibliography

IEC 60603-7, *Connectors for electronic equipment – Part 7: Detail specification for 8-way, unshielded, free and fixed connectors*

IEC 60603-7-3, *Connectors for electronic equipment – Part 7-3: Detail specification for 8-way, shielded, free and fixed connectors, for data transmission with frequencies up to 100 MHz*

IEC 60603-7-7, *Connectors for electronic equipment – Part 7-7: Detail specification for 8-way, shielded, free and fixed connectors for data transmission with frequencies up to 600 MHz*

IEC 61076-2-101, *Connectors for electronic equipment – Product requirements – Part 2-101: Circular connectors – Detail specification for M12 connectors with screw-locking*

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

IEC 61162-3, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 3: Serial data instrument network*

IEC 61174, *Maritime navigation and radiocommunication equipment and systems – Electronic chart display and information system (ECDIS) – Operational and performance requirements, methods of testing and required test results*

IEC 61754-20, *Fibre optic connector interfaces – Part 20: Type LC connector family*

~~IEC 61996-1, *Maritime navigation and radiocommunication equipment and systems – Shipborne voyage data recorder (VDR) – Part 1: Voyage data recorder (VDR) – Performance requirements – Methods of testing and required test results*~~

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

ISO/IEC 11801:1995, *Information technology – Generic cabling for customer premises*

ISOC RFC 826:1982, *Ethernet Address Resolution Protocol (ARP), Standard STD0037 (and updates)*

ISOC RFC 894:1984, *A Standard for the Transmission of IP Datagrams over Ethernet Network , Standard STD0041 (and updates)*

ISOC RFC 1112:1989, *Host Extensions for IP Multicasting, Standard STD0005 (and updates)*

ISOC RFC 1122:1989, *Requirements for Internet Hosts – Communication Layers, Standard STD0003*

ISOC RFC 2365, *Administratively Scoped IP Multicast, Best Current Practice BCP0023*

ISOC RFC 3232:2002, *Assigned Numbers: RFC 1700 is Replaced by an On-line Database*

ISOC RFC 4288, *Media Type Specifications and Registration Procedures*

ISOC RFC 4289, *Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures*

IMO resolution MSC.252(83), *Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS)*

TIA/EIA-568-A:1995, *Commercial Building Wiring Standard*

TIA/EIA-604-10-A:2002, *FOCIS10 – Fibre Optic Connector Intermatebility Standard, Type LC*

_____

IEC 61162-450

Edition 1.1 2016-03

FINAL VERSION

Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

IEC 61162-450:2011-06+AMD1:2016-03 CSV(en)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

FOREWORD

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

This Consolidated version of IEC 61162-450 bears the edition number 1.1. It consists of the first edition (2011-06) [documents 80/615/FDIS and 80/621/RVD] and its amendment 1 (2016-03) [documents 80/795/FDIS and 80/796/RVD]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

International Standard IEC 61162-450 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems.

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

The committee has decided that the contents of the base publication and its amendment 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.

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 450: Multiple talkers and multiple listeners – Ethernet interconnection

1 Scope

This part of IEC 61162 specifies interface requirements and methods of test for high speed communication between shipboard navigation and radiocommunication equipment as well as between such systems and other ship systems that need to communicate with navigation and radio-communication equipment. This part of IEC 61162 is based on the application of an appropriate suite of existing international standards to provide a framework for implementing data transfer between devices on a shipboard Ethernet network.

This standard provides a higher speed and higher capacity alternative to the IEC 61162-1 and IEC 61162-2 standards while retaining these standards' basic data format. This standard provides a higher data capacity than IEC 61162-3.

This standard specifies an Ethernet based bus type network where any listener may receive messages from any sender with the following properties.

- This standard includes provisions for multicast distribution of information formatted according to IEC 61162-1, for example position fixes and other measurements, as well as provisions for transmission of general data blocks (binary image), for example between radar and VDR.
- This standard is limited to protocols for equipment (Network nodes) connected to a single Ethernet network consisting only of OSI level one or two devices and cables (Network infrastructure).
- This standard provides requirements only for equipment interfaces. By specifying protocols for transmission of IEC 61162-1 sentences and general binary image data these requirements will guarantee interoperability between equipment implementing this standard as well as a certain level of safe behaviour of the equipment itself.
- This standard permits equipment using other protocols than those specified in this standard to share a network infrastructure provided that it is supplied with interfaces which satisfy the requirements described for ONF (see 4.6).
- This standard does not contain any system requirements other than the ones that can be inferred from the sum of individual equipment requirements. Thus, to ascertain system properties that cannot be derived from equipment requirements alone, additional analysis or standards will be required. In particular, this applies to requirements to maintain system functionality in the face of a single point failure in equipment or networks. Informative Annex D contains guidance on how to address such issues.

2 Normative references

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

IEC 60825-2, *Safety of laser products – Part 2: Safety of optical fibre communication systems (OFCS)*

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

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

IEC 61996-1, *Maritime navigation and radiocommunication equipment and systems – Shipborne voyage data recorder (VDR) – Part 1: Performance requirements, methods of testing and required test results*

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

ISOC RFC 768, *User Datagram Protocol, Standard STD0006*

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

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

ISOC RFC 826, *An ethernet Address Resolution Protocol*

ISOC RFC 1918, *Address Allocation for Private Internets, Best Current Practice BCP0005*

ISOC RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

ISOC RFC 5000, *Internet Official Protocol Standards, Standard 0001*

ISOC RFC 5227, *IPv4 Address Conflict Detection*

ISOC RFC 5424, *The Syslog Protocol*

NMEA 0183:2008, *Standard for interfacing marine electronic devices, Version 4.00*

NOTE The standards of the Internet Society (ISOC) are available on the IETF websites http://www.ietf.org. Later updates can be tracked at http://www.rfc-editor.org/rfcsearch.html

3 Terms and definitions

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

3.1
ASCII
printable 7 bit character encoded in one byte

3.2
binary image
data block without formatting known to this protocol, i.e., non IEC 61162-1 formatted data, that can be transmitted with the protocol defined in 7.3.

NOTE The term “binary image” is used to differentiate the general data transfer protocol (which may or may not be in ordinary text format) from the transmission of sentences that is always in 7 bit ASCII format.

3.3
byte
group of 8 bits treated as one unit; this corresponds to what is also sometimes called an octet

3.4
command-response pair
CRP
messages exchanged between parties that synchronize state changes on both sides through the exchange

NOTE 1 CRP are defined in Annex A.

NOTE 2 Both the command and the reply message may also be used as a sensor broadcast message in some cases. Thus, the implementation of the semantics of the message exchange is somewhat different between different users of the exchange.

3.5
datagram
one atomic UDP transmission unit on the Ethernet as defined in ISOC RFC 768 and as constrained elsewhere in this standard

3.6
Ethernet
a carrier sense, multiple access collision detect (CSMA/CD) local area network protocol standard as defined in IEEE 802.3 and later revisions and additions to IEEE 802

NOTE The types of Ethernet media that can be used for implementation of this standard are defined in Clause 5.

3.7
function block
specified functionality implemented by equipment

NOTE Equipment normally implements multiple function blocks. Requirements to equipment are the sum of requirements to the function blocks it implements. Function blocks are defined in Clause 4. Types of function blocks are System Function Block (SF), Other Network Function Block (ONF), Network Function Block (NF) and Serial to Network Gateway Function Block (SNGF).

3.8
internet assigned number authority
IANA
global coordination of the Domain Name Server (DNS) Root, IP addressing, and other Internet protocol resources, including UDP and TCP port numbers

NOTE The currently assigned numbers are listed in http://www.iana.org/assignments/port-numbers.

3.9
internet protocol
IP
used and defined in ISOC RFC 791 (and updates)

3.10
message
collection of one or more sentences that are grouped by mechanisms internal to the sentence, for instance by sequence numbers as in the TXT sentence, i.e. a stand alone sentence is a message

3.11
message type
classification of IEC 61162-1 sentence formatters into SBM, MSM and CRP types

NOTE 1 SBM, MSM and CRP types are defined in Annex A.

NOTE 2 This standard defines different requirements to the transmission of different message types.

3.12
multi-sentence messages
MSM
logical group of messages and/or sentences where the full meaning of the group is dependent on the receiver reading the full group

NOTE 1 Multi-sentence messages that are grouped together with a TAG construct is also a sentence group.

NOTE 2 MSM are defined in Annex A.

3.13
network
one physical Ethernet network with one Internet address space, consisting only of the network nodes, switches, cables and supporting equipment such as power supply units

3.14
network function block
NF
function block responsible for physical connectivity to the network and connectivity to the transport layer as described in 4.3

3.15
network infrastructure
the part of the Network that provides a transmission path between network nodes

NOTE The network nodes are not part of the network infrastructure.

3.16
network node
physical device connected to the network and which have an Internet address (also called an Internet host)

NOTE A network node will normally correspond to equipment as the latter term is used in this standard.

3.17
other network function block
ONF
function block that interfaces to the network, but which is not using the protocol definition in Clauses 5, 6 and 7 of this standard (for example real time streaming of Radar and CCTV image transfer, VDR sound transfer, etc.)

NOTE Requirements as defined in 4.6 ensure that an ONF can co-reside with SF network nodes and function blocks that make use of this standard's protocol.

3.18
sensor broadcast message
SBM
messages consisting of only one sentence

NOTE 1 SBM type messages are sent with a sufficiently high update rate to ensure that the receiver can maintain the correct status even in environments where some messages may be lost.

NOTE 2 SBM are defined in Annex A.

3.19
sentence
standard information carrying unit as defined in IEC 61162-1

3.20
sentence group
logical group of sentences (which may consist of only one) that need to be processed together to give full meaning to the information contained in the sentence(s)

NOTE 1 The grouping of sentences into sentence group is done by TAG block mechanisms. The sentences in a sentence group may or may not have the same formatter. A multi sentence message grouped by this mechanism is also a sentence group.

NOTE 2 This standard allows the explicit grouping of sentences by using coding in a datagram. This standard does not enforce any relationship between datagram and sentence group. Thus a datagram may contain more than one sentence group or a sentence group may be split over two or more datagrams.

3.21
serial to network gateway function block
SNGF
function block that enables transfer of sentences between the network and devices that are compliant with the IEC 61162-1 and IEC 61162-2 serial line interface

3.22
system function block
SF
function block, identified by a unique system function ID (SFI), that is the only function block that can send information in a datagram format as defined in clause 7

3.23
system function ID
SFI
parameter string as defined in 4.4.2

3.24
transmission group
a pair of a multicast address and a port number that are used by an SF to transmit sentences

NOTE The transmission groups are defined in Table 4 and Annex A defines default transmission groups for the SF.

3.25
transport annotate and group
TAG
formatted block of data, defined in NMEA 0183, that adds parameters to IEC 61162-1 sentences

NOTE Informative Annex B gives an overview of the TAG blocks used in this standard.

3.26
user datagram protocol
UDP
connection-less datagram protocol defined by ISOC RFC 768; it makes no provision for transport-layer acknowledgement of packets received

4 General network and equipment requirements

4.1 Network topology example

Figure 1 shows a possible IEC 61162-450 network topology consisting of one IP Local Area Network (LAN) and a number of different network nodes, each containing different function blocks. This diagram is informal and does not imply any requirements other than the ones defined in the following subclauses.

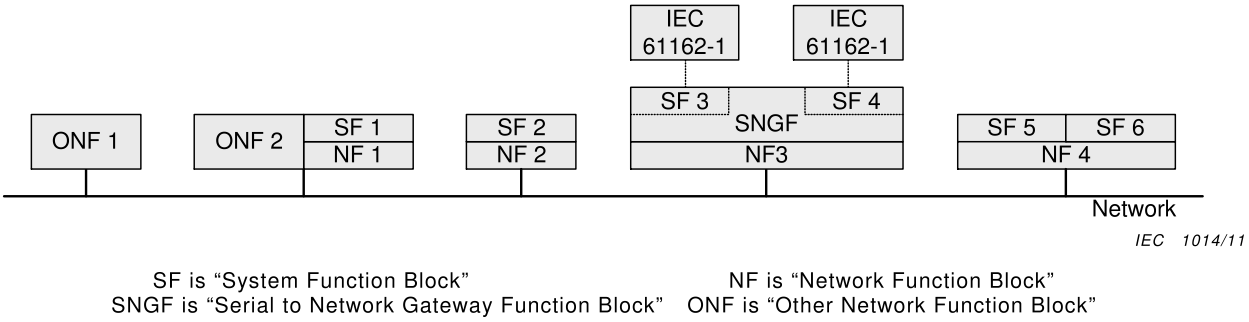

Figure 1 – Network topology example

Some examples of network nodes are (see Figure 1):

- a sensor, for example a GNSS receiver that is also a network node (SF2 and NF2).
- a device that sends or receives IEC 61162-450 compliant data (sentences and/or binary image) as well as other types of information onto the network, for example an ECDIS that can also load chart data from another device (SF1, ONF2 and NF1).
- two independent functions, such as a gyrocompass also approved as a rate of turn sensor that are implemented in one network node (SF5, SF6 and NF4).
- a system device function block represented by an IEC 61162-1 compliant equipment connected to a serial to network gateway function (SNGF). In this case, the SNGF will format outgoing sentences according to requirements in this standard (SF3, SF4, SNGF and NF3)
- a device that does not send or receive IEC 61162-450 compliant data (sentences and/or binary image), but which satisfies minimum requirements for compatible use of the same network (ONF1).

4.2 Basic requirements

4.2.1 Requirements for equipment to be connected to the network

(see 8.2.1)

The requirements for equipment connected to the network are as follows.

- All equipment connected to the network including network infrastructure equipment, shall satisfy the relevant physical and electrical requirements defined in 5.1.
- All equipment that implements one or more of SF and/or SNGF shall implement the NF. This equipment shall satisfy the requirements to the function blocks they implement as defined in 4.3 (NF), 4.4 (SF) and 4.5 (SNGF).
- All other equipment that is not network infrastructure equipment and that shares the network infrastructure shall comply with requirements to an ONF as defined in 4.6.
- Network infrastructure equipment, i.e., switches, shall satisfy requirements in 4.2.2.
- All equipment connected to a network shall satisfy the requirements of IEC 60945.

Any other equipment is not allowed to be connected to the network.

4.2.2 Additional requirements for network infrastructure equipment

(see 8.2.2)

The following requirements are included to avoid potential problems with certain network infrastructure equipment:

- routers and repeater hubs shall not be used to interconnect components of an IEC 61162-450 network;

- switches that are used to interconnect equipment compliant with IEC 61162-450 shall not implement multicast filtering techniques, such as IGMP snooping or CGMP.

NOTE 1 IGMP is Internet Group Management Protocol and CGMP is Cisco Group Management Protocol. If switches are capable of implementing multicast filtering techniques, then this functionality should be disabled.

