IEC 61162-450

Edition 3.0 2024-04
COMMENTED VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 61162-450:2024-04 CMV(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC 61162-450

Edition 3.0 2024-04
COMMENTED VERSION

INTERNATIONAL STANDARD

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 978-2-8322-8714-9

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

This commented version (CMV) of the official standard IEC 61162-450:2024 edition 3.0 allows the user to identify the changes made to the previous IEC 61162-450:2018 edition 2.0. Furthermore, comments from IEC TC 80 experts are provided to explain the reasons of the most relevant changes, or to clarify any part of the content.

A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text. Experts' comments are identified by a blue-background number. Mouse over a number to display a pop-up note with the comment.

This publication contains the CMV and the official standard. The full list of comments is available at the end of the CMV.

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

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

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

a) clarification of serial to network gateway function (SNGF) in 4.5 with the addition of two new figures;
b) addition of further destination multicast addresses and port numbers in 6.2;
c) clarification of TAG block parameters in 7.2 together with Annex B, a new Annex H and associated tests in 8.9.4;
d) clarification of the sender process for binary files in 7.3.6 and the receiver process for binary files in 7.3.7 with updated Figure 6 and Figure 7;
e) clarifications of SFI collision detection and use of SRP sentence in 7.5 together with a new Annex G;
f) revision of tests for handling malformed data received on the serial line in 8.5.5.

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

Draft	Report on voting
80/1094/FDIS	80/1098/RVD

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

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

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

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

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

- reconfirmed,
- withdrawn, or
- revised.

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 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 document 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 document specifies an Ethernet based bus type network where any listener can receive messages from any sender with the following properties.

- This document 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 file), for example between radar and VDR, and also includes provisions for multicast distribution of information formatted according to IEC 61162-3, for example position fixes and other measurements.
- This document 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 document provides requirements only for equipment interfaces. By specifying protocols for transmission of IEC 61162-1 sentences, IEC 61162-3 PGN messages and general binary file data, these requirements will guarantee interoperability between equipment implementing this document as well as a certain level of safe behaviour of the equipment itself.
- This document permits equipment using other protocols than those specified in this document to share a network infrastructure, provided that it is supplied with interfaces which satisfy the requirements described for ONF.
- This document includes provisions for filtering of the network traffic in order to limit the amount of traffic to manageable level for each individual equipment.

This document does not contain any system requirements other than the ones that can be inferred from the sum of individual equipment requirements. An associated standard, IEC 61162-460, further addresses system requirements.

2 Normative references

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

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

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

IEC 61162-1~~:2016~~, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 1: Single talker and multiple listeners* **1**

IEC 61162-3~~:2008~~, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 3: Serial data instrument network* **1**

IEEE Std 802.3-~~2015~~2022, *IEEE Standard for Ethernet* **2**

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)* **3**~~

~~RFC 793:1981, *Transmission Control Protocol (TCP)* **3**~~

ISOC RFC 826, *An ethernet Address Resolution Protocol*

ISOC RFC 1112, *Host Extensions for IP Multicasting, Standard STD0005 (and updates),* (include IGMP version 1)

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

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

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

ISOC RFC 3376, *Internet Group Management Protocol, Version 3*

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* **3**~~

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.

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

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

3.1
ASCII
printable 7 bit character encoded in one byte

3.2
binary file
data block without formatting known to this protocol, i.e., non IEC 61162-1 formatted data, which can be transmitted with the protocol defined in 7.3 or in 7.5

Note 1 to entry: The term "binary file" 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

Note 1 to entry: 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 to entry: CRP are defined in Annex A.

Note 2 to entry: 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
atomic UDP transmission unit on the Ethernet as defined in ISOC RFC 768 and as constrained elsewhere in this document

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

Note 1 to entry: The types of Ethernet media that can be used for implementation of this document are defined in Clause 5.

3.7
function block
specified functionality implemented by equipment

Note 1 to entry: 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.

3.8
Internet Group Management Protocol
IGMP
communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships

Note 1 to entry: The IGMP is an integral part of IP multicast.

3.9
IGMP snooping
process of listening to Internet Group Management Protocol (IGMP) network traffic

3.10
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 1 to entry: The currently assigned numbers are listed in http://www.iana.org/assignments/port-numbers.

3.11
Internet protocol
IP
signalling protocol used and defined in ISOC RFC 791 (and updates)

3.12
message
collection of one or more sentences that are grouped by use of the TAG block grouping protocol or **4** mechanisms internal to the sentence, for instance by sequence numbers as in the TXT sentence

Note 1 to entry: A stand-alone sentence is a message.

3.13
message type
classification of IEC 61162-1 sentence formatters into SBM, MSM and CRP types

Note 1 to entry: SBM, MSM and CRP types are defined in Annex A.

Note 2 to entry: This document defines different requirements to the transmission of different message types.

3.14
multi-sentence message
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 to entry: Multi-sentence messages that are grouped together with a TAG construct are also a sentence group.

Note 2 to entry: MSM are defined in Annex A.

3.15
network
physical Ethernet network with one Internet address space, consisting only of the network nodes, switches, cables and supporting equipment such as power supply units

3.16
network function block
NF
function block responsible for physical connectivity to the network and connectivity to the transport layer as described in 4.3

3.17
network infrastructure
part of the network that provides a transmission path between network nodes

Note 1 to entry: The network nodes are not part of the network infrastructure.

3.18
network node
physical device connected to the network and which have an Internet address

Note 1 to entry: A network node is also called an "Internet host".

Note 2 to entry: A network node will normally correspond to equipment. "Equipment" is used in this document.

3.19
other network function block
ONF
function block that interfaces to the network, but which is not using the protocol definition in Clause 5, Clause 6 and Clause 7

EXAMPLE Real time streaming of radar and CCTV image transfer, or VDR sound transfer.

Note 1 to entry: Requirements as defined in 4.7 ensure that an ONF can co-reside with SF network nodes and function blocks that make use of this document's protocol.