NOTE 2 Routers are network infrastructure devices that can forward datagrams between networks. Repeater hubs are network infrastructure devices without internal storage that repeat incoming datagrams onto all outgoing connections. Switches are network infrastructure devices that based on forwarding tables can process, and forward *datagrams between nodes on the same network, using intermediate storage in the switch before retransmission*.

NOTE 3 Although multicast filtering techniques, such as IGMP snooping or CGMP, are not allowed to be activated, it is acceptable to manually configure individual ports of the switches to block unnecessary traffic flow (for example to isolate simple sensors from ECDIS and radar).

4.3 Network function (NF) requirements

4.3.1 General requirements

All equipment that implements a NF shall satisfy the requirements in Clauses 5 and 6.

4.3.2 Maximum data rate requirements

(see 8.3.1)

The manufacturer shall specify the maximum input rate under which the equipment can still perform all functions required by its performance standards.

Maximum input rate shall be specified as:

a) maximum number of datagrams per second received, intended for and processed by the equipment;

b) maximum number of datagrams per second received by but not intended for the equipment;

c) maximum number of datagrams per second received by, but not intended for, the equipment at 50 % of the maximum load for item a).

NOTE “Received by” means datagrams that are received on a transmission group that the equipment listens to. “Intended for” are datagrams that are processed by the equipment as part of its specified function.

The maximum data rates shall be the mean rate over a 10 s measurement period.

4.3.3 Error logging function

(see 8.3.2)

4.3.3.1 Internal logging

Means shall be provided in each NF to record errors that occur in the NF itself as well as SF and SNGF using it. Subclauses 4.5.2, 7.1.2, 7.2.5 and 7.3.9 give minimum requirements as to what shall be logged.

As a minimum, the manufacturer shall provide mechanisms by which error logs can be inspected by a human operator. It is allowed that the inspection is done through a simple network mechanism such as a terminal emulator, a datagram as defined in this standard or any other reasonable method.

The minimum requirements for the log are to count the number of each occurrence. The counter may reset itself by a manufacturer specified method.

4.3.3.2 External logging

A NF may be configured to support external logging, where non-trivial information is sent to a logging server. In this case a “syslog” message, as defined in ISOC RFC 5424, shall be used.

Syslog messages shall be formatted as ASCII text messages and sent as UDP packets on port 514 and the multicast address defined in Table 6. Error messages defined in this standard shall be reported through a simplified message as described in Table 1, where italicised words are place-holders for data explained in the right hand column. Other characters shall be transmitted as shown, including spaces.

Table 1 – Syslog message format

Element	Description
<pri>	The combined priority and facility code (number from 0 to 199 inclusive) enclosed in pointed brackets. For the errors defined in this standard, the value 131 shall be used (facility “local use 0” and priority “error condition”).
Version	The version code. The code 1 (one) shall be used for messages from this version of the standard.
Space	One space character.
Timestamp	Timestamp, containing date and time and optional UTC offset, in a valid format, for example 1985-04-12T23:20:50-03:00. The example shows date, followed by upper case “T”, then local time and finally offset from UTC (3 hours west – negative, east offsets shall be prefixed by a ‘+’. UTC offset can be abbreviated to a single upper case “Z”, without leading ‘-‘ or ‘+’). Alternatively, the timestamp field may be nil (‘-‘, a single dash character).
Space	One space character
Hostname	The host name of the network node, represented as the IP address in dotted decimal notation. Alternatively, this field may be nil (‘-‘, a single dash character).
Space	A space character
Appname	The application name. This shall be the string “450-“ followed by the configured SFI code if the error originates in the SF or SNGF, “NF” if the error originates from the network function block or “ONF” if it originates in the ONF function block.
Space	A space character
Procid	Normally, this field should be nil (‘-‘ a dash character). Other values as defined in the Syslog standard may be used.
Space	A space character
Msgid	For errors defined in this standard, this field shall be the error code as defined in Table 2.
Space	A space character
Structured	This field can be nil (‘-‘, a single dash character) or contain information as defined in ISOC RFC 5424.
Space	A space character
Msg	A free format message in ASCII format.

A ”syslog” packet shall not exceed 480 bytes and shall be sent as a single UDP datagram.

NOTE This standard does not specify requirements for equipment receiving syslog messages. This type of equipment would fall into the category of ONF. As the above specification is a subset of the full ISOC RFC 5424 specification, implementers of such equipment should refer to ISOC RFC 5424 and make sure that syslog messages from other ONF can be received and processed without problems.

To facilitate the use of the syslog protocol, the errors defined in this standard have been assigned a message identity as defined in Table 2.

Table 2 – Syslog error message codes

Message identity	Description	Sub-clause
101	SNGF buffer overflow	4.5.2
102	Datagram header error	7.1.2
103	TAG or sentence format error	7.2.5
104	Binary image error	7.3.9

Additional information can be given in the “Msg” field, if available.

4.4 System function (SF) requirements

4.4.1 General requirements

(see 8.4.1)

Equipment that implements an SF shall satisfy the following requirements:

- requirements in 6.2 shall be satisfied for all equipment implementing SF;
- requirements in 7.2 shall be satisfied for all equipment implementing IEC 61162-1 sentence transmitting or receiving function blocks;

  NOTE This also includes function blocks with the ability to send heartbeat (HBT) sentences.
- requirements in 7.3 shall be satisfied for equipment that implements an SF that can transmit or receive binary image data.

4.4.2 Assignment of unique system function ID (SFI)

(see 8.4.2)

The format of the SFI parameter string shall be “ccxxxx” where “cc” is two valid characters as defined in IEC 61162-1 and “xxxx” is four numeric characters.

An SF implementing the functionality of an equipment that has been given a talker mnemonic code in IEC 61162-1 shall use this talker mnemonic as the “cc” characters in the SFI.

NOTE Other SF may have their SFI string format defined in other standards or the manufacturer may have to choose a code. In the latter case, the already defined talker mnemonic codes should be avoided.

The numeric character string "xxxx" will be an instance number in the range "0000" to "9999" The numeric character string “9999” is reserved for an un-configured SF and shall not be used by any transmitting SF during normal operation. However, all receiving equipment shall accept the “9999” string.

During normal operation, the SFI parameter string shall be unique for all SF in an IEC 61162-450 network.

NOTE It is recommended that all SF on a ship, independent on whether they are residing on one common network or not, are given a ship unique SFI.

Means shall be provided by the manufacturer to configure the SFI for each SF (see 7.2.3.4).

4.4.3 Implementing configurable transmission groups

(see 8.4.3)

Each SF shall be assigned a single transmission group for all outgoing messages. The default for this transmission group is determined by the SFI as described in Annex A.

For each SF that the equipment implements, the manufacturer shall document the default transmission groups the SF listens to and what sentences it expects to receive on each group. The default transmission groups can be selected by the manufacturer from the list of groups in 6.2.2.

Means shall be provided to configure all transmission groups to another than the default. Only the transmission groups listed in 6.2.2 are allowed to be configured.

NOTE All transmission groups can be used for configuration, i.e., a system integrator may use, for instance the NAVD group also for non-navigational SFs, if desired. However, an overall load analysis of the network needs to take the actual configuration into consideration.

4.5 Serial to network gateway function (SNGF) requirements

4.5.1 General requirements

(see 8.5.1)

The SNGF shall implement all relevant functionality defined in 4.4 for each SF it supports.

Each serial port shall be implemented as a separate SF and assigned a separate SFI.

The default SFI shall use the talker mnemonic “SI”.

The SNGF may implement different types of filtering with regard to what serial line sentences are retransmitted as datagrams and what datagrams will result in a serial line sentence being sent. Any filtering methods shall be described in manufacturer’s documentation.

NOTE A typical filtering method would be to use the destination TAG ‘d' to determine what sentences in incoming datagrams are to be sent on the serial line.

4.5.2 Serial line output buffer management

(see 8.5.2)

An SNGF function block shall provide an independent buffer for each serial port it can send sentences onto. The manufacturer shall specify the maximum buffer capacity for each port. The maximum capacity may be configurable at installation.

The buffer shall be implemented as a FIFO (First In, First Out) buffer. In case of a full buffer, newly arrived sentences shall be discarded, unless these sentences are specified as prioritized (see below). Newly arrived sentences will be inserted into the buffer when buffer space is available. The method of treatment of sentences grouped by the TAG g (see 7.2.3.3) may be configurable or specified in the manufacturer’s documentation.

The SNGF may implement a priority-based functionality for some sentences with specified sentence formatters. The prioritised formatters may be configurable or specified in the manufacturer’s documentation.

Processing of prioritized sentences shall be as follows:

- only one sentence with identical talker ID and sentence formatter shall exist in the buffer;

NOTE When prioritizing AIS VDM and VDO sentences, the string beginning with the “!” character and ending with the 7th character of the encapsulation field should be used for comparison to identify identical sentences. A match of this string from a newly arrived sentence with one in the buffer means the sentence contains the same ITU-R M.1371 message from the same MMSI as the sentence already in the buffer, and can then replace the older sentence at its position in the queue.

- if a sentence, or a TAG block grouped sentences, with identical talker ID and sentence formatter exists in the buffer, the new sentence or sentences will replace the existing sentence at its position in the queue;

NOTE When prioritizing TAG block grouped sentences, several fields within the TAG block need to be compared as well as the sentence comparisons. All of the compared components should match those of the current TAG block group in order to the replace TAG block group in the queue. The components to compare are: The TAG block source parameter code value, the “number of lines” portion of the TAG block group parameter code, and the sentences within the TAG block group.

- otherwise, the new sentence shall follow the FIFO principle as described above.

If a sentence is discarded from the queue, this event shall be logged as an error internally in the equipment as defined in 4.3.3. The equipment shall have separate error counts for each serial port.

4.5.3 Datagram output requirements

(see 8.5.3)

The SNGF shall format outgoing datagrams as defined in 7.2.

The SNGF shall transmit one IEC 61162-1 sentence per outgoing IEC 61162-450 datagram to minimise delays.

4.6 Other network function (ONF) requirements

(see 8.6)

The ONF represents a function that is allowed to share the same network infrastructure as the network function blocks (NF) on an IEC 61162-450 network.

The ONF shall conform to the requirements given in 4.2.1.

The ONF equipment shall not use any IP multicast address reserved by this standard as defined in 5.4.

Documentation shall be provided describing the network protocols used by the ONF to send datagrams or byte steams for instance UDP, TCP/IP or other.

Documentation shall be provided demonstrating that the ONF cannot negatively impact the normal performance of the network or other equipment connected to the network.

5 Low level network requirements

5.1 Electrical and mechanical requirements

(see 8.7.1)

The cable and connectors used shall at least meet the specifications listed in Table 3 when used in protected environment as defined in IEC 60945.

The safety requirements and installation practices specified in IEEE 802.3, 14.7 and Clause 27 shall be followed. Also refer to IEEE 802.3, informative Annex 67.

Fibre optic interfaces shall comply with the laser safety requirements for Class 1 devices specified in IEC 60825-2.

Table 3 – Interfaces, connectors and cables

IEEE 802.3 Interface	Max network segment link distance	Mechanical device interface connector type (protected environment)	Pin assignment	Cable category, minimum
100BASE-TXS IEEE 802.3, 14.7 and Clauses 24 and 25	100 m	IEC 60603-7-3, 8-way shielded modular connector Refer to 802.3 Clause 3,IEC 60603-7 Figures 1 through 5 and IEEE 802.3/25	See b)	CAT5 STP Two shielded twisted pairs ANSI/ TIA/EIA-568-A:1995 and ISO/IEC 11801:1995 (Class D).
(not specified)	See a)	Terminal block	See b)	CAT5 STP Two shielded twisted pairs
100BASE-SX IEEE 802.3, Clauses 24 and 26	550 m	IEC 61754-20 LC type duplex optical connector. d)		Two multimode optical fibres Short wavelength 850 nm
1000BASE-T IEEE 802.3, Clause 40 (802.3ab)	100 m	IEC 60603-7-7, 8-way shielded modular connector Refer to 802.3 Clause 3 and IEC 60603-7 Figures 1 through 5. See IEEE 802.3/25	See c)	CAT5 STP Four shielded twisted pairs ANSI/ TIA/EIA-568-A:1995 and ISO/IEC 11801:1995 (Class D).
1000BASE-SX IEEE 802.3, Clause 38 (802.3z)	220 m (62/125 μm, low modal bw) 550 m (50/125 μm, high modal bw)	IEC 61754-20 LC type duplex optical connector. d)		Two multimode optical fibres Short wavelength 850 nm
For use in exposed environments, additional provisions are necessary. Consideration should be given to the M12-type specified in IEC 61076-2-101, Amendment 1 for copper network cable. And similar rugged connector for external fibre optic connectorization.				

a) In this case, the maximum operating distance should be specified by the manufacturer.

b) The 8-way modular connector specified in IEC 60603-7 is the “8P8C” type that has commonly been used in desktop computer LAN connections and incorrectly but widely referred to as “RJ45”. Wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack; the same at each end of a cable. The color-order from wire 1 to 7 shall be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown; the same at both ends of the cable. Refer to IEEE 802.3, 25.4.3 and IEC 60603-7-3.

c) The 8-way modular connector specified in IEC 60603-7 is the “8P8C” type that has commonly been used in desktop computer LAN connections and incorrectly but widely referred to as “RJ45”. Wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack; the same at each end of a cable. The color-order from wire 1 to 7 shall be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown; the same at both ends of the cable. Refer to IEEE 802.3, 40.8.1 and IEC 60603-7-7.

d) See TIA/EIA-604-10-A:2002.

5.2 Network protocol requirements

(see 8.7.2)

Equipment shall implement IP v4 as generally described in ISOC RFC 5000 with a minimum requirement of support for the following specific network protocols:

- ARP – Address Resolution Protocol as described in ISOC RFC 826 and as updated in ISOC RFC 5227;
- IP – Internet Protocol as described in ISOC RFC 791 and as updated in ISOC RFC 2474;
- UDP – User datagram Protocol as described in ISOC RFC 768;
- ICMP – Internet Control Message Protocol as described in ISOC RFC 792.

5.3 IP Address assignment for equipment

(see 8.7.3)

Means shall be provided to configure the equipment to an address in the range 172.16.0.1 to 172.31.255.254 (B type private addresses as described in ISOC RFC 1918) with a 16 bit network address mask. The assigned IP address shall remain fixed during normal operation of the equipment, including powering the equipment down and up.

5.4 Multicast address range

(see 8.7.4)

The range 239.192.0.1 to 239.192.0.64 is reserved for current and future use in the application layer protocols (see 6.2.2).

ONF equipment shall not use multicast addresses in the range 239.192.0.1 to 239.192.0.64.

NOTE ISOC RFC 2365 defines the multicast address range 239.192.0.0 to 239.192.63.255 as the IPv4 Organization Local Scope, and is the space from which an organization should allocate sub-ranges when defining scopes for private use. The specified range of IP multicast addresses map to Ethernet MAC addresses 01005E400001 to 01005E400040 (Hexadecimal).

6 Transport layer specification

(see 8.8)

6.1 General

This Clause specifies how UDP multicast messages are used to communicate between equipment over an Ethernet network.

Equipment may implement functionality for sending, receiving or both. The provisions in this Clause applies to both, but shall be tested independently as described in Clause 8.

An example of the structure of an Ethernet frame with a IEC 61162-450 sentence is given in Figure 2. The uppermost block shows the full Ethernet frame with the UDP user available data block shown in white. The IP and UDP headers are included in the grey blocks. The lower block shows the UDP user available data block with an IEC 61162-450 formatted sentence included. The numbers above the Ethernet frame gives the size of each block. The numbers in front of the UDP user data block gives the offset from the start of the block (0 – zero).

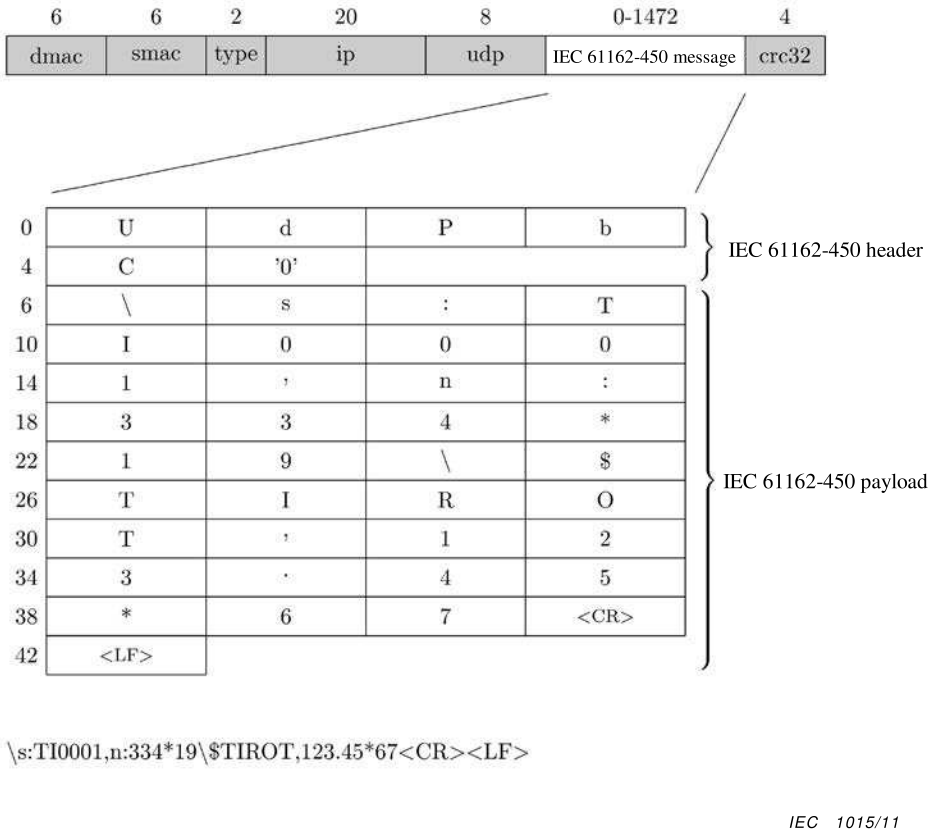

Figure 2 – Ethernet frame example for a SBM from a rate of turn sensor

6.2 UDP messages

6.2.1 UDP multicast protocol

Senders and receivers shall as a minimum be able to use the UDP protocol as defined by ISOC RFC 768 and as further specified in this standard.

6.2.2 Use of multicast addresses and port numbers

Port numbers shall be allocated from the Dynamic Port range that IANA has reserved for dynamic and/or private port numbers (range 49152 to 65535, inclusive).

Table 4 defines multicast addresses and destination port numbers that shall be used when transmitting sentences from a system function block. The mapping of SFI to default transmission group is described in Annex A.

NOTE The purpose of the port differentiation is to provide a mechanism that allows a certain level of load reduction for the receiving equipment.

Table 4 – Destination multicast addresses and port numbers

Transmission group	Category	Multicast address	Destination port
MISC	SF not explicitly listed below	239.192.0.1	60001
TGTD	Target data (AIS), tracked target messages (Radar)	239.192.0.2	60002
SATD	High update rate, for example ship heading, attitude data.	239.192.0.3	60003
NAVD	Navigational output other than that of TGTD and SATD groups	239.192.0.4	60004
VDRD	Data required for the VDR according to IEC 61996	239.192.0.5	60005
RCOM	Radio communication equipment	239.192.0.6	60006
TIME	Time transmitting equipment	239.192.0.7	60007
PROP	Proprietary and user specified SFs	239.192.0.8	60008
USR1 to USR8	User defined transmission group 1 to 8	239.192.0.9 to 239.192.0.16	60009 to 60016
NOTE The USR1 to USR8 transmission groups can be used, for example, for proprietary data in binary format.			

Table 5 defines multicast addresses and destination port numbers that shall be used when transmitting binary image data.

Table 5 – Destination multicast addresses and port numbers for binary data transfer

Category	Multicast address	Destination port
Simple Binary image transfer [a]	239.192.0.21 to 239.192.0.25	60021 to 60025
Re-transmittable binary image transfer [b]	239.192.0.26 to 239.192.0.30	60026 to 60030
[a] Address 239.192.0.25, port 60025 is the recommended default for ECDIS route transfer (see IEC 61174). [b] Address 239.192.0.26, port 60026 is the recommended default for VDR image transfer (see IEC 61996-1). Address 239.192.0.30, port 60030 is the recommended default for ECDIS re-transmittable data blocks for route transfer (see IEC 61174).		

Table 6 lists other multicast addresses and ports reserved by this standard.

Table 6 – Destination multicast addresses and port numbers for other services

Category	Multicast address	Destination port
Syslog	239.192.0.254	514

The addresses 239.192.0.17 to 239.192.0.20 and 239.192.0.31 to 239.192.0.64 are reserved for future expansion.

6.2.3 UDP checksum

All devices shall calculate and check the UDP checksum as defined by ISOC RFC 768. It is not permitted to set the checksum field to zero (no checksum).

A datagram that has an incorrect or missing checksum shall be discarded by the receiver.

6.2.4 Datagram size

The network function block shall not transmit more than 1 472 bytes of data in each datagram, including header as defined in Clause 7.

Receiving equipment is allowed to discard datagrams that have a size larger than the maximum specified size.

NOTE UDP datagrams can be up to 64 kByte in size when they are sent as a number of IP fragments.

7 Application layer specification

7.1 Datagram header

(see 8.9.2)

7.1.1 Valid header

All UDP multicast datagram shall contain one of the following strings, followed by a null character (all bits set to zero) as the first six bytes of the datagram:

- "UdPbC" for transmission of IEC 61162-1 formatted sentences as described in 7.2;
- "RaUdP" for transmission of binary images as described in 7.3;
- "RrUdP" for transmission of re-transmittable binary images as described in 7.3.

Incoming datagrams with an unknown header should be discarded without processing the content beyond the header.

NOTE Future editions of this standard may define other header codes. Any such header code will be different from the ones already in use and will at least contain six bytes, possibly including a trailing null character.

7.1.2 Error logging

The equipment shall maintain a count of received datagrams that do not have a valid header and make this available as defined in 4.3.3.

7.2 General IEC 61162-1 sentence transmissions

7.2.1 Application of this protocol

(see 8.9.1)

This protocol provides a mechanism by which IEC 61162-1 sentences can be sent to one or more receivers on the network. The protocol allows several sentences to be merged into one datagram.

7.2.2 Types of messages for which this protocol can be used

(see 8.9.3)

This protocol shall be used for SBM and MSM (see Annex A) type messages. The protocol shall also be used for CRP message exchanges with provisions specified in Annex C.

7.2.3 TAG block parameters for sentences transmitted in the datagram

(see 8.9.4)

7.2.3.1 Valid TAG block

Each sentence shall be preceded with one or more TAG blocks as defined in NMEA 0183 Section 7 (see also Annex B), containing the parameter codes described in the following

subclauses. If a parameter code is assigned a value more than once in the TAG blocks and only one value is expected, the last parameter value shall be used.

In this standard all identities are set at the time of installation and shall not be dynamically configurable during normal operation. The control sentences for changing parameter codes in NMEA 0183 shall not be used during normal operation.

7.2.3.2 TAG block checking

Only sentences preceded by valid TAG blocks as defined in 7.2.3.1 shall be processed by the receiver.

NOTE Receivers need to parse all TAG blocks and should ignore parameters that are not understood by the receiver. For the processing specified in this standard, only the last TAG block should be used.

7.2.3.3 Grouping control – g

The g parameter code shall be used by talkers to group TAG blocks and/or sentences. As a minimum it shall be used to group sentences that are classified as belonging to message type "MSM" in Table A.2, when the multi-sentence group consists of more than one message. It is not required to include the “g” parameter-code for single line sentences.

Receivers shall accept the g parameter code for all message types.

A valid MSM type sentence where internal data fields specifies that it belongs to a group of more than one message shall be discarded if the g group is missing or contains inconsistent information.

The group code is determined by the sending device. The initial group code value shall be one ("1") and the group code increment value shall be one ("1"). The group code shall be reset to one ("1") after it reaches 100, i.e., the valid range is 1-99, inclusive.

The following example shows the g parameter code used to group sentences in two different groups, each consisting of two sentences:

```
\g:1-2-34*59\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
\g:2-2-34*5A\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-46*5C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D
\g:2-2-46*5F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20
```

7.2.3.4 Source identification – s

The s parameter code is mandatory for talkers and shall contain the system function ID (SFI see 4.4.2) corresponding to the function block from where the sentence originates.

7.2.3.5 Destination identification – d

The d parameter code is optional and shall, if used, contain the system function ID (SFI see 4.4.2) corresponding to the intended recipient of the sentence.

Multiple d parameters may be specified, if more than one receiver exists.

NOTE This may be the case for redundant control functions.

For CRP type sentences, the destination code shall be read and processed to ensure that only the intended recipients take action on the content of the sentence. Other receivers may also read the message, for example for voyage data recording purposes, but shall not take any further action on the contents.

7.2.3.6 Line-count parameter – n

The n parameter code shall be used to assign a sequence number to each sentence transmitted from a system function block. The format of the parameter value is a positive integer. The value shall start at one ("1") and shall be incremented by one ("1") for each sentence or TAG block transmitted from this system function block. The parameter value shall be reset to one ("1") when it reaches 1000, i.e., the valid range is 1-999, inclusive.

For function blocks that transmit datagram to more than one transmission group destination, separate line counters shall be maintained for each transmission group (see 6.2.2).

7.2.3.7 Text string parameter – t (Proprietary data)

The t parameter code is a free text field. This standard reserves coding for proprietary TAG-codes with the fields defined below where the leading p and the three letter manufacturer mnemonic code is required for this type of text string.

```
t:p<manufacturer mnemonic code in lower case><proprietary data>
```

An example used for proprietary authentication of lines using grouping and source for manufacturer “mmm” might be

```
\g:1-2-34,s:TI0001,n:333*6B\$TIROT,123,45*67
\g:2-2-34,n:334,t:pmmma;MD5;0x12345678*74\
```

7.2.4 Requirements for processing incoming datagrams

Any syntax error in a TAG block or a sentence shall make the receiving equipment discard the complete datagram without any further processing.

7.2.5 Error logging

(see 8.10)

The equipment shall maintain counts of errors detected in processing datagrams containing IEC 61162-1 sentences or binary images. As a minimum, the following errors shall be counted and made available as defined in 4.3.3:

- any TAG block formatting errors as defined in 7.2.3.1;
- TAG checksum error;
- TAG syntax error (line length, use of delimiters, invalid characters);
- TAG framing error (incorrect start or termination of TAG block);
- any sentence syntax errors, including formatting, length or checksum as defined in 7.2.4.

7.3 Binary image transfer using UDP multicast

(see 8.11)

7.3.1 Application of this protocol

This protocol provides a mechanism by which non IEC 61162-1 formatted data, for instance radar images, can be transmitted to one or more receivers. This protocol supports the transmission of images from zero bytes up to 4 billion image blocks.

Equipment using this mechanism shall be able to use one or both of the following two forms of image transfer:

- non re-transmittable transfers where sender sends the complete binary image without any feed-back from receiver;

- re-transmittable transfers where limited feed-back from receiver can be used to re-transmit certain parts of the image.

Table 7 gives a description of terms used in this application.

Table 7 – Description of terms

Term	Description
DWORD	Double Word. One unsigned 32-bit integer (in range 0 to 4294967295). The DWORD is constructed from four consecutively transmitted BYTE, where the transmission order on the network is most significant BYTE first followed by next most significant BYTE till the least significant BYTE.
Null character	A BYTE with the value zero
Reserved bytes	A number of bytes in the datagram that may be ignored by the receiver. The reserved bytes may be additional header information that only has meaning for newer versions of the protocol or they may also be used for manufacturer specific purposes.
WORD	One unsigned 16-bit integer (in range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTE, where the transmission order on the network is the most significant BYTE followed by the least significant BYTE.
STRING[n]	A sequence of exactly n BYTE, interpreted as a string of characters. The transmission order on the network is left-most character first. If the string is shorter than n, additional trailing bytes shall be set to null character All strings in the header are encoded in ISO 18859-1 (ISO Latin 1).

7.3.2 Binary image structure

The binary images are transmitted over the network in one or more datagrams. The binary image structure is a sequential and unpadded stream of bytes divided into three main groups: Header; Binary image descriptor and Binary image data, see Table 8. The Header is needed for synchronisation and data integrity validation. The binary image descriptor is needed for the description of the binary image data and is only used in the first datagram for each image transfer.

Table 8 – Binary image structure

Header
Binary image descriptor (Only in first datagram)
Binary image data fragment
Header (zero or more)
Binary image data fragment (zero or more)

A minimum binary image transmission will consist of the three first blocks where the Binary image fragment may have zero length.

The Header shall be repeated as the first element of any datagram that contains Binary image data fragments.

7.3.3 Header

7.3.3.1 Header format

The purpose of the Header is to provide the data transfer status to receivers. This allows a receiver to identify if there is any data loss during image transfers, and how much data loss occurs. In addition, the Header is used to provide a re-transmission mechanism for re-transmittable image transfer.

The Header format is defined in the Table 9.

Table 9 – Header format

Data item	TYPE	Description
Token	STRING[6]	Identifier as ASCII string with a length of 5 bytes followed by a null character, see 7.1.1.
Version	WORD	Defines the header version. The header version with value 1 is defined in this standard. Extensions and/or modified versions may update this value
SrcID	STRING[6]	Define the source system identifier in format ”ccxxxx”, see 4.4.2.
DestID	STRING[6]	Define the destination system identifier In format “ccxxxx”, see 4.4.2. When Destid = ”XXXXXX”, then any device can be a destination.
Type	WORD	Identifies the information in the Header.
BlockID	DWORD	Binary image block identifier. The initial value is randomly generated within a range 0 to (2^{32} – 1 = 42949672950) and is incremented by 1 after a whole block is transmitted.
SequenceNum	DWORD	Defines the sequnce number of the binary image block. In ACK, this is used to inform the sender what block was last received.
MaxSequence	DWORD	The number of datagrams needed for the transmission of this image data block. When SequenceNum is equal to MaxSequence, it means that this datagram is the last datagram of the data block. The Maxseq is used only for DATA type message. For other messages (QUERY,ACK), this field shall be 0.