3.20
PGN to network gateway function block
PNGF
function block that enables transfer of sentences between the network and devices that are compliant with the IEC 61162-3 serial data instrument network interface

3.21
PGN message
parameter group number message
message consisting of an 8-bit or 16-bit number that identifies each parameter group

Note 1 to entry: The parameter group number (PGN) is analogous to the three-character sentence formatter in IEC 61162-1. By definition, parameter groups identified by 16-bit parameter group numbers are broadcast to all addresses on the network. Parameter groups identified by 8-bit parameter group numbers may be used to direct data for use by a specific address.

[SOURCE: IEC 61162-3:2008, 3.1.21, modified – The word "message" has been added to the term, and the definition has been rephrased.]

3.22
sensor broadcast message
SBM
message consisting of only one sentence

Note 1 to entry: SBMs 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 to entry: SBMs are defined in Annex A.

3.23
sentence
standard information carrying unit as described in IEC 61162-1

3.24
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 to entry: A sentence group may consist of only one sentence.

Note 2 to entry: The grouping of sentences into sentence group is done by TAG block mechanisms.

Note 3 to entry: This document allows the explicit grouping of sentences by using coding in a datagram. This document 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.

3.25
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

Note 1 to entry: One SNGF may contain several system function blocks which each have their own SFI. Furthermore, the SNGF itself has an SFI for administrative purposes. **5**

3.26
system function block
SF
function block, identified by a unique system function ID (SFI), which is the only function block that can send information in a datagram format as defined in Clause 7

3.27
system function ID
SFI
parameter string as defined in 4.4.2

3.28
transmission group
pair of a multicast address and a port number that are used by an SF to transmit sentences

Note 1 to entry: The transmission groups are defined in Table 4, and Annex A defines default transmission groups for the SF.

3.29
transport annotate and group
TAG
formatted block of data, defined in NMEA 0183, which adds parameters to IEC 61162-1 sentences

Note 1 to entry: Annex B gives an overview of the TAG blocks used in this document.

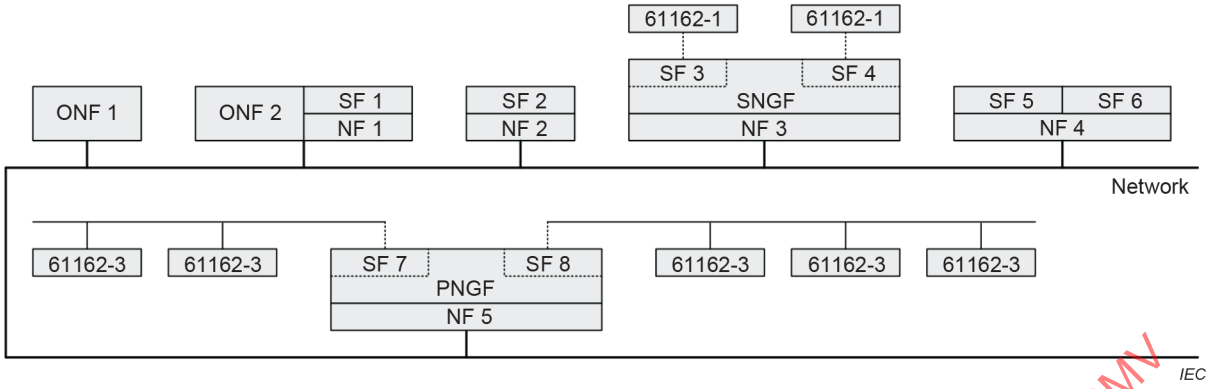
3.30
user datagram protocol
UDP
connection-less datagram protocol defined by ISOC RFC 768

Note 1 to entry: ISOC RFC 768 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 Clause 4.



Key

SF	system function block
NF	network function block
SNGF	serial to network gateway function block
ONF	other network function block
PNGF	PGN to network gateway function block

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 file) 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 document (SF3, SF4, SNGF and NF3);
- a system device function block presented by an IEC 61162-3 compliant equipment connected to network gateway function (PNGF); in this case, the PNGF will format outgoing sentences according to requirements of this document (SF7, SF8, PNGF and NF5);
- a device that does not send or receive IEC 61162-450 compliant data (sentences and/or binary file), 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), 4.5 (SNGF) and 4.6 (PNGF).
- 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 4.7.
- 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.

  NOTE This requirement applies only to devices on the network when the network is in normal operation. During commissioning or maintenance, when the system is not being used for safety-related navigation, other equipment can be temporarily connected to the network that does not comply with 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)

To avoid potential problems with certain network infrastructure equipment, repeater hubs shall not be used to interconnect components of an IEC 61162-450 network.

NOTE 1 Repeater hubs are network infrastructure devices without internal storage that repeat incoming datagrams onto all outgoing connections.

NOTE 2 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.

Switches used in an IEC 61162-450 network shall have means to filter network traffic using IGMP snooping. When the IGMP snooping is enabled and when a multicast datagram is received, the switch shall forward it only to the ports which have joined the same multicast group. The means which shall be provided to support multicast data filtering using IGMP snooping are the following:

- IGMP snooping shall be provided based on IGMPv1, IGMPv2 or IGMPv3; the selection of the IGMP version shall be based on highest version supported by all the connected nodes;
- multicast traffic filtering shall be provided based on IP multicast address;
- multicast data filtering shall not be enabled for the address range of 224.0.0.1 to 224.0.0.255 as recommended in RFC 4541.

In addition to or instead of multicast filtering techniques, such as IGMP snooping, it is also permitted to configure manually individual ports of the switches to block unnecessary traffic flow (for example to isolate simple sensors from ECDIS and radar).

See Annex D for IGMP snooping compatibility issues of nodes based on IEC 61162-450:2011[1]. **6**

Another possible method to filter and control network traffic is described in Annex E.

4.3 Network function (NF) requirements

4.3.1 General requirements

All equipment that implements a NF shall satisfy the requirements in Clause 5 and Clause 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 except for the equipment applicable standards or functions otherwise specified by the manufacturer. **7**

[1] This publication has been withdrawn.

Maximum input rate shall be specified as:

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

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

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

NOTE 1 "Received by" means datagrams that are received on all transmission groups that the equipment listens to.

NOTE 2 "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, for example by trained service engineer. It is allowed that the inspection is done through a simple network mechanism, such as a terminal emulator, as defined in this document 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 document 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 document, 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 document.
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 h 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 document, 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.
Italicised words are place-holders for data explained in the right hand column. 8	

A "syslog" packet shall not exceed 480 bytes and shall be sent as a single UDP datagram. The "syslog" packet for multiple occurrences of same message identity shall not be reported more often than once per minute. The "syslog" packet for any occurrence of message identity shall not be delayed more than 10 min.

This document does not specify requirements for equipment receiving syslog messages. This type of equipment would fall into the category of ONF. As Table 1 is a subset of the full ISOC RFC 5424 specification, implementers of such equipment shall 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 document have been assigned a message identity as defined in Table 2.

Table 2 – Syslog error message codes

Message identity	Description	Subclause
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 file error	7.3.9
201	PNGF buffer overflow	4.6.2
202	PGN message errors	7.4.2 and 7.4.4
203	No available address for devices	7.4.3.2

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

4.3.4 Provisions for network traffic filtering – IGMP

NOTE The purpose of the IGMP for this document is to provide the possibility to perform network traffic filtering based on IGMP snooping.

The manufacturer shall specify the version of IGMP as defined in ISOC RFC 1112, RFC 2236 and RFC 3376 that the NF supports. At least version 1 as defined in ISOC RFC 1112 shall be implemented.

See Annex D for compatibility issues of nodes based on IEC 61162-450:2011.

4.4 System function block (SF) requirements

4.4.1 General requirements

(see 8.4.1 and 8.2.3)

Equipment that implements an SF shall satisfy the following requirements:

- requirements in 6.2 shall be satisfied for all equipment implementing SF;
- implements at least one of the datagram types defined in Clause 7, but does not have to implement all of them;
- implemented datagram types shall be specified in the manufacture's documentation (see 7.1.1);
- requirements in 7.2 shall be satisfied for all equipment implementing IEC 61162-1 sentence transmitting or receiving function blocks;
- requirements in 7.3 shall be satisfied for equipment that implements an SF that can transmit or receive binary file data;
- requirements in 7.4 shall be satisfied for all equipment implementing IEC 61162-3 PGN message transmitting or receiving function blocks.

4.4.2 Implementing configurable transmission groups

(see 8.4.3)

As default, each SF shall be assigned a single transmission group/multicast address 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 and the SFs which are assigned to them within the valid range of multicast addresses defined in 5.4. A system integrator may, for example, split an SF into different transmission groups to support optimal load balancing for a given system. Where non-default configurations of SF and transmission groups are utilised, the details should be documented by the system integrator.

4.4.3 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. If the talker mnemonic is proprietary (i.e. consists of character "P" followed by a three-character manufacturer's mnemonic code), then two first characters are used as the "cc" characters in the SFI.

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 shall be avoided.

The numeric character string "xxxx" will be an instance number in the range "0001" to "9999". The numeric character string "9999" is reserved for an unconfigured 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. For implementation of interface redundancy (i.e. a single device is available through multiple paths in the network), the SF and related SFI shall be the same. The combination of source parameter codes "s" shall be unique for each path (see 7.2.3.4). **9**

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.

There may be multiple SF, each communication with their own SFI, assigned to a single IP address or MAC address.

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

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.

The SNGF may support one or more serial ports (see Figure 2). ~~Unless the SNGF implements multi-SF serial port, each serial port shall be implemented as a separate SF and assigned a separate SFI. If practical, the "cc" part of the SFI shall be based on the talker identifier in use by the serial port~~.

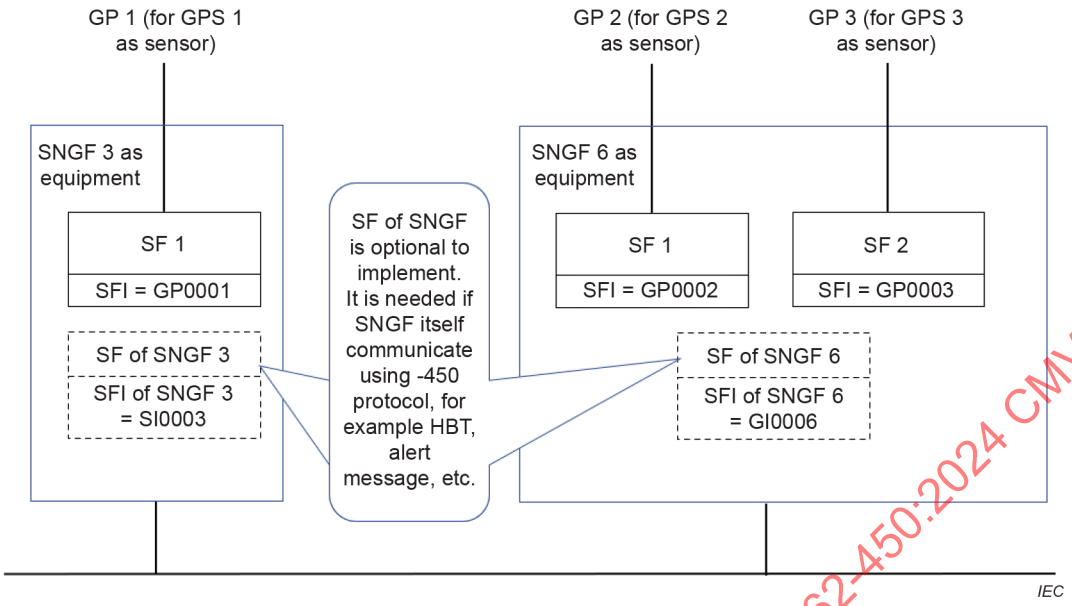


Figure 2 – SNGF examples

Each serial port shall be implemented as a separate SF and assigned a separate SFI, unless the SNGF implements multi-SF serial port (see 4.5.4 and Figure 3) or the SNGF implements interface redundancy. If practical, the "cc" part of the SFI shall be based on the talker identifier in use by the serial port; otherwise, an appropriate Talker Identifier shall be used.