7.3.3.2 Use of header token

Header token is used to identify both the type of data block and transfer mode but shall not be used to accept or reject transmissions. Two tokens are defined in 7.1.1:

- “RaUdP” – Simple binary image transfer service with UDP;
- “RrUdP” – Re-transmittable binary image transfer service with UDP.

7.3.3.3 Version

Defines the header version. It shall be set to one for this edition of the standard.

7.3.3.4 Destination identifier

For transmissions to one specific receiver, the field shall contain the destination SFI. The field shall be “XXXXXX” otherwise.

7.3.3.5 Message type

Message type gives the information about which information is contained in the datagram:

- DATA (0x01) This type is used for transmission of binary image data including image descriptor.
- QUERY (0x02) This type is used by the sender to query the reception status from the receiver. The length of this message payload is always zero (0). It is recommended that an image sender sends a QUERY message if there is no ACK message for 1 s after a last datagram of the image block is sent or after a QUERY message is sent.
- ACK (0x03) This message is used as an acknowledgement from the receiver. This message is transmitted by the receiver either when a whole binary image is received without any error or when errors occurred during the binary image reception, for example one sequence number is skipped. Also, when a receiver receives a QUERY message from the sender, it also responds with an ACK message.

Non re-transmittable transfer makes use of only DATA message but re-transmittable transfer uses all messages.

7.3.3.6 Image block identifier

Block identifier is used to identify each image block. Since an image block is fragmented into several datagrams, the block identifier is used to assemble one or more datagrams into an image block in a receiver.

7.3.3.7 Sequence number and maximum sequence number

Sequence number (SequenceNum) and maximum sequence number (MaxSequence) is used for segmentation and re-assembly purposes. When a receiver gets a datagram, it checks the sequence number and maximum sequence number to determine if any errors have occurred or if it has received a whole message.

The sequence number is also used in ACK messages. In ACK messages, the sequence number identifies the last message the receiver receives without any error. The maximum sequence number is not used for control (Query) messages.

7.3.4 Binary image descriptor structure

The binary image descriptor format is defined in the Table 10.

Table 10 – Binary image descriptor format

Data item	TYPE	Description
Length	DWORD	Defines the binary image descriptor length in bytes. This is the length of the header as defined in this clause including the reserved bytes.
imageLength	DWORD	Defines the length of the full image content in bytes, excluding headers and descriptor.
Status of acquisition	WORD	The status for the data return. A zero is returned for normal operation. Non-zero value is used to indicate an error condition. A descriptive text may be put in the status and information text field
Device	BYTE	Data source (device) as binary value, 1 => equipment 1, 2 => equipment 2, etc. The value can be between 1 and 255
Channel	BYTE	Subdivision according to data source (device), values from 1 to 255, default = 1
TypeLength	BYTE	The length of the DataType field.
DataType	STRING[n]	This string defines the data block encoding by assigning a MIME content type to the data block for the server followed by null character. For example, “image/jpeg” is used for JPEG image type. The image quality shall comply with the image test of IEC 61996-1
Status and information text	STRING[n]	Status information (e.g. successful operation or error codes). This may be one or more strings, each terminated by a binary null
NOTE 1 There is no error check for the binary image header contents as this is handled by the UDP layer. In this specification, UDP header checksum is mandatory. NOTE 2 MIME is Multipart Internet Mail Extensions. The MIME content type was originally used for email services but is widely used for many other applications including Web. Also, it has flexibility to support new media types. The specification of the MIME content type and registration is defined in ISOC RFC 4288 and 4289.		

The Device and Channel fields are defined by the application and may be used by receivers to determine how to process the image data.

DataType shall be encoded by the MIME content-type which is “type/sub-type”, and is defined by IANA. Table 11 illustrates some examples of MIME content type for image and compressed data. More updated information is available on the IANA web site, http://www.iana.org/assignments/media-types/.

Table 11 – Examples of MIME content type for DataType codes

Content type	File extension	MIME type/sub-type
GIF	gif	Image/gif
Microsoft Windows bitmap	bmp	image/x-ms-bmp
Gnu tar format	gtar	application/x-gtar
4.3BSD tar format	tar	application/x-tar
DOS/PC – Pkzipped archive	zip	application/zip

7.3.5 Binary image data fragment

The package data format is defined in Table 12.

Table 12 – Binary image data fragment format

Data item	TYPE	Description
Datablock	BYTE[datalength]	This item is the data either split into pieces or in one block.

The length of the image fragment is the length of the UDP datagram (as obtained from the UDP header) minus any headers that are inserted in front of the image fragment. All datagrams except the first datagram of the image which requires two headers (Header + Image Descriptor), carry only one header (Header).

The image fragment length is allowed to be zero for one or more datagrams.

NOTE There is no error check for the data contents as this is handled by the UDP layer.

7.3.6 Sender process for binary image transfer

7.3.6.3 General

Each single binary image transfer shall be identified by a unique combination of SrcID and BlockID (see Table 9). Within the same SrcID, the Device and Channel (see Table 10) shall be used to distinguish between different data sources of binary image transfers.

NOTE If a single SrcID has multiple needs to send binary images (e.g. ECDIS sending screen image, chart source information and Route exchange), then each single binary image transfer is identified, for example: ECDIS number 1 send screen image as Device = 1 and Channel = 1, and Chart source information as Device = 1 and Channel = 2.

7.3.6.1 Non re-transmittable sender process

The following steps are performed for the basic sending process:

a) a sender process waits until it gets an image block including image descriptor;

b) a block identifier is assigned for the image block (if this is the first image, then it is assigned randomly. Otherwise, the instance identifier of the previous image block + 1 is used). The BlockID shall be unique for each binary image transfer from the same SrcID;

c) an image block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer;

d) get the first datagram of the image block;

e) assign a sequence number, which is assigned to one initially;

f) compose a header including token, source id, destination id and maximum sequence number;

g) send a datagram to the network;

h) if all datagrams of the image block are not transmitted, get a next datagram and go to Step (e);

i) otherwise, then go to Step (a).

7.3.6.2 Re-transmittable sender process

The sender processing steps for re-transmittable binary image transfer is as follows:

a) a sender process waits until it gets an image block including image descriptor;

b) a block identifier is assigned for the image block (if this is the first image, then it is assigned randomly. Otherwise, the block identifier of the previous image block + 1 is used). The BlockID shall be unique for each binary image transfer from the same SrcID;

c) an image block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer;

d) get the first datagram of the image block;

e) assign a sequence number, which is assigned to one initially;

f) set re-transmission counter zero(0);

g) compose a header including token, source id, destination id and maximum sequence number;

h) send a datagram to the network;

i) if the sender receives an ACK message, whose sequence number is less than the maximum sequence number,

- get a datagram whose sequence number is sequence number in ACK message plus one,
- increase re-transmission count by one,
- go to Step (g);

j) if all datagram of the image block is not transmitted,

- get a next datagram,
- go to Step (g);

k) otherwise,

- set a ACK timer,
- wait for an ACK message;

l) if the sender receives an ACK message whose sequence number is equal to the maximum sequence number, then go to Step (a);

m) if the sender receives an ACK message whose sequence number is less than the maximum sequence number, then go to Step (h);

n) if ACK Timer expires and re-transmission counter is less than three, then,

- increase the re-transmission counter,
- go to Step (j);

o) if ACK Timer expires and re-transmission counter is equal to three, then,

- clear the sending buffer,
- go to Step (a).

7.3.7 Receiver process for binary image transfer

7.3.7.3 General

Each single binary image transfer shall be identified by a unique combination of SrcID and BlockID (see Table 9). Within the same SrcID, the Device and Channel (see Table 10) shall be used to distinguish between different data sources of binary image transfers.

NOTE If a single SrcID has multiple needs to send binary images (e.g. ECDIS sending screen image, chart source information and Route exchange), then each single binary image transfer is identified, for example: ECDIS number 1 send screen image as Device = 1 and Channel = 1, and Chart source information as Device = 1 and Channel = 2.

7.3.7.1 Non re-transmittable receiver process

The receiver process steps of the non re-transmittable binary image transfer is as follows:

a) waits for receiving new datagram;
b) if the BlockID of the received datagram for same source identified by the combination of SrcID, Device and Channel is not equal to that of the previous datagram,
   - if there is any data in the receiver buffer, it is delivered to the SF,
   - the receiver buffer is cleared;
c) put a datagram into the receiver buffer;
d) if the sequence number is same as the maximum sequence number,
   - the all data in the received buffer is delivered to the SF,
   - the receiver buffer is cleared;
e) go to Step (a).

7.3.7.2 Re-transmittable receiver process

The re-transmittable receiver process steps are performed only by the receiver whose identifier is same as the DestID in the Header as follows:

a) waits for receiving new datagram;
b) if the received datagram is QUERY message then,
   - compose a Header with the BlockID and sequence number of the previous datagram,
   - send a datagram to the sender,
   - go to Step (a);
c) if the BlockID of the received datagram for same source identified by the combination of SrcID, Device and Channel is not equal to that of the previous datagram,
   - if there is any data in the receiver buffer, it is delivered to the SF,
   - the receiver buffer is cleared;
d) if the sequence number is not same as the sequence number of the previous datagram plus one, then,
   - compose a Header with the block identifier and sequence number of the previous datagram,
   - send a datagram to the sender,
   - go to Step (a);
e) put a datagram into the receiver buffer;
f) if the sequence number is same as the maximum sequence number,
   - all the data in the received buffer is delivered to the SF,
   - the receiver buffer is cleared;
g) go to Step (a).

7.3.8 Other requirements

7.3.8.1 Re-transmittable messages that cannot be processed

Both receiver and sender shall silently ignore messages that are related to the retransmit process that they cannot process themselves.

7.3.8.2 Multiple binary image blocks

A receiver that receives a binary image block more than once shall ignore all but one of the transmissions.

NOTE It is allowed both to ignore the first (overwrite buffer) or the last (ignore).

7.3.8.3 Retransmissions size

If a sender retransmits one or more binary image blocks, each of the blocks shall have the same size and same header information.

7.3.8.4 Maximum outgoing rate

The data volume for each binary image source shall not exceed 2 MBytes per second.

NOTE This provision is included to guarantee spare network capacity for other transmissions in between the blocks of a large binary image. When the image is transmitted as multicast it will flood the network and can inhibit transmissions of other data.

7.3.8.5 End of transmission

The receiver shall assume that a transmission has ended unsuccessfully when it gets a binary image block from same source identified by the combination of SrcID, Device and Channel (see Table 9 and Table 10) with a new BlockID. Then the receiver stops the current receiving process and becomes ready for the new image block receiving. The transmission shall also be considered finished when the last block is signalled by the SequenceNum from the sender. When a receiver gets the last block, then it sends an ACK message to the sender so as to start new image block transmission.

The sender shall assume that a transmission has ended unsuccessfully when it requires more than three re-transmissions of the binary image blocks including control messages. The sender assumes that the transmission is successfully finished only if it receives an ACK message with the SequenceNum which is equal to the MaxSequence. When a transmission is ended, a sender starts a new transmission if necessary.

7.3.8.6 Gaps between ACK messages

In general, a receiver shall, immediately after loss detection, transmit an ACK message to the sender if a binary image block has been lost either by having a gap in sequence numbers or by finding errors in the block. Since there is a time delay between the reception of the ACK message and re-transmission of lost data at the sender, a receiver waits for the sender's response. For this purpose, a receiver should wait at least 200 ms before it sends another ACK message. However, when a receiver receives all messages correctly, it shall send an ACK message immediately to the sender.

NOTE ACK message is used both for positive and negative acknowledge. See 7.3.3.5 for the description of the ACK message.

7.3.8.7 Maximum retransmissions

The maximum number of re-transmissions is limited for three times. If an image block requires more than three times re-transmission, the sender stops the transmission and starts a new image block transmission.

In addition to data message re-transmission, control messages can be re-transmitted in case the control message is lost. The re-transmission counter increases whenever the control message is transmitted.

7.3.8.8 Timer management

Re-transmission timer is managed at the sender. A sender sets the re-transmission timer when either a whole image block is transmitted and waits for an ACK message, or a control message (QUERY) message is transmitted. When the re-transmission timer expires, the sender (re-) transmits a QUERY message and sets the timer again unless the re-transmission counter reaches three.

7.3.8.9 UDP port and IP addresses

Multicast addresses and ports for the service type are given in Table 5. As a default, addresses for simple and re-transmittable imager transfer service shall be 239.192.0.21 and 239.192.0.26 respectively. As a default, the port for simple and re-transmittable binary transfer shall be 60021 and 60026 respectively.

The receiver shall reply with ACK to the sender using the incoming datagram's multicast address and destination port. Optionally a reply with ACK to the sender may use any multicast address within the range from 239.192.0.21 to 239.192.0.30 and corresponding port number within the range from 60021 to 60030. This option requires that the system supports separate multicast address and port assignment for binary Image transfer sending and for ACK messages of binary Image transfer. For this option the default is 239.192.0.22 and 60022.

7.3.9 Error logging

Equipment shall maintain a count of the events of invalid binary image structures processed and make the count available. As a minimum, the following events shall be logged:

- the number of image blocks where errors occur;
- missing datagrams;
- unrecognized header.

8 Methods of test and required results

8.1 Test set-up and equipment

The following test methods require test equipment capable of transmitting and receiving UDP datagrams over the Ethernet interface and the use of a network protocol analyser. The test equipment shall be capable of supporting the Ethernet interface appropriate for the device under test. The equipment shall also be capable of generating invalid data.

The test equipment shall be configured to transmit UDP broadcast messages for the ports defined in 6.2.2.

Simulation equipment is required capable of

- generation of test UDP datagrams containing unique and numbered content, syntactically correct and incorrect sentences with datagram intensity that can be varied to exceed IEC 61162-1 and IEC 61162-2 channel capacity,
- generation of IEC 61162-1 test sentences containing unique and numbered content, syntactically correct and incorrect with variable length and correct, incorrect and missing checksum,
- generation of non re-transmittable and re-transmittable binary images.

8.2 Basic requirements

8.2.1 Equipment to be connected to the network

(see 4.2.1)

Verify through inspection of test documentation, that the network devices have been tested against the relevant requirements contained in IEC 60945.

For the purposes of IEC 60945 the following definitions apply.

- **Performance check**
  A performance check is the successful transmission and reception of data.

- **Performance test**
  A performance test consists of evaluating performance under different test scenarios.

8.2.2 Network infrastructure equipment

(see 4.2.2)

If the device under test is an IGMP snooping or CGMP enabled switch, confirm that IGMP snooping or CGMP can be disabled and that the documentation describes how to disable it.