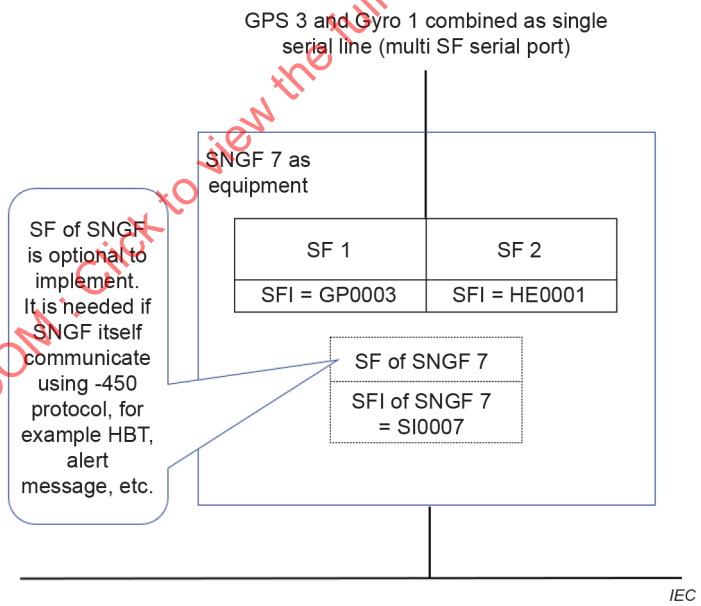


Figure 3 – SNGF example, multi SF serial port

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 the installation manual.

NOTE A typical filtering method would be to use the destination TAG “d” to determine what sentences in incoming datagrams need to be sent on the serial line. 10

All sentences, including those with unidentified or illegal content, as well as proprietary sentences shall be transmitted, unless subject to filtering **11**, from the SF associated with the serial port. Sentences with unidentified or illegal content shall be sent with a legal transport annotate and group (TAG) block as defined in 7.2.3, but with the raw received serial data following the TAG block.

As a destination, each serial port shall be associated with the corresponding SFI. Outgoing sentences shall be transmitted exactly as received in the datagram.

The SNGF may support one or more sources distinguished by different talker mnemonics at each serial port. Each source in a shared serial port shall be implemented as a separate SF and assigned a separate SFI. If practical, the "cc" part of the SFI shall be based on the talker mnemonic in use by each source in a shared serial port. As a destination, each source in a shared serial port shall be based on the SFI. Proprietary sentences include no talker identifier and, based on setup parameters, they shall use the same SFI as standardized sentences from the same source. The STN sentence is an additional qualifier for the following sentence. The STN sentence and the following sentence belong to the same SF and shall use the same SFI.

~~Proprietary sentences belong to the default SF of the associated serial port or to the SF determined by the preceding STN sentence.~~

Proprietary sentences received from serial port shall be associated with the SF of the serial port based on

- talker mnemonic used by non-proprietary sentences (see above paragraph), or
- the SF determined by the preceding STN sentence, or
- optionally, the SF set by the configuration for the serial port.

Malformed sentences (see 4.5.5) received from a serial port shall be associated with the SF either

- of the talker mnemonics, if available, of the malformed sentence, or
- of the talker mnemonic used by non-malformed sentences for the serial port, or
- set by the configuration for the malformed sentences.

The manufacturer shall declare in the installation manual which alternatives have been used for association with the SF for malformed sentences. **12**

The TAG block for source identification "s" shall be based on the SFI. If available, routing from a ~~450~~ **13** network to serial ports shall be based on the TAG block for destination identification "d".

The ~~default~~ **14** SFI of a SNGF used for administrative purposes, such as syslog, heartbeat (HBT) of SNGF itself, etc., **15** 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 the 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.~~ **16**

4.5.2 Serial line output buffer management

(see 8.5.2)

An SNGF function block shall provide an independent buffer for each separate SF implemented 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. Exception is a multi-sentence message or a TAG block group of sentences: they shall only be replaced in their entirety.

  NOTE When prioritizing AIS VDM and VDO sentences, the string beginning with the "!" character and ending with the 7th character of the encapsulation field is 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 single sentence, multi sentence message 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 or sentences at its position in the queue. This replacing shall not cause logging of an error nor sending anything to syslog.

  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 either transmit one IEC 61162-1 sentence or, if part of a multi sentence sequence, may transmit multiple IEC 61162-1 sentences per outgoing IEC 61162-450 datagram. The multi sentence sequence includes the case described in IEC 61162-1~~:2016, 7.3.9~~ Multi-sentence messages **17**, and the cases for which IEC 61162-1 requires a sentence sent prior sending another sentence. The datagram shall include the correct SFI, source identification (s:) and, if required, destination identification (d:).

4.5.4 Multi SF serial port

(see 8.5.4)

The SNGF is allowed to implement more than one SFs for any single serial line. Received sentences on this serial line with a valid talker mnemonic will be transmitted from one of the associated SFs dependent on the talker mnemonics. Each SF shall be assigned a separate SFI

and, as a destination, transmit outgoing sentences on the serial line according to the rules in 4.5.1.

Proprietary sentences received on the serial line include no talker identifier. It shall be determined by setup parameters from what SF they shall be transmitted.

Unidentified data from the serial line shall be sent from all SFs associated with the serial port. This sending of unidentified data shall not cause logging of an error nor sending anything to syslog.

4.5.5 Handling malformed data received on serial line

(see 8.5.5)

The SNGF is intended as a remote serial data converter with minimum data processing. For each of the cases below, the SNGF shall send a datagram with the malformed data as required by 4.5.1 and 4.5.4. If the formatted message exceeds the maximum datagram length (see 6.2.4), the data shall be truncated from the end. The following cases shall cause a message containing the malformed data to be sent:

1) if data has been received before a start character;
2) if data has been received after a valid start character and the maximum sentence and TAG block length has been exceeded;
3) if data has been received after a valid start character and end of line (CR,LF) has not been received after 1 s;
4) if a reserved character has been received and not having been appropriately escaped;
5) if random binary data is received on the serial line.

"Start character" is a valid start of sentence ("$", "!") or TAG block start character.

4.6 PGN to network gateway function (PNGF) requirements

(see 8.12)

4.6.1 General requirements

(see 8.12)

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

The ~~default~~ **14** SFI of a PNGF used for administrative purposes, such as syslog, heartbeat (HBT) of PNGF itself, etc., **15** shall use the talker mnemonic "SI".

The PNGF may implement different types of filtering based on the PGN messages from and to IEC 61162-3 network. Any filtering methods shall be described in the manufacturer's documentation.

NOTE The accurate timing between PGN messages available in the IEC 61162-3 network is not supported when the same is converted into IEC 61162-450 network.

4.6.2 Output buffer management from IEC 61162-450 network to IEC 61162-3 network

(see 8.12)

A PNGF function block shall provide an independent buffer for each IEC 61162-3 network it can send into. The manufacturer shall specify the maximum buffer capacity for each port. The maximum capacity may be configurable at installation.

PNGF buffer management shall be based on the IEC 61162-3 priority included into each message. The manufacturer shall describe the method in documentation.

If the buffer is full and a PGN message is discarded, it shall be recorded as specified in 4.3.3.

4.6.3 Datagram output requirements

(see 8.12)

The PNGF shall format outgoing messages as defined in 7.4.1.

The PNGF shall transmit one IEC 61162-3 PGN message per outgoing IEC 61162-450 datagram to minimise delays.

4.6.4 PGN group number

(see 8.12)

A PGN group is defined as a logical group of devices that can share the information and message. A message from a device is broadcasted to all devices that belong to the same PGN group. A device may belong to more than one PGN groups. The maximum number of PGN groups is no more than four. The PGN group may be used for filtering of messages (see 4.6.1).

4.7 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 document 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 describing the impact of the ONF 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 Std 802.3™-2015, 14.7 and Clause 27, shall be followed. Also refer to IEEE Std 802.3-2015, informative Annex 67.~~ **18**

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

The physical layer requirement for IEC 61162-3 ports of the PNGF shall be compliant with IEC 61162-3:2008, Clause 4.

Table 3 – Interfaces, connectors and cables 19

IEEE 802.3 interface	Max. network segment link distance	Mechanical device interface connector type (protected environment)	Pin assignment	Cable category, minimum
100BASE-~~TXS~~TX IEEE Std 802.3-~~2015, 14.7 and~~ 2022 Clauses 24 and 25	100 m	IEC 60603-7-3, 8-way shielded modular connector Refer to ~~IEEE Std 802.3-2015, Clause 3,~~ IEC 60603-7:2020, Figures 1 through 5, and IEEE Std 802.3:2022, Clause 25	b	CAT5 STP Two shielded twisted pairs ANSI/TIA~~/EIA~~-568-A, ANSI/TIA~~/EIA~~-568-B or ISO/IEC 11801 (class D).
(not specified)	a	Terminal block	b	CAT5 STP Two shielded twisted pairs
100BASE-SX IEEE Std 802.3-~~2015~~2022, 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 Std 802.3:~~2015~~2022, Clause 40	100 m	IEC 60603-7-7, 8-way shielded modular connector Refer to ~~IEEE Std 802.3-2015, Clause 3, and~~ IEC 60603-7:2020, Figures 1 through 5. ~~See IEEE Std 802.3/25~~	c	CAT5 STP Four shielded twisted pairs ANSI/TIA~~/EIA~~-568-A, ANSI/TIA~~/EIA~~-568-B or ISO/IEC 11801 (Class D).
1000BASE-SX IEEE Std 802.3-~~2015~~2022, Clause 38	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 for copper network cable. And similar rugged connector should be considered for external fibre optic connections.				

[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 8 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 Std 802.3-~~2015~~2022, 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 8 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 Std 802.3-~~2015~~2022, 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 IPv4 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;

The following protocols may be supported depending upon the requirements of the equipment: **20**

- UDP – User datagram Protocol as described in ISOC RFC 768;

  NOTE 1 For equipment that is purely an ONF (neither SF nor SNGF), this is not necessarily required. Such an ONF device can communicate only over TCP or only over UDP, or perhaps even with raw IP or ICMP packets. **21**

- UDP Multicast – Host groups as described in ISOC RFC 966 and Host extensions as described in ISOC RFC 1112;

  NOTE 2 For equipment that is purely an ONF (neither SF nor SNGF), this is not necessarily required. Such an ONF device can communicate only over TCP or only over UDP, or perhaps even with raw IP or ICMP packets. **22**

- TCP – Transmission Control Protocol as described in ISOC RFC 793;

  NOTE 3 TCP is generally not required for SF and SNGF functions. Whilst it can make sense for some equipment to support TCP, this document does not require TCP to be used. **23**

- ICMP – Internet Control Message Protocol as described in ISOC RFC 792;

  NOTE 4 There is no requirement in this document relating to ICMP. **24**

- IGMP – Internet Group Management Protocol as described in ISOC RFC 1112, RFC 2236 or RFC 3376;

  NOTE 5 It is sensible to support IGMP snooping particularly for SF and SNGF devices, but it is not strictly required within this document. See D.2.1. **25**

5.3 IP address assignment for equipment

(see 8.7.3)

Means shall be provided to configure the equipment to any of the addresses reserved for use in private networks as described in ISOC RFC 1918 with any valid network address mask. The default sub-net mask shall be set appropriately for 192.168.0.0/24 (legacy class C). The assigned IP address shall remain fixed during normal operation of the equipment, including powering the equipment down and up.