Confirm by inspection of manufacturer provided information that the device under test does not provide the functions of router or a repeater hub.

8.3 Network function (NF)

8.3.1 Maximum data rate

(see 4.3.2)

Confirm by inspection that the manufacturer has specified the maximum datagram input rates as specified in items a) to c) in 4.3.2.

After activating all NF ports of the equipment under test with the specified maximum aggregate datagram rate as specified in 4.3.2, check that the performance of the equipment is not degraded in any way.

8.3.2 Error logging function

(see 4.3.3)

Confirm the manufacturer has provided means to inspect a log of detected errors.

NOTE Tests for the errors to be logged are given in 8.5.2, 8.9.2, 8.10 and 8.11.4.

Confirm that, if external data logging capability is provided, that the output of Syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

8.4 System function (SF)

8.4.1 General

(see 4.4.1)

For SFs that implement IEC 61162-1 and IEC 61162-1-2 interfaces, verify compliance in accordance with the test methods and required test results of IEC 61162-1, Annex B.

8.4.2 Assignment of unique system function ID (SFI)

(see 4.4.2)

Check that means are provided to assign and configure the SFI, as described in 4.4.2.

8.4.3 Implementing configurable transmission groups

(see 4.4.3)

Check that means are provided to assign and configure the transmission groups. Check that documentation has been provided describing the transmission groups supported by the device.

8.5 Serial to network gateway function (SNGF)

8.5.1 General

(see 4.5.1)

Check that it is possible to enter unique SFIs for all serial ports of the device and that the mapping of SFI to serial port is correctly implemented by analyzing the UDP datagrams.

Check that documentation is available describing any filtering used in the device.

8.5.2 Serial line output buffer management

(see 4.5.2)

Verify the output routing by feeding the network under test with datagrams containing sentences for all available serial outputs and check that sentences are routed to the output ports having the set SFIs.

Verify output buffer overflow handling by increasing the datagram data rate until possible capacity of the serial lines are exceeded and check that

- sentences are correctly discarded, maintaining the FIFO order and not affecting sentence integrity,
- the buffer overflow events are logged as required.

Verify required functionality for prioritized messages by repeating the test with the unit set for prioritized messages and check that behaviour is correct.

Verify message buffer integrity by repeating the test also with grouped messages and check that overflow handling maintains group integrity, meaning that whole groups are discarded, regardless of the prioritized message setting.

8.5.3 Datagram output

(see 4.5.3)

Verify datagram conversion by feeding the input ports of the network under test with sentences and check that these are transmitted in UDP datagrams with correct syntax and SFI.

The test sentences should include TAG blocks and grouped messages.

8.6 Other network function (ONF)

(see 4.6)

Verify by inspection of the manufacturer’s documentation that information for the use of ONF is provided as described in 4.6.

Verify using the test equipment described in 8.1 that the ONF does not use any of the multicast IP addresses reserved in 5.4.

8.7 Low level network

8.7.1 Electrical and mechanical requirements

(see 5.1)

Verify by observation that one of the connectors specified in Table 3 is available on the equipment.

Verify by inspection of manufacturer documentation that one or more of these interfaces meets the requirements of Table 3.

Verify by inspection of manufacturer documentation that the laser safety requirements for Class 1 devices are met.

8.7.2 Network protocol

(see 5.2)

Confirm by inspection of documented evidence that the relevant IEEE 802.3 data link protocol is used.

Verify using the network protocol analyser that IP (Version 4) protocol is used and that no IP option is used.

Confirm using ping program that each device supports the network protocols specified.

8.7.3 IP address assignment for equipment

(see 5.3)

Confirm by observation that means are provided to configure an IP address for the device.

Confirm that an IP address for the device is configured with the range of 172.16.0.1 to 172.31.255.254.

Using the test equipment described in 8.1 and documentation provided by the manufacturer, verify by transmitting and receiving data that the equipment does not change its IP address and IP port settings after an OFF/ON power cycle.

8.7.4 Multicast address range

(see 5.4)

Verify using the network protocol analyser that each datagram is transmitted and received with the multicast address 239.192.0.1 to 239.192.0.64.

8.8 Transport layer

(see Clause 6)

Verify that UDP messages are transmitted and received at each of the appropriate port numbers as defined in Tables 4 and 5.

Verify that UDP are discarded if the received UDP checksum is invalid.

Verify that each datagram contains no more than 1 460 bytes.

8.9 Application layer

8.9.1 Application

(see 7.2.1)

Using the test equipment described in 8.1 and documentation provided by the manufacturer verify by transmitting and receiving data that each SF and SNGF port of the equipment under test can send and receive IEC 61162-1 sentences and allows several sentences to be merged into one datagram if applicable.

8.9.2 Datagram header

(see 7.1)

Check that all UDP multicast datagrams are headed by:

- "UdPbC" for transmission of IEC 61162-1 formatted sentences;
- "RaUdP" for transmission of binary images;
- "RrUdP" for transmission of re-transmittable binary images;

followed by a null character (all bits set to zero) as the first six bytes of the datagram.

Check that incoming datagrams with an unknown header are discarded without processing the content beyond the header.

Verify that UDP datagram can be logged if UDP header is unrecognized or invalid, or has a UDP checksum error, including receiving datagrams with a zero checksum.

8.9.3 Types of messages

(see 7.2.2)

Using the test equipment described in 8.1, and documentation provided by the manufacturer, verify by transmitting and receiving data that each SF and SNGF port of the equipment under test can send and receive each of the message types specified by the manufacturer; one or more of SBM, MSM and CRP. For CRP messages, verify that the requirements of Clause C.4 are met by inspection of recorded datagrams and, in the case of timeout handling, the equipment's error log data.

8.9.4 TAG block parameters

(see 7.2.3)

8.9.4.1 Test of the transmitter

Verify using a receiving protocol analyzer that

- all members of group have same group code value,
- next group code value after 99 is 1,
- the device under test transmits the source identifier (two separate test cases – default and configured),
- if used, the device under test transmits valid destination code,
- line count value increments for each line and resets after 999 to 1,
- the heartbeat sentence (HBT) is transmitted at least once every 60 s,
- the device under test only feeds sentences preceded by a valid TAG block (for example "\s:II0001,n:23*31\$LCGLL,5420.123,N,01030.987,E,,A,A*58<CR><LF>") into the network.

8.9.4.2 Test of the receiver

Verify using a transmitting protocol analyzer that

- lines without a TAG block are not used as defined in 7.2.3.1,
- adding a TAG block containing syntactically correct parameter codes (for example “\z:Y23G81*56\”) not defined in this standard is transparent to normal operation,
- only complete sentence groups are used,
- TAG block lines with the device under test as destination are processed.

8.9.4.3 Test for bidirectional communication

If the network under test supports CRP then using a bidirectional protocol analyzer verify that source and destination are correct in the CRP communication.

8.9.4.4 Configuration

Verify by inspection of documentation that it is not possible to dynamically configure any identities after installation.

8.10 Error logging

(see 7.2.5)

By feeding test sentences with variable contents into the network, verify that the network under test processes only sentences preceded by a valid TAG block as defined in 7.2.3.1 and verify that

- lines with TAG checksum errors increase the corresponding error log count as defined in 4.3.3,
- lines with TAG syntax errors increase the corresponding error log count as defined in 4.3.3,
- lines with TAG framing errors (i.e. missing \ character at start, stop and between adjacent TAG blocks) increase the corresponding error log count as defined in 4.3.3.

Check handling of incorrect messages by feeding the network under test with sentences having

- incorrect syntax,
- incorrect checksum,
- incorrect message length.

Verify that these sentences are discarded and that the network’s error logs are updated.

8.11 Binary image transfer using UDP multicast

(see 7.3.)

8.11.1 Sender process test

8.11.1.1 Non re-transmittable image transfer

Using a test set-up with non re-transmittable binary images, verify that

- header tokens are set correctly,
- header version is one (=1),
- srcID is correctly set,
- destID is set by “XXXXXX”,

- unique BlockID is correctly set,
- BlockID, SequenceNum and MaxSequence are correctly set,
- Device is correctly set,
- Channel is correctly set,
- the IP address and port numbers are assigned by one of the addresses for non re-transmittable binary image transfer,
- there is no response when a receiver sends any ACK messages.

8.11.1.2 Re-transmittable image transfer

Using a test set-up with re-transmittable binary images, verify that

- header tokens are set correctly,
- header version is one (=1),
- SrcID and DestID is correctly set by “ccxxxx”,
- Unique BlockID is correctly set,
- BlockID, SequenceNum and MaxSequence are correctly set,
- Device is correctly set,
- Channel is correctly set,
- the IP address and port numbers are assigned by one of the addresses for re-transmittable binary image transfer,
- a new data transmission is started after an ACK message, whose SequenceNum is equal to the MaxSequence, after all data is transmitted,
- a QUERY message is sent when there is no ACK message after all data is transmitted,
- a QUERY message is sent when there is no ACK message after a QUERY message is transmitted,
- image data is re-transmitted when an ACK message, whose SequenceNum is less than the MaxSequence, is received,
- the number of re-transmissions including the number of QUERY message is always less than or equal to three,
- new data transmission is started when the number of re-transmission including the number of QUERY message is more than three,
- log messages are correct.

8.11.2 Receiver process test

8.11.2.1 Non-retransmittable image transfer

Using a test set-up with non re-transmittable binary images, verify that

- messages are received correctly on given IP and port address,
- each separate image transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- a new receiving process starts when a message with new BlockID is received for the combination of SrcID, Device and Channel,
- the received messages are the same as that of the transmitted data when there is no loss,
- any log information is provided if there is any loss,
- log messages are correct.

8.11.2.2 Re-transmittable image transfer

Using a test set-up with re-transmittable binary images, verify that

- messages are received correctly on given IP and port address,
- each separate image transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- an ACK message is transmitted when the received SequenceNum is equal to the MaxSequence with the same instance identifier,
- an ACK message is transmitted when a receiver detects that there is a gap in the SequenceNum between two consecutive messages,
- a new receiving process starts when a message with new BlockID is received for the combination of SrcID, Device and Channel,
- the received messages are the same as that of the transmitted data,
- the receiver does not send any control message when a sender sends an image block with different DestID,
- log messages are correct.

8.11.3 Image descriptor test

Using a test set-up with binary images, verify that

- the device and channel is correctly set,
- image length in the descriptor is the same as the size of the received data,
- the received data format is the same as that of the data type in the descriptor.

8.11.4 Image transfer error logging

Using a test set-up with binary images, verify that the following events can be logged

- number of image blocks where errors occur,
- missing datagrams,
- unrecognized headers.

Annex A
(normative)

Classification of IEC 61162-1 talker identifier mnemonics and sentences

A.1 General

Table A.1 gives a mapping from talker identifier mnemonic to a default transmission group for an SF.

Table A.2 classifies each of the IEC 61162-1 sentence formatters as belonging to one of three types of message

- sensor broadcast message (SBM) see 3.18,
- multi-sentence message (MSM) see 3.12,
- command-response pair (CRP) see 3.4.

A.2 Talker identifier mnemonic to transmission group mapping

Table A.1 maps the two first characters of the SFI that is normally the IEC 61162-1 talker identifier mnemonic, to the default transmission group the SF shall use for transmitting sentences. For the two character codes listed in Table A.1, the transmission group is identified in column three. For two character codes not in this table, the SF shall use the MISC transmission group as default.

Proprietary sentences that do not use a talker identifier mnemonic can be given a default transmission group by the manufacturer.

Table A.1 – Classification of IEC 61162-1 talker identifier mnemonics

Type of equipment	Talker identifier	Transmission group
Heading/track controller (autopilot) general	AG	NAVD
magnetic	AP	NAVD
Automatic identification system	AI	TGTD
Bilge system	BI	MISC
Bridge navigational watch alarm system	BN	VDRD
Communications: digital selective calling (DSC)	CD	RCOM
data receiver	CR	RCOM
satellite	CS	RCOM
radio-telephone (MF/HF)	CT	RCOM
radio-telephone (VHF)	CV	RCOM
scanning receiver	CX	RCOM
Direction finder	DF	NAVD
Duplex repeater station	DU	MISC

Type of equipment	Talker identifier	Transmission group
Electronic chart system (ECS)	EC	NAVD
Electronic chart display and information system (ECDIS)	EI	NAVD
Emergency position indicating radio beacon (EPIRB)	EP	RCOM
Engine room monitoring system	ER	MISC
Fire door controller/monitoring system	FD	VDRD
Fire extinguisher system	FE	VDRD
Fire detection system	FR	VDRD
Fire sprinkler system	FS	VDRD
Galileo positioning system	GA	NAVD
Global positioning system (GPS)	GP	NAVD
GLONASS positioning system	GL	NAVD
Global navigation satellite system (GNSS)	GN	NAVD
Heading sensors: compass, magnetic	HC	NAVD
gyro, north seeking	HE	SATD
fluxgate	HF	NAVD
gyro, non-north seeking	HN	SATD
Hull door controller/monitoring system	HD	VDRD
Hull stress monitoring	HS	VDRD
Integrated instrumentation	II	MISC
Integrated navigation	IN	NAVD
LORAN: LORAN-C	LC	NAVD
Navigation light controller	NL	MISC
Radar and/or radar plotting	RA	TGTD
Propulsion machinery including remote control	RC	MISC
Sounder, depth	SD	NAVD
Steering gear/steering engine	SG	MISC
Electronic positioning system, other/general	SN	NAVD
Sounder, scanning	SS	MISC
Turn rate indicator	TI	SATD
Microprocessor controller	UP	MISC
(0<=#<=9) User configured talker identifier	U#	MISC
Velocity sensors: Doppler, other/general	VD	NAVD
speed log, water, magnetic	VM	NAVD
speed log, water, mechanical	VW	NAVD

Type of equipment	Talker identifier	Transmission group
Voyage data recorder	VR	MISC
Watertight door controller/monitoring system	WD	VDRD
Water level detection system	WL	VDRD
Transducer	YX	MISC
Timekeeper, time/date: atomic clock	ZA	TIME
chronometer	ZC	TIME
quartz	ZQ	TIME
radio update	ZV	TIME
Weather instrument	WI	NAVD
Serial to Network Gateway Function[a]	SI	MISC

[a] This talker is not defined in IEC 61162-1, but included here for use by SNGF function blocks.

A.3 List of all sentence formatters and the sentence type

Table A.2 classifies the existing IEC 61162-1 formatters. The rightmost column lists related sentence formatters for MSM and CPR sentences.