~~Specific 450-Nodes may choose to exclude a few sub-nets to facilitate internal sub-nets (internal to the equipment) which shall be documented.~~ A 450-Node may reserve sub-nets for non-450 use, for example, for internal use (internal to the equipment) or for other interfaces. All reserved sub-nets shall be documented **26**. The following sub-nets shall always be available to the IEC 61162-450 network: 192.168.0.0/24 – 192.168.10.0/24 and 172.16.0.0/16 (class B).

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).

The multicast address range 239.192.0.57 to 239.192.0.64 is used for interconnection with IEC 61162-3 networks.

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

NOTE 1 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~~ allocates sub-ranges when defining scopes for private use.

NOTE 2 ~~The default TTL (i.e. number of hops) is 1 for multicast.~~ The multicast time to live (TTL i.e. number of hops) is adaptable to allow transmission over multiple network routers. The default TTL value is 64 **27**. The sub-net mask is set appropriately for a class C (local area network).

5.5 Device address for instrument networks

Means shall be provided to assign a device address range from 0 to 251 when the PNGF transmits to an IEC 61162-3 network. The device address may be set automatically.

6 Transport layer specification

(see 8.8)

6.1 General

Clause 6 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 of Clause 6 applies to both, but shall be tested independently as described in 7.6.

An example of the structure of an Ethernet frame with a IEC 61162-450 sentence is given in Figure 4. 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).

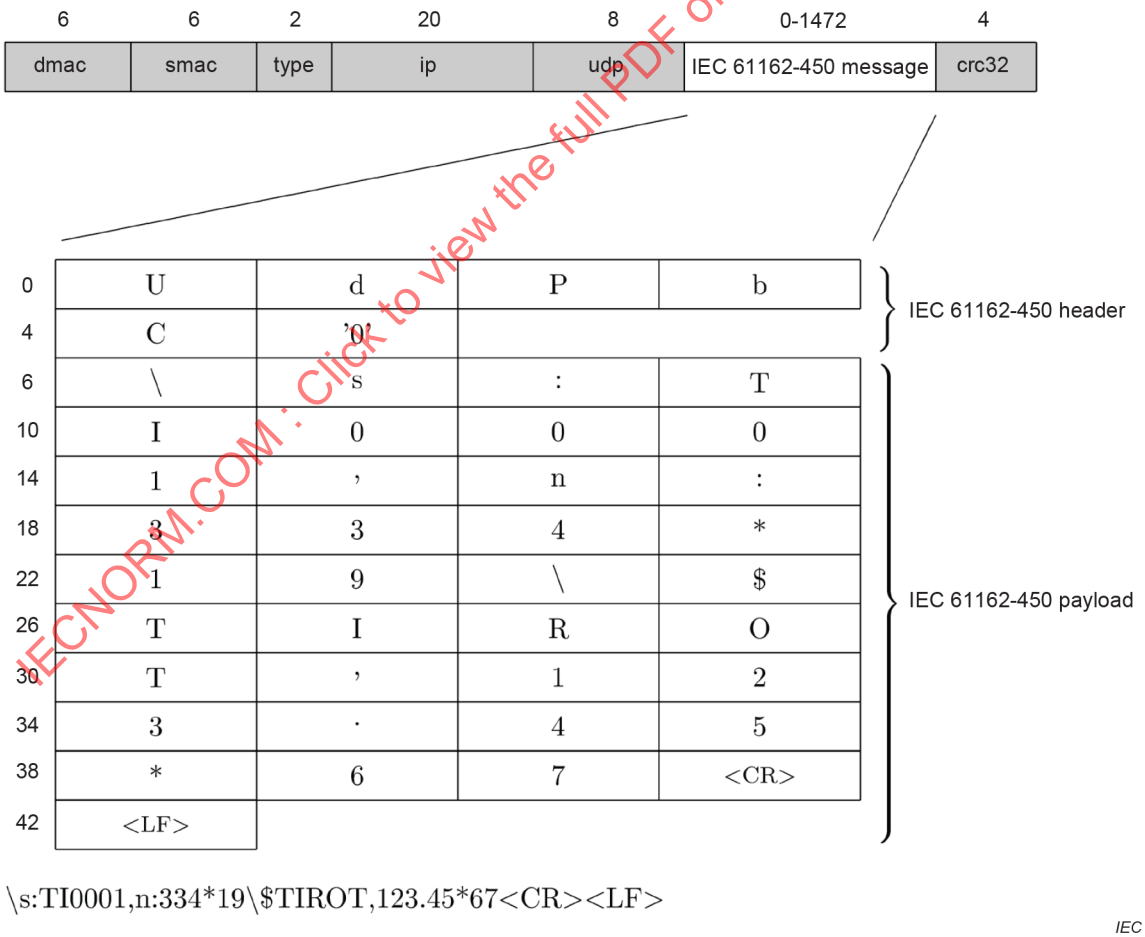


Figure 4 – Ethernet frame example for a SBM from a rate of turn sensor

6.2 UDP messages

6.2.1 UDP multicast protocol

UDP Multicast – IP multicast is a technique for many-to-many communication over an IP infrastructure in a network. The destination nodes send join and may send leave messages. IP multicast scales to a larger receiver population by not requiring prior knowledge of who or how many receivers there are. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers only when necessary. The most common transport layer protocol to use multicast addressing is User Datagram Protocol (UDP).

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

6.2.2 Use of multicast addresses and port numbers

Port numbers shall be allocated from the dynamic port range that the internet assigned number authority (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. If provided by the equipment, the default ~~multicast address or destination port number~~ transmission group can be changed by the parameter setup system of the equipment to ~~the multicast addresses or destination port numbers of the transmission groups USR1 to USR8, RCOM, PROP~~ any transmission group in Table 4 or any in Table 5 (for example to support use of same transmission group for both "binary file" and related sentences, for example ECDIS route exchange and RRT-sentence). **28**

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 61996-1	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	User defined transmission group 1	239.192.0.9	60009
USR2	User defined transmission group 2	239.192.0.10	60010
USR3	User defined transmission group 3	239.192.0.11	60011
USR4	User defined transmission group 4	239.192.0.12	60012
USR5	User defined transmission group 5	239.192.0.13	60013
USR6	User defined transmission group 6	239.192.0.14	60014
USR7	User defined transmission group 7	239.192.0.15	60015
~~USR1 to~~ USR8	User defined transmission group ~~1 to~~ 8	~~239.192.0.9 to~~ 239.192.0.16	~~60009 to~~ 60016 **29**
BAM1 ~~to BAM2~~	~~Optionally,~~ BAM compliant alert source reporting to CAM group 1	239.192.0.17 ~~to 239.192.0.18~~	60017 ~~to 60018~~
BAM2	BAM compliant alert source reporting to CAM group 2	239.192.0.18	60018
CAM1 ~~to CAM2~~	CAM of the BAM group 1	239.192.0.19 ~~to 239.192.0.20~~	60019 ~~to 60020~~
CAM2	CAM of the BAM group 2	239.192.0.20	60020 **29**
NETA	Network administration, e.g. SFI collision detection	239.192.0.56	60056
PGP1 ~~to PGP4~~	~~Primary~~ PGN Group 1 ~~to PGN Group 4~~	239.192.0.57 ~~to 239.192.0.60~~	60057 ~~to 60060~~
PGP2	PGN Group 2	239.192.0.58	60058
PGP3	PGN Group 3	239.192.0.59	60059
PGP4	PGN Group 4	239.192.0.60	60060 **29**
PGB1 ~~to PGB4~~	Backup PGN group 1 ~~to PGN Group 4~~	239.192.0.61 ~~to 239.192.0.64~~	60061 ~~to 60064~~
PGB2	Backup PGN group 2	239.192.0.62	60062
PGB3	Backup PGN group 3	239.192.0.63	60063
PGB4	Backup PGN group 4	239.192.0.64	60064 **29**

NOTE 1 The USR1 to USR8 transmission groups can be used, for example, for proprietary data in binary format.

~~NOTE 2 BAM1/BAM2 and CAM1/CAM2 are available for system integrators to balance the traffic, for example higher volume radar in BAM1/CAM1 and low volume sensor, for example gyro, in BAM2/CAM2.~~

NOTE 2 To balance the traffic or to provide backward compatibility, in addition to the implementation of mandatory use of BAM1/BAM2 and CAM1/CAM2, BAM related communication can be configured to use e.g. SATD or NAVD transmission groups. **30**

Table 5 defines multicast addresses and destination port numbers that shall be used when transmitting binary file data. If provided by the equipment, the default multicast address or

destination port number can be changed by the parameter setup system of the equipment to the multicast addresses or destination port numbers of the transmission groups USR1 to USR8, RCOM, PROP in Table 4 or any in Table 5 (for example to support use of same transmission group for both "binary file" and related sentences).

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

Category	Multicast address	Destination port
Non re-transmittable binary file transfer group 1 [a]	239.192.0.21 ~~to 239.192.0.25~~	60021 ~~to 60025~~
Non re-transmittable binary file transfer group 2 [a]	239.192.0.22	60022
Non re-transmittable binary file transfer group 3 [a]	239.192.0.23	60023
Non re-transmittable binary file transfer group 4 [a]	239.192.0.24	60024
Non re-transmittable binary file transfer group 5 [a]	239.192.0.25	60025 **29**
Re-transmittable binary file transfer group 1 [b]	239.192.0.26 ~~to 239.192.0.30~~	60026 ~~to 60030~~
Re-transmittable binary file transfer group 2 [b]	239.192.0.27	60027
Re-transmittable binary file transfer group 3 [b]	239.192.0.28	60028
Re-transmittable binary file transfer group 4 [b]	239.192.0.29	60029
Re-transmittable binary file transfer group 5 [b]	239.192.0.30	60030 **29**

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

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

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

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

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

Category	Multicast address	Destination port
Syslog	239.192.0.254	514
Sending to syslog can use multicast or UDP unicast. Some switches can support only UDP unicast.		

The addresses 239.192.0.31 to 239.192.0.55 are reserved for future expansion.

~~It may be noted that~~ IANA has defined that port range 49152 to 65535 is reserved for dynamic and private use. The specific ports for this document are within this IANA range. ~~It should be noted that~~ Operating systems also use this IANA range for their internal use as ephemeral ports. This double use may cause port number conflicts resulting for lost communication of IEC 61162-450 messages. It is recommended to consider limiting the ephemeral port range of the operating system of equipment connected to an IEC 61162-450 network to avoid port number conflicts.

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 kB 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 datagrams 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 files as described in 7.3;
- "`RrUdP`" for transmission of re-transmittable binary files as described in 7.3;
- "`NkPgN`" for transmission of IEC 61162-3 PGN messages as described in 7.4;

All TCP/IP datagrams shall contain the following string, followed by a null character (all bits set to zero) as the first six bytes of the datagram:

- "`RrTcP`" for transmission of binary files as described in 7.6.

NOTE 1 Datagram means packet in this context.

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

NOTE 2 Future editions of IEC 61162-450 can 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 0183:2008, Section 7 (see also Annex B), containing the parameter codes described in 7.2.3.3 to 7.2.3.8. Adding of TAG blocks with parameter codes happens between existing TAG blocks with parameter codes and the start of IEC 61162-1 sentence. 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 (i.e. parameter value closest to the start of IEC 61162-1 sentence) shall be used.~~

~~In this document, 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.~~

Each sentence shall be preceded with one or more TAG blocks as defined in Annex B, containing one or more of the parameter codes described in 7.2.3.3 to 7.2.3.8. Adding of TAG blocks with parameter codes happens after the last existing TAG block.