Table A.2 – Classification of IEC 61162-1 sentences

	Description	SBM	MSM	CRP	Related sentence formatters
Q	Query sentence			X	Any reply message
AAM	Waypoint arrival alarm	X			
ABK	AIS addressed and binary broadcast acknowledgement	X			ABK, ABM, AIR, BBM
ABM	AIS Addressed binary and safety related message		X		ABM
ACA	AIS channel assignment message		X		ACA, ACS
ACK	Acknowledge alarm			X	ALR, ACK
ACS	AIS Channel management information source		X		ACA, ACS
AIR	AIS Interrogation request.				ABK
AKD	Acknowledge detail alarm condition			X	ALA, AKD
ALA	Report detailed alarm condition			X	ALA, AKD
ALR	Set alarm state			X	ALR, ACK
APB	Heading/track controller (autopilot) sentence B	X			
BBM	AIS Broadcast binary message		X		BBM
BEC	Bearing and distance to waypoint – dead reckoning	X			
BOD	Bearing origin to destination	X			
BWC	Bearing and distance to waypoint – great circle	X			
BWR	Bearing and distance to waypoint – rhumb line	X			
BWW	Bearing waypoint to waypoint	X			

	Description	SBM	MSM	CRP	Related sentence formatters
CBR	Configure Broadcast Rates for AIS AtoN Station Message Command		X		MEB
CUR	Water current layer – Multi-layer water current data	X			
DBT	Depth below transducer	X			
DDC	Display Dimming Control	X			
DOR	Door status detection		X		DOR
DPT	Depth	X			
DSC	Digital selective calling information	X			
DSE	Expanded digital selective calling	X			
DTM	Datum reference	X			
ETL	Engine telegraph operation status	X			
EVE	General event message	X			
FIR	Fire detection		X		FIR
FSI	Frequency set information	X			
GBS	GNSS satellite fault detection	X			
GEN	Generic binary information	X			
GFA	GNSS fix accuracy and integrity	X			
GGA	Global positioning system (GPS) fix data	X			
GLL	Geographic position – latitude/longitude	X			
GNS	GNSS fix data	X			
GRS	GNSS range residuals	X			
GSA	GNSS DOP and active satellites	X			
GST	GNSS pseudorange noise statistics	X			
GSV	GNSS satellites in view	X			
HBT	Heartbeat supervision sentence	X			
HDG	Heading, deviation and variation	X			
HDT	Heading true	X			
HMR	Heading monitor receive			X	HMS
HMS	Heading monitor set			X	HMR
HSC	Heading steering command	X			
HSS	Hull stress surveillance systems	X			
HTC	Heading/track control command			X	HTD
HTD	Heading /track control data			X	HTC
LR1	AIS long-range reply sentence 1		X		LRF, LRI
LR2	AIS long-range reply sentence 2		X		LRF, LRI
LR3	AIS long-range reply sentence 3		X		LRF, LRI
LRF	AIS long-range function		X		LR1, LR2, LR3, LRF
LRI	AIS long-range interrogation		X		LR1, LR2, LR3, LRF
MEB	Message input for broadcast command		X		CBR
MSK	MSK receiver interface	X			

	Description	SBM	MSM	CRP	Related sentence formatters
MSS	MSK receiver signal status	X			
MTW	Water temperature	X			
MWD	Wind direction and speed	X			
MWV	Wind speed and angle	X			
NAK	Negative acknowledgment			X	ALR, NAK
NRM	NAVTEX receiver mask			X	NRX
NRX	NAVTEX received message		X		
OSD	Own ship data	X			
POS	Device position and ship dimensions report or configuration command			X	
PRC	Propulsion remote control status	X			
RMA	Recommended minimum specific LORAN-C data	X			
RMB	Recommended minimum navigation information	X			
RMC	Recommended minimum specific GNSS data	X			
ROR	Rudder order status	X			
ROT	Rate of turn	X			
RPM	Revolutions	X			
RSA	Rudder sensor angle	X			
RSD	Radar system data	X			
RTE	Routes	X			
SFI	Scanning frequency information	X			
SSD	AIS ship static data	X			
STN	Multiple data ID	X			
THS	True heading and status	X			
TLB	Target label	X			
TLL	Target latitude and longitude	X			
TRC	Thruster control data	X			TRD
TRD	Thruster response data	X			TRC
TTD	Tracked Target Data		X		
TTM	Tracked target message	X			
TUT	Transmission of multi-language text		X		
TXT	Text transmission		X		
UID	User identification code transmission	X			
VBW	Dual ground/water speed	X			
VDM	AIS VHF data-link message		X		Sometimes single
VDO	AIS VHF data-link own-vessel report	X			
VDR	Set and drift	X			
VER	Version		X		
VHW	Water speed and heading	X			
VLW	Dual ground/water distance	X			

	Description	SBM	MSM	CRP	Related sentence formatters
VPW	Speed measured parallel to wind	X			
VSD	AIS voyage static data	X			
VTG	Course over ground and ground speed	X			
WAT	Water level detection	X			
WCV	Waypoint closure velocity	X			
WNC	Distance waypoint to waypoint	X			
WPL	Waypoint location	X			
XDR	Transducer measurements	X			
XTE	Cross-track error, measured	X			
XTR	Cross-track error, dead reckoning	X			
ZDA	Time and date	X			
ZDL	Time and distance to variable point	X			
ZFO	UTC and time from origin waypoint	X			
ZTG	UTC and time to destination waypoint	X			

Annex B
(informative)

TAG block example

NOTE Abbreviations related to the IEC 61162 series of standards and NMEA 0183 series are not included in the below example. For their meaning refer to those standards.

B.1 Validity of this information

NMEA 0183 series defines the syntax and semantics of the TAG block. This Annex shows a few examples of how the TAG block can be used in relation to this standard and these examples are included for information only.

B.2 TAG Block structure in this standard

The TAG block structure examples provided are not intended to include all possible uses for the TAG block.

NMEA 0183 lists all the possible combinations of input lines, and settings for the listener destination-identification and listener source-identification data fields.

TAG block parameter codes that have specific meaning within the context of this standard in the TAG blocks are listed in Table B.1.

A TAG Block is able to associate or link data in the TAG block and IEC 61162-1 sentences and is intended to be used to facilitate transport of IEC 61162-1 sentences over a network.

One use of the source parameter to identify a System Function block (SF) or a Network Function block (NF) device is shown below.

```
\s:GP0002,d:SI0001,d:SI0005,n:23*21\$GNGNS,122310.2,3722.425671,N,
12258.856215,W,DA,14,0.9,1005.543,6.5,5.2,23*59<CR><LF>
```

In the example the source "s" identified is a system function block with implied talker identifier “GP” (Global Positioning System – GPS) that has been designated as equipment number "0002". The destination "d:" for the information is two SNGF serial ports with equipment numbers “0001” and “0005” . Other equipment listening on the same transmission group can also read and process this information. This sentence is line number "n:" 23, from this GNSS source.

```
\g:1-2-98,n:248,s:AI0002*76\
!AIVDM,2,1,9,A,54a5;h02=UWH?I=08004pEA@D000000000000016BHQ,0*7B

\g:2-2-98,n:249,s:AI0002*74\
!AIVDM,2,2,9,A,?84bD0@URC0H13p0kkQ1@0000000,2*16
```

In the second example shown directly above, the "g" character is employed to group the sentences from an AIS source identified with SFI “AI0002”. The g code is divided into three fields where the use of each field (from left to right) are:

1. The line number for this particular TAG block and associated sentence.

2. The total number of lines.

3. The group code. Used to differentiate between different groups of TAG blocks and sentences.

\g:1-2-34,s:HE0003,n:23,d:VR0001*3C\$HETHS,181.3,A*26<CR><LF>

In this third example the gyro compass with SFI “HE0003” is providing its data to the destination device which is a voyage data recorder with SFI “VR0001”. In this case the destination code is strictly speaking superfluous as all devices listening on the transmission group can read and process the information.

Parameter codes and data for use in the IEC 61162-450 protocol can be located in different TAG blocks and the same parameter code may occur several times. In this case the last occurrence (reading from left to right) of the parameter code should be used.

\g:1-2-
98,s:sbAIS02*72\\n:248,s:AI0002*05\ !AIVDM,2,1,9,A,54a5;h02=UWH?I=08004pEA@D00
0000000000016BHQ,0*7B

This is shown in the last example which is a variant of first line of the second example above. In this case the grouping information should be taken from the left most TAG block while the line number and source code should be taken from the right most. The source code in the left most TAG block is not in IEC 61162-450 format and does presumably contain information not intended for use in this protocol.

In general a TAG block will consist of a list of parameter code and value pairs. Each parameter code and associated value code is separated by a comma and the code and value pair is separated by a colon.

The maximum length of a TAG block is 80 characters. It is delineated by a back-slash at the start and the end of the TAG block.

B.3 TAG block parameter-code dictionary

Table B.1 lists the currently defined parameter-codes that are required when using TAG block within this standard. All codes are one lower case character.

NOTE Table B.1 is a subset of TAG Block parameters defined in NMEA 0183, section 7. NMEA 0183 defines for example additional TAG Blocks for UNIX time (c), Relative time (r), etc.

Table B.1 – Defined parameter-codes

Parameter-code	Description	Form of parameter value
d	Destination-identification	Alphanumeric string (15 char. maximum)
g	Sentence-grouping	Grouped numeric string (alphanumeric)
n	Line-count	Positive integer
s	Source-identification	Alphanumeric string (15 char. maximum)
t	Text	Free text, including proprietary information

Annex C
(normative)

Reliable transmission of command-response pair messages

C.1 Purpose

The rules that are listed below are included to promote reliable bidirectional exchanges of sentences classified as command-response pair (CRP) in Annex A. All equipment making use of CRP message exchanges shall follow these rules.

C.2 Information exchange examples

Examples of bidirectional communication where command-response pair typically occur include

- query for sentences,
- alarm and acknowledge,
- equipment initialisation with response success or fail,
- command followed by data or status as response.

Although the content differs, the information exchange is similar in structure.

C.3 Characteristics

Two parties exist in the communication, see Figure C.1. The Network device 1 (ND1) is transmitting the command and the ND2 is transmitting a response as a result of the processing of the command.

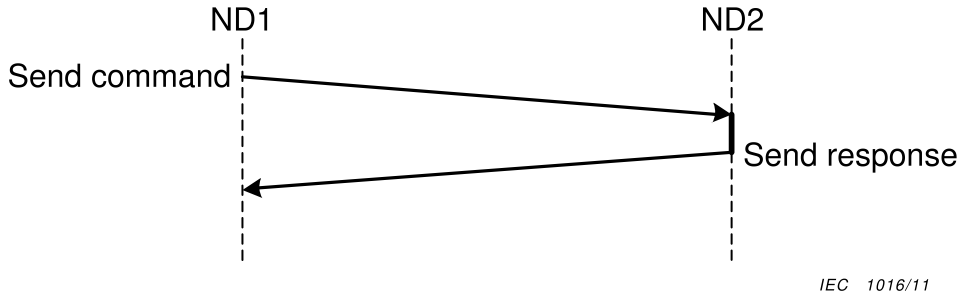

Figure C.1 – Command response communications

C.4 Requirements

The requirements for reliable communication include:

- TAG block parameter “s” shall be used to uniquely identify the source of the sentence;
- TAG block parameter “d” shall be used to uniquely identify the destination of the sentence;
- TAG block parameter “g” shall be used to group sentences if required;
- TAG block parameter “n” shall be used to assign a sequence number to each sentence transmitted from a system function block, if required;
- timeout handling to detect loss of messages;

- optional timestamp to limit the effect of time delays for transmission.

C.5 Data flow description

C.5.1 Heartbeat message

The heartbeat sentence (HBT) is intended to inform that the unit is in normal operation, if no other requirements specify other messages for this purpose, for example as done in C.5.4. It shall be sent at a stated interval. The example below transmits interval set to 60 s and shows the sequential sentence identifier incremented from 3 to 4 to distinguish sentences.

```
...
\s:YX0001,n:123*01\$YXHBT,60,A,3*07<CR><LF>
...
\s:YX0001,n:231*01\$YXHBT,60,A,4*00<CR><LF>
```

C.5.2 Command response pair

This example is for command-response to set NAVTEX receiver mask from an INS.

```
\s:IN0001,d:NR0001,n:123*68\$INNRM,2,1,00001E1F,00000023,C*38<CR><LF>
```

The response within timeout from the NAVTEX receiver is if operation is successful

```
\s:NR0001,d:IN0001,n:234*6D\$NRNRM,2,1,00001E1F,00000023,R*32<CR><LF>
```

or if unsuccessful operation

```
\s:NR0001,d:IN0001,n:234*6D\$NRNAK,IN,NRM,NR0001,2,Unvalid setting*16<CR><LF>
```

or if a bad checksum in the TAG block or any TAG block in a grouped TAG block

```
\s:NR0001,d:IN0001,n:234*6D\$NRNAK,IN,NRM,NR0001,6,Checksum failure in TAG
Block*58<CR><LF>
```

or if a bad checksum in the sentence or any sentence in a TAG block group of sentences

```
\s:NR0001,d:IN0001,n:234*6D\$NRNAK,IN,NRM,NR0001,6,Checksum failure in
sentence*62<CR><LF>
```

C.5.3 Alert handling

Figure C.2 shows the two main states N and A that the sensor device can be in with respect to alerts.

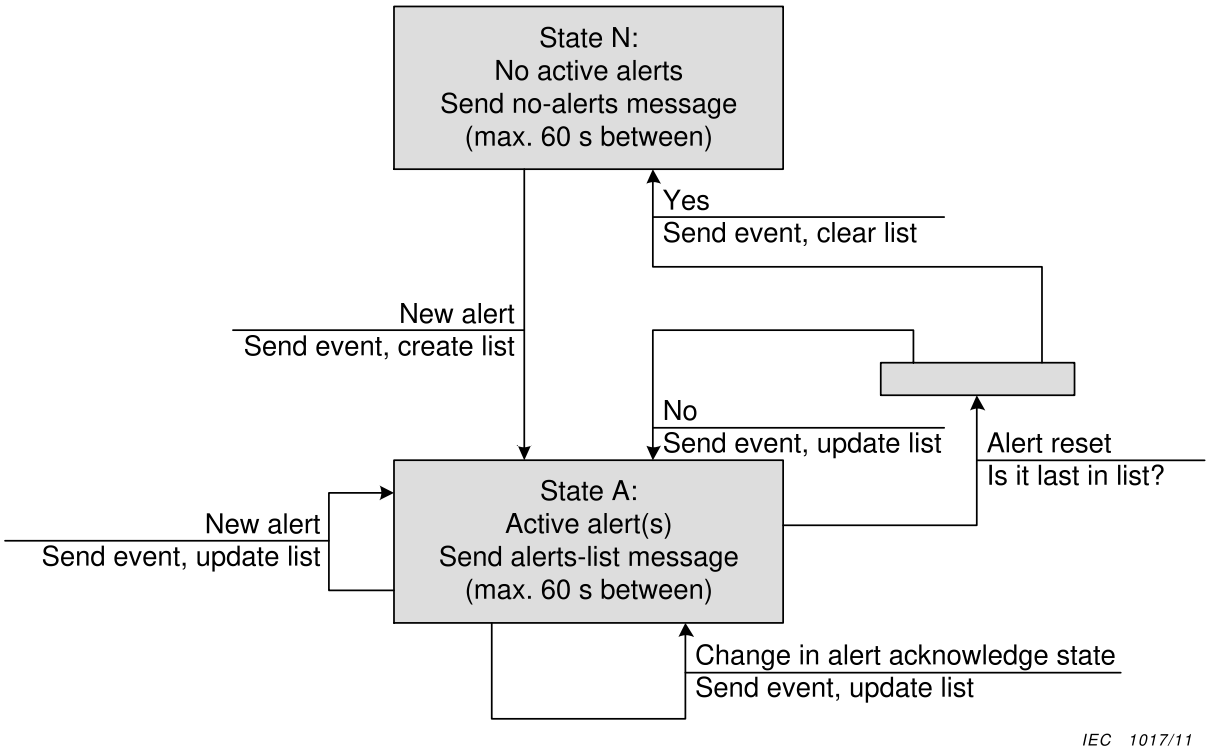

Figure C.2 – State diagram

The sensor device has two main states:

- *State N:* No active alerts. The device shall send a “no-alerts” message (see below) with a period not exceeding 60 s.
- *State A:* The device has one or more active alerts, of which zero or more may be acknowledged and the rest (possibly zero) are unacknowledged. In this state, the device shall send all active alerts with a period not exceeding 60 s. When multiple alerts are active in the device, it is recommended to transmit all active alerts as “a list” of alerts (alert-list message).

In addition to the periodic transmissions as mentioned above, the device shall immediately send an Alert message (ALR sentence), when (Values for alert condition and acknowledge state in parenthesis):

- a new alert is raised in the device – (A,V);
- an existing alert is acknowledged in the device (either on the device itself or by remote acknowledgement) – (A,A);
- an existing alert condition becomes non-active (V,V or V,A).

The alert message may include the time stamp when the alert last changed status (normally current time) and include the alert number, explanatory text as well as appropriate alert and acknowledgement flags. It may optionally be followed by a TXT message to give additional contextual information. The TXT message should be contiguous with its associated ALR. An example is included below.

```
\g:1-3-14,s:YX0001,d:BN0001,n:321*08\$YXALR,123456,906,A,V,Sensor
    fault*05<CR><LF>
\g:2-3-14,n:322*12\$YXTXT,02,01,06,Selftest error 17*2C<CR><LF>
\g:3-3-14,n:323*12\$YXTXT,02,02,06,See service manual*4F<CR><LF>
```

NOTE 1 This specification does not put any restrictions on the transitions that are reported through an event message. Thus, receivers should be prepared to receive and process all possible combinations and sequences of alert state events.

NOTE 2 The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.5.4 No-alerts message

The *no-alerts* message shall be sent to inform that the device has no active alerts. It shall be repeated with a period not exceeding 60 s. This message may be used to clear the receiver's alert list.

This message is sent as an ALR message, but without time stamp, and shall include a 'V' flag in both the alert condition and acknowledgement field. The *no-alerts* (list empty) message is included below.

```
\s:YX0001,d:BN0001,n:456*79\$YXALR,,,,V,V,*72
```

NOTE The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.5.5 Alerts-list message

The alert/alert-list message shall be sent to periodically refresh the alert list so that the listener can verify that it has the correct internal list of active alerts. This will, in turn, help to remedy problems that may occur due to lost datagrams at earlier stage, synchronization of recently added receivers, etc.

The alert/ alert-list message shall be repeated with a period not to exceed 60 s, if any alerts are active.

The alert/ alert-list message consists of the same message(s) sent when the corresponding event occurred, but all active alerts shall be reported, and preferably with no delay between messages. An example with two messages in the list is included below:

```
\s:YX0001,d:BN0001,n:567*7A\$YXALR,123456,123,A,A,Battery power in
    use*33<CR><LF>
\s:YX0001,d:BN0001,n:568*75\$YXALR,130507,456,A,V,Self test
    failure*18<CR><LF>
```

NOTE 1 The time stamp will wrap around after 24 h. For alerts that are active longer than 24 h, the receivers will need to keep track of the original event time.

NOTE 2 The use of ALR and ACK in these examples does not preclude the use of other alert management sentences in the future.

C.6 Alert acknowledgement

C.6.1 General principles

If the alert handling device has a bi-directional data link to the sensor device, it is possible to send remote acknowledgements to alerts (ACK sentence) based on user action, e.g., through an acknowledgement button. This means that one can leave the resolution of potentially lost acknowledgement or alert status messages to the user. The user should note that the acknowledgement was not effected and, if necessary, repeat the acknowledgement at the local or remote station.

C.6.2 Alert acknowledgement

If alert acknowledgement is implemented, exactly one acknowledgement message shall be sent each time the operator initiates an acknowledgement.

```
\s:BN0001,d:YX0001,n:123*7E\$BNACK,234*5C<CR><LF>
```

C.6.3 Alarm acknowledge capability

In some cases, the sensor device needs to know if the alert handling device is able to communicate with it. This may, for example be used to implement silent alerts on the sensor device.

In this case, it is necessary to send an empty alarm acknowledge message from the external alert handling device to the device at regular intervals. The message should be sent at an interval not to exceed 60 s.

\s:BN0001,d:YX0001,n:123*7E\$BNACK,*69<CR><LF>

The alert handling device shall not send any messages, including heartbeat, if the empty acknowledgement message from the sensor device has not been received in a period of maximum 130 s. This time shall be reduced appropriately if the specified repetition interval is shorter.

Annex D
(informative)

Network and system design guidance

D.1 General

This informative annex provides guidance on network and system design.

The purpose of this annex is to provide some guidelines as to how a ship system can be made safer and more maintainable. Safety does in particular address the needs of a system that should be continuously available or at least degrade in a manner that retains some minimum functionality for the operator.

D.2 Security

D.2.1 Connections to external networks and systems

D.2.1.1 General

In general one can look at the ship network as a black (here, white) box that has a number of interfaces to systems outside the network (hashed). The interfaces will normally have to be implemented so that they provide some form of “isolation” to avoid problems propagating from one system to another (dark gray boxes). This is illustrated in Figure D.1.

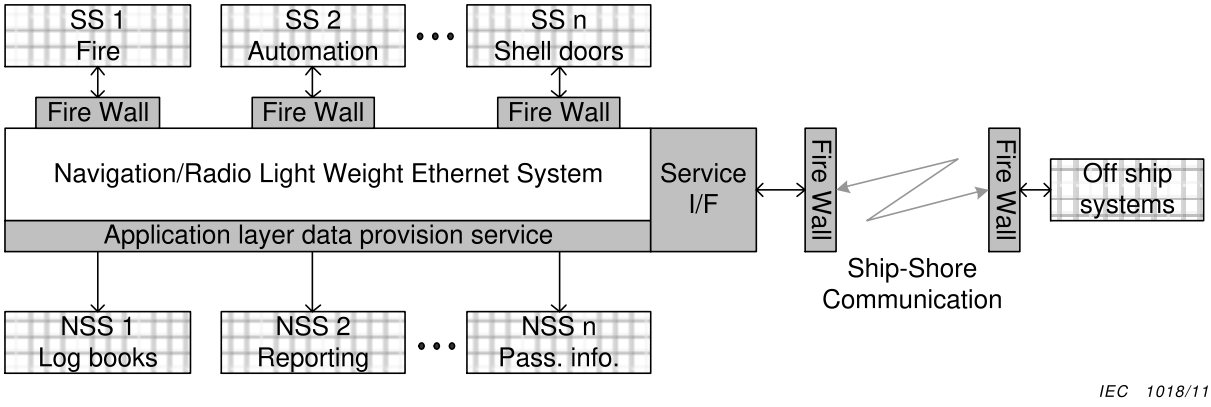

Figure D.1 – General system design architecture

One can define three different types of interfaces as follows.

a) Non-navigational data transfers in the navigational network (SS n), for example shell door status. These need some form of fire wall to be interfaced to the network.

b) Inter-system data transfers such as navigational data communications with other systems on the ship (NSS n). This may be interfaces for electronic log books, reporting systems or passenger information systems. One possibility here would be to define an application layer data provision service that also acts as a fire wall between external systems and the network.

c) Off-ship data transfers such as an interface to a ship management service or remote maintenance functions over a ship/shore data link. This is also a potential security and safety risk for the navigational services as it can change the functionality of the integrated bridge system. Thus, a number of fire walls will normally be needed.

D.2.1.2 Non-navigational data transfers

For the systems labelled SS in Figure D.1, an additional problem is that these systems have their own regulatory requirements that, in general, preclude direct connection between these systems and any other network on the ship.

D.2.1.3 Inter-system data transfers

For inter-system data transfers the easiest way to implement the required services is probably through an application layer firewall that connects the navigation network to a “public” on board network that also can provide a link to the satellite terminal. The details of the functions of this firewall depend on the general topology of ship networks and how different external systems can connect to the firewall.

D.2.1.4 Ship to shore data transfers

For connection to shore one could use VPN (Virtual Private Network) or similar technology to make sure that only authorized users get access to the system and that nobody can interfere when such access has been established. An example topology is shown below. Here, VPN is used in combination with application level fire walls.

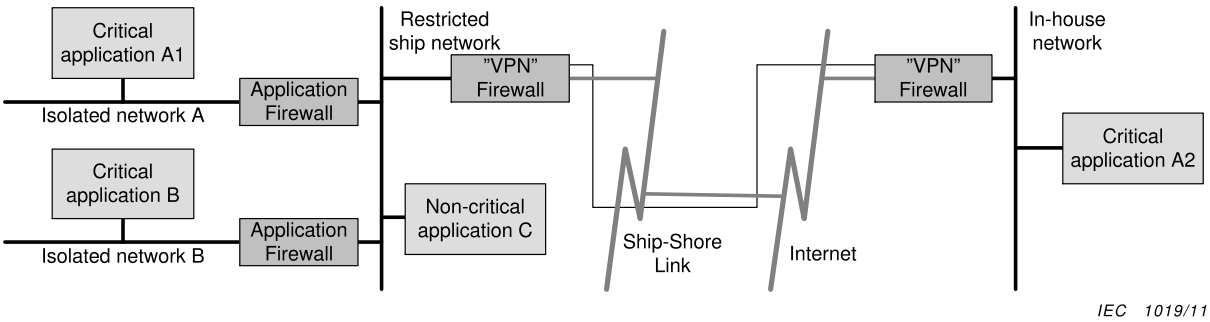

Figure D.2 – Example of ship-shore communication architecture

Ship operators are understandably concerned about security whenever the topic of internetworking ships navigation and control systems is raised. However, they tend to ignore the reality that bridge systems are often already connected by the “sneakernet” meaning that a memory stick or some other storage device is manually fitted into the bridge system to transfer data from a non-secured PC. This approach is extremely high-risk and potentially exposes the bridge system to all of the potential threats of the Internet and yet there are no protocols in place to protect these vulnerable systems from such threats.

A shipboard security architecture should comply with information security industry’s best practices, based on the following general principles:

- security and attack mitigation based on policy;
- security implementation throughout the infrastructure (not just on specialized devices);
- secure management and reporting;
- authentication and authorization of users and administrators to critical resources;
- intrusion detection for critical resources and subnets.

Implementation of these principles requires a layered approach to security “in-depth” which includes

- perimeter firewall(s) and intrusion detection,
- no Internet access permitted by any sensitive system,
- no non-encrypted Internet access by any Navigation System device (only VPN traffic),

- high security policy implementations on all sensitive nodes.

Figure D.3 shows how these principles can be realised onboard a ship.

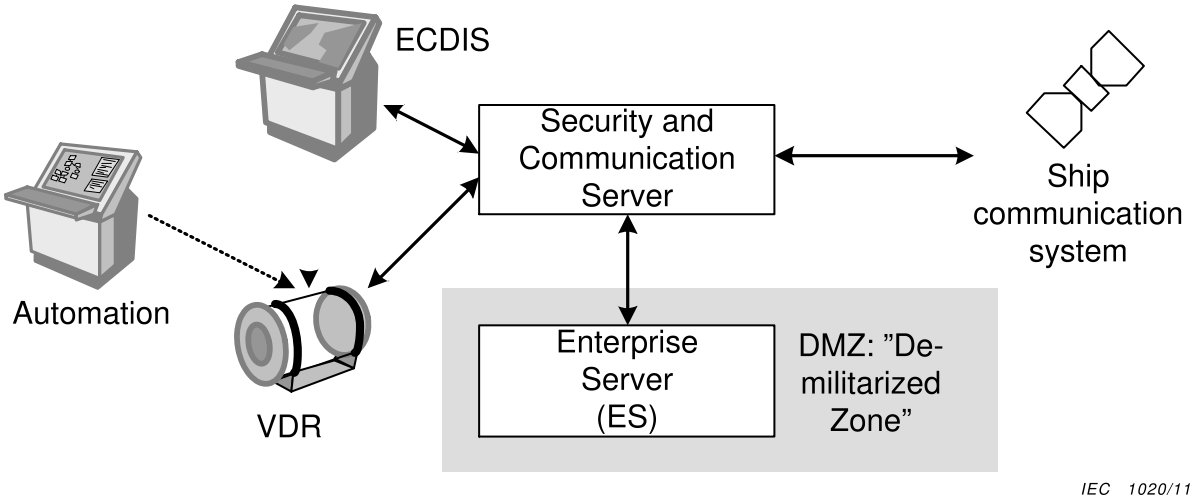

Figure D.3 – Security infrastructure

The Security and Communications Server isolates shipboard navigation and automation systems (safety dependent systems) from unsecured equipment. It also secures traffic from the shipboard enterprise server (trusted-software components) to the Internet and vice versa.

D.2.2 Physical isolation of network and equipment

This standard assumes that the physical network is only available to authorised persons and that it is not possible to tamper with the network through direct access to it. The network designer needs to take special precautions where equipment is placed so that general crew or passengers do not have access to it. This will also mean that these persons should not get access to the network through the equipment or by removing the equipment and getting access directly to the network cable.

D.2.3 Security mechanisms

The security should be supported by all or some of the network nodes except hubs since these simply relay the physical signals and do not perform any processing. At least one of the following security functions should be provided in the network.

a) Device Authentication: Device authentication is a mechanism to verify that all devices connected to the network are authorized devices. If the device is not authorized, the device is not allowed to access network. So, all devices should be registered and pre-authorized before it starts the communication.

b) Rate Control: Rate control is the mechanism to control the incoming/outgoing traffic volume at the network nodes including devices. Each node can limit the incoming/outgoing traffic rate for each network interface. So, each node configures the incoming/outgoing traffic rate based on the estimation of the maximum network traffic. For example, when a switch configures an Ethernet interface with incoming traffic rate with 1 Mbps, it can receive at most a maximum of 1 Mbps with the interface. This is very useful to protect the network from the worm virus attacks or the malicious network attacks such as flooding attacks. Since those attacks generate huge volume of the network traffic, the network and devices can easily be saturated or malfunctioned.

c) Firewall: A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. Firewalls are frequently used to prevent unauthorized Internet users from accessing

private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

d) Intrusion protection system (IPS): Any connection to the internet can be subject to attack from outsiders in an attempt to gain unauthorized access to the systems. An Intrusion Protection System (IPS) goes beyond scanning for viruses or malware and looks directly at traffic behaviour. If an attacker is attempting to gain access to the network through known hacking behaviour, the IPS system will immediately shut them down while allowing legitimate traffic to pass uninterrupted.