An example of applying one and more parameter code "s" is as follows.

Original source = GP0001

```
\s:GP0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\\s:TT0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A
*27<CR><LF>
```

If a parameter code is assigned a value more than once in all TAG blocks and only one value is expected, the parameter code value closest to the start of the IEC 61162-1 sentence and IEC 61162-450 conformant (see 7.2.3.4) shall be used.

NOTE The IEC 61162-450 conformant parameter code "s" can be added by SNGF or ONF.

In case of multiple source parameter codes "s", the original source is the right most “s” parameter in the left most TAG block from the start of the IEC 61162-1 sentence and IEC 61162-450 conformant (see 7.2.3.4).

If a device modifies the content of a received IEC 61162-1 sentence, then the TAG blocks containing source parameter codes "s" shall be removed and replaced by a TAG block containing a source parameter code "s" based upon the SFI of the device which did the modification.

It is possible that a TAG block, or a group with two or more TAG blocks, may contain multiple destinations. Each listener is responsible for recognizing its own identifier, and each listener would treat the TAG block line (see Clause B.5) or group of TAG block lines as addressed to that unit.

- First example

  Two valid datagrams are shown below. The second datagram shows two occurrences of parameter code "s", where the first occurrence (AC1000) is the original source and the second occurrence closest to the sentence (BC1000) identifies the device that this sentence passed through.

```
\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,
0*7C

\s:AC1000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,
3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
```

- Second example

  The datagram below shows the case when one parameter code "s" (002300000) is from a non IEC 61162-450 conformant source. A receiver can use or ignore this non IEC 61162-450 conformant source. Note that parameter code "s" (BC1000) closest to the sentence is IEC 61162-450 conformant.

```
\s:002300000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,
,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
```

For compliance with this document, all TAG block parameter codes are set at the time of installation and shall not be dynamically configurable during normal operation.

NOTE The control sentences for changing parameter codes in NMEA 0183 are not used during normal operation. **31**

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.

A TAG block may contain parameter codes and their values known and/or not known by the receiver. Further there may be multiple occurrences of a parameter code. The examples below assist in correct interpretation.

If the value of the "s" parameter code is not understood by the receiver, for example not encoded as in this document (see 7.2.3.4), then the message shall be ignored, for example:

```
\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
```

If the "s" parameter code is available twice, the first instance encoded as in this document (see 7.2.3.4) and the second instance not understood by the receiver, then the message shall be accepted based on the parameter code understood by the receiver and the existence of the not understood parameter code is ignored, for example

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R
=23BTB3F00Uh,0*7C
```

NOTE The above example could be the result of a node adding its TAG block in front of existing TAG blocks instead of in front of the start of the sentence (see 7.3.2.1).

When the "s" parameter code is available twice, only the closest to the start of the IEC 61162-1 sentence is used (in the example below s:AI0001) and the other is ignored, for example.

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:AI0001*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23
BTB3F00Uh,0*7C
```

If the message contains known (for instance "s") and unknown parameter codes (for instance "c" defined in this document, but not implemented by the receiver), then the message shall be accepted and the unknown parameter code shall be ignored, for example:

```
\s:BC1000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
```

If all parameter codes are unknown for the receiver (for instance "h" is not defined in this standard and "c" is not implemented by the receiver), then the message shall be ignored, for example:

```
\h:002300000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*
37
```

32

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.

NOTE An example of optional use is to associate or link related sentences together, for example GGA and VTG sentences from a GNSS receiver could be grouped together. **33**

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

A valid MSM type sentence where internal data fields specify 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 value of the "g" parameter code is divided into three fields. The fields within the "g" parameters are separated using "-".as delimiter. The uses 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. This is used to differentiate between different groups of TAG blocks and sentences.

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.,~~ 99 is used, hence the valid range is 1 to 99, inclusive. The receiver shall make no assumption about the initial value of the group code.

When used, the "g" parameter code shall be the first parameter code in the TAG block.

All grouped sentence of type MSM of a message shall be included in the same group of linked lines, but the group of linked lines may include also other than the MSM type sentences.

It is recommended that grouped sentences are sent in as few datagrams as possible to minimise the probability of out of order packets being received.

Below is an example of compliant use. In this example, four VDM sentences are grouped (first 2 are individual and last 2 are part of MSM).

```
\g:1-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
\g:2-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
\g:3-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\g:4-4-45*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

Below is an example of non-compliant use of grouping. In this example, the grouping of the first three lines does not include the second part of the MSM message.

```
\g:1-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F 00Uh,0*7C
\g:2-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD 8@Ip,0*37
\g:3-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\d:AB0001, d:AB0002,s:BC1000*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

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,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-46,s:IN0001*3F\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D
\g:2-2-46,s:IN0001*3C\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20
```

Additional requirements for use of "g" parameter code are:

1) all grouped TAG block lines shall be sent in increasing sequence as indicated by the first numeric value in the “g” parameter code;
2) grouped TAG block lines shall not be sent with more than one second delay between each TAG block line.

Receivers may ignore the complete group if the above two requirements are not met.

An example of non-compliant use of the first requirement is a variant of the previous example with an incorrect sequence (two lines are sent in the wrong order):

```
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-34,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
```

34

7.2.3.4 Source identification – s

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

Received messages without any known "s" parameter code shall be ignored. 35

Multiple "s" parameter codes may be used to indicate the path a message takes. The first or right-most “s” parameter code is the SFI of the device which creates the message. Subsequent equipment SFIs for source parameter codes may be added to the left to indicate the path the message takes.

For example, a SNGF may add its SFI as a source parameter to a message to indicate that the message originates from a particular SNGF, see Figure 2 and Figure 3 for an example for the configuration of sensor SFI and SNGF SFI. 36

7.2.3.5 Destination identification – d

The "d" parameter code ~~is~~ shall be provided for CRP type sentences and optional for other types 37 and shall, if used, contain the system function ID (SFI