The security functions and the locations that will provide these functions are summarised in Table D.1.

Table D.1 – Overview of possible security functions

Security functions	Location	Security level	Mechanisms
Device authentication	Switch and Gateway	Low	MAC/IP address filtering Smart card/ Hardware-based authentication Device certificate IEEE 802.1x
Rate control	Switch (and Gateway)	Low	Per interface Per traffic class Per traffic stream
Firewall	Switch and Gateway	Medium	Packet filtering Application gateway Circuit-level gateway Proxy server
Intrusion protection system	Gateway	High	

D.3 Safety and redundancy

D.3.1 Overview

Many ship systems, among them navigation, need a high degree of availability. The following objectives are defined.

- Redundancy: Functions that rely on communication between equipment will need more than one communication path.
- Fail to silent: Faults in a network should only affect connected equipment's ability to communicate with other equipment. Fault handling shall allow equipment that is not directly affected by the fault to continue to operate to the degree that lack of communication allows. This can be achieved by a switch rate control mechanism that can limit traffic from malfunctioning equipment.
- Avoid fault propagation: The network should, as far as possible, be designed to not propagate consequences of a failure from one part of the network to another. This also applies to faults occurring in one equipment that may threaten the whole system, for example equipment that transmits to other equipment with high volume garbage traffic. This can also be achieved by a switch rate control mechanism that can limit traffic from malfunctioning equipment.

D.3.2 IGMP snooping

For a network to work with IGMP snooping, all equipment in the network will need to incorporate the same version of IGMP. It is very unlikely that this can be achieved in a

shipborne network over the lifetime of a ship as equipment is changed and maintained. This standard requires therefore that IGMP snooping is disabled and the network documentation should provide this information.

D.3.3 Redundancy

For ships, the most common approach is to design the complete system so that no single fault or no likely combination of faults shall render critical functions unavailable. To achieve this, one will normally duplicate the necessary components and the communication paths between them or provide fall back modes of operation. A simple example of duplication is provided in Figure D.4.

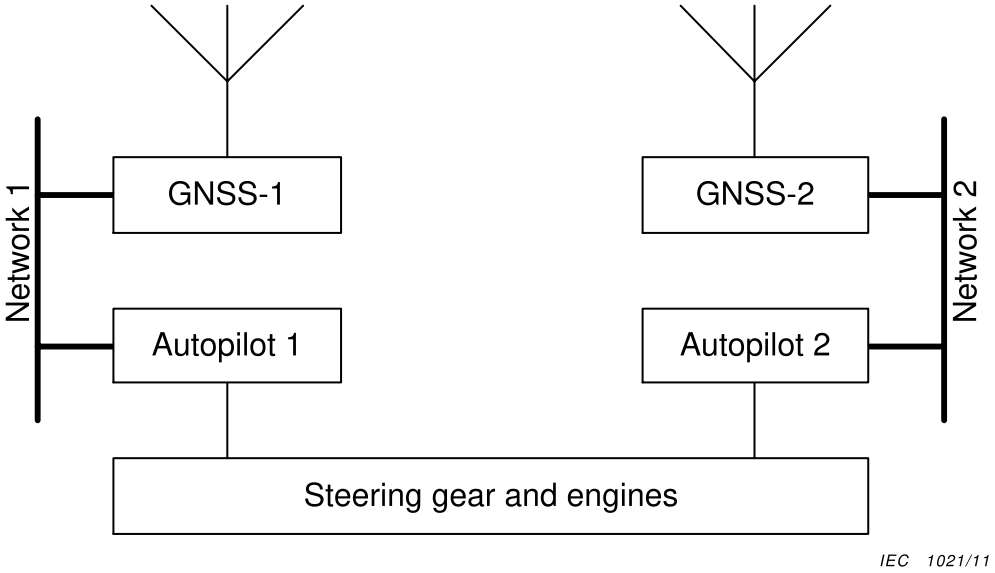

Figure D.4 – Decoupled system

This system will probably rely on some form of manual switch-over between the two autopilots so that the two networks are totally segregated and there is no possibility for any faults in one sub-system to propagate to the other.

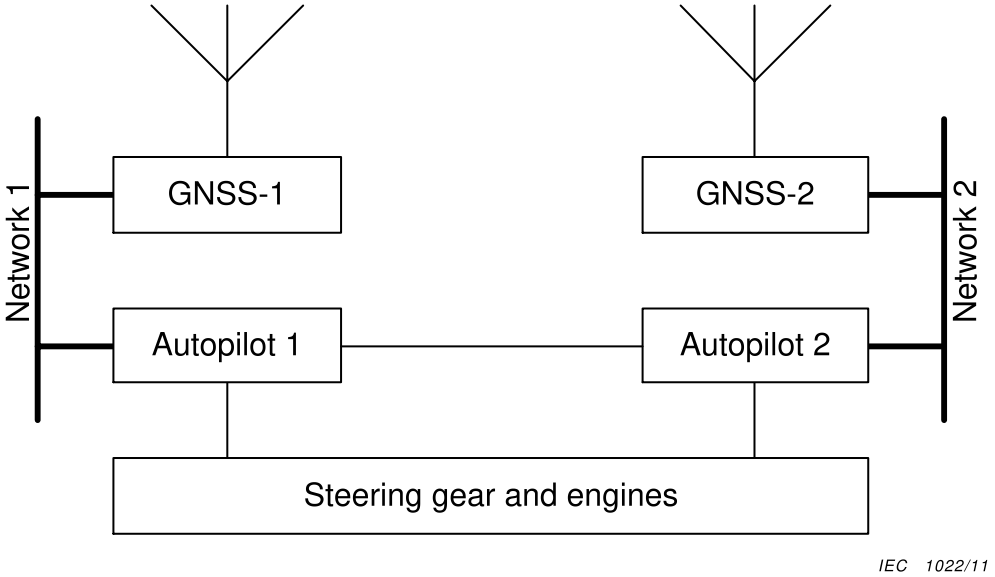

Figure D.5 – Loosely coupled system

A slightly more complex example is shown in Figure D.5 where an automatic coordination function via a digital communication link has been added. This has benefits in automatic, continuous and faster switch-over when problems are detected.

However, in this case there is a possibility that a failure mode in network 1 propagates to autopilot 2 through this data link. One may also conceivably get new common failure modes, triggered by the same event, in the two autopilots. These possibilities are normally low and can in most cases be disregarded if the two communicating devices have been properly designed.

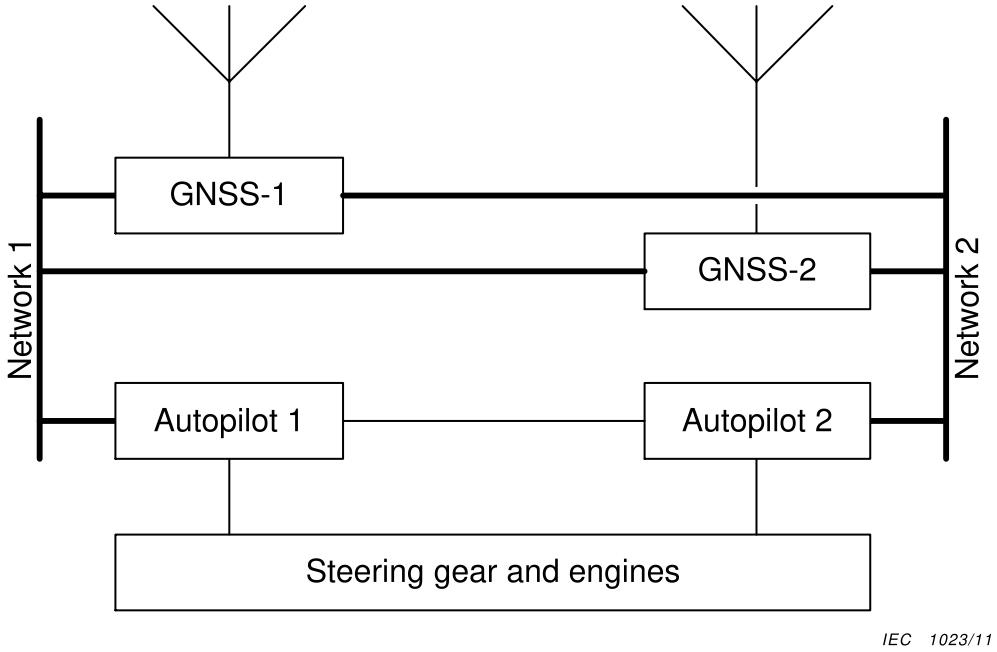

Figure D.6 – Strongly coupled system

One can consider the alternate system design in Figure D.6. At the cost of duplicated connections from each GNSS to both networks, this system provides much higher availability in that it can tolerate both a single general network fault as well as a fault in one of the GNSS receivers before functionality is degraded. Also, the coupling of sensor data allows new integrated navigation system functions to be implemented where one can increase the integrity of the position fix data.

However, this also adds new failure propagation possibilities, through each GNSS, from one network to the other. Also, a new common failure mode possibility is added in that each of the GNSS may have a failure mode where it overloads both networks, rendering the complete system without the autopilot function. On the other hand, failure modes associated with wrong data from each GNSS can be avoided as better integrity and data checks easily can be implemented.

As has been shown, there are important benefits to be had through coupling between the two networks, but this coupling provides the possibilities for new failure modes. The provisions of this standard allows for decoupled redundant systems to be designed with little or no system level analysis beyond that which is performed through equipment documentation and tests. This may also apply to loosely coupled systems, but in this case the designer of equipment that is connected together may need to prove that this coupling does not pose any problem in relationship to common mode failures in networks.

For strongly coupled systems, a system design review will normally have to be performed to identify any potential failure modes, their effects and criticality and measures to remedy any problems.

D.3.4 Failure propagation through a network

In addition to having some failure modes associated with its communication function, the network may also propagate failures from the network itself or other nodes. Table D.2 shows the most important types of such failure modes.

Table D.2 – Network failure propagation possibilities

Failure mode	Cause	Probability	Criticality
Network overload	General network traffic may overload listening nodes	Medium	High
Denial of service	One node may overload a single other node by excessive service requests or general garbage data.	Medium	High
Broadcast storms	Network devices fail in such a way as to overload nodes with garbage or duplicated real messages.	Low	High

An analysis of the traffic patterns and network load needs to be performed which may have various forms as follows.

- A receiver cannot process as many input messages as it gets, due, for example to too many senders being able to address this receiver. This can be analysed off-line by using equipment specifications and comparing these with each other. Note in particular that this standard uses multicast where several different senders can send messages to the same receiver.
- A network to serial line gateway has a special problem in that it is constrained to a maximum output rate given by the serial line capacity. This problem has been catered for in this standard in the equipment requirements for this type of device. Note however, that overload will make the gateway discard some messages.
- Hostile denial of service attacks may occur through an external gateway. This is discussed in D.2.3.
- Other forms of denial of service may occur due to equipment failures or errors in configuration. This has a relatively low probability and can normally be discarded for tested and approved equipment.

D.3.5 Non IEC 61162-450 equipment connected to a network

Other uses of the Ethernet network is allowed based on rules set for ONF (Other Network Function) specified in this standard (see 4.6).

D.4 Maintenance and manageability

D.4.1 Maintainability

One important aspect of safety is the time needed to repair a fault. The “single fault tolerance” principle is based on the ability to make corrective actions before a new fault occurs. Also, the issue of fault avoidance through problem detection and early repair is important.

D.4.2 System and management functionality

This standard contains no direct requirements to system management functions. However, early detection of problems and determining where the problems originate from is important for maintaining networked navigation systems.

Some of the possibilities that can be considered to simplify management of networked systems are the following.

- If the network has a firewall to outside networks, this node can also be used to collect statistics and error messages from the other nodes on the network. This can then be made

available to crew or to service personnel. Any other node can also be assigned this function, but the firewall function will also enable easy transfer to external systems.

- The heartbeat sentence can be used to collect some information from the nodes. One may also listen to other sentences when this gives system state information.
- Management protocols like SNMP (Simple Network Management Protocol) can be used to report additional information both from network nodes and network equipment like switches. This requires SNMP support in the relevant nodes.
- One may also use functionality in ICMP (Internet Control Message Protocol) to check if nodes are available. All nodes should be able to process, for example ping requests.

Finally, one should also consider the use of other protocols to facilitate for example time coordination in the system. The most common protocol for this is NTP (Network Time Protocol).

D.4.3 System and network integrator

In modern practice, after delivery of a ship from a shipyard, there is no system integrator or ship-board responsibility for network system, security and maintenance. This needs to be taken into account in network and system design.

Bibliography

IEC 60603-7, *Connectors for electronic equipment – Part 7: Detail specification for 8-way, unshielded, free and fixed connectors*

IEC 60603-7-3, *Connectors for electronic equipment – Part 7-3: Detail specification for 8-way, shielded, free and fixed connectors, for data transmission with frequencies up to 100 MHz*

IEC 60603-7-7, *Connectors for electronic equipment – Part 7-7: Detail specification for 8-way, shielded, free and fixed connectors for data transmission with frequencies up to 600 MHz*

IEC 61076-2-101, *Connectors for electronic equipment – Product requirements – Part 2-101: Circular connectors – Detail specification for M12 connectors with screw-locking*

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

IEC 61162-3, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 3: Serial data instrument network*

IEC 61174, *Maritime navigation and radiocommunication equipment and systems – Electronic chart display and information system (ECDIS) – Operational and performance requirements, methods of testing and required test results*

IEC 61754-20, *Fibre optic connector interfaces – Part 20: Type LC connector family*

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

ISO/IEC 11801:1995, *Information technology – Generic cabling for customer premises*

ISOC RFC 826:1982, *Ethernet Address Resolution Protocol (ARP), Standard STD0037 (and updates)*

ISOC RFC 894:1984, *A Standard for the Transmission of IP Datagrams over Ethernet Network , Standard STD0041 (and updates)*

ISOC RFC 1112:1989, *Host Extensions for IP Multicasting, Standard STD0005 (and updates)*

ISOC RFC 1122:1989, *Requirements for Internet Hosts – Communication Layers, Standard STD0003*

ISOC RFC 2365, *Administratively Scoped IP Multicast, Best Current Practice BCP0023*

ISOC RFC 3232:2002, *Assigned Numbers: RFC 1700 is Replaced by an On-line Database*

ISOC RFC 4288, *Media Type Specifications and Registration Procedures*

ISOC RFC 4289, *Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures*

IMO resolution MSC.252(83), *Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS)*

TIA/EIA-568-A:1995, *Commercial Building Wiring Standard*

TIA/EIA-604-10-A:2002, *FOCIS10 – Fibre Optic Connector Intermatebility Standard, Type LC*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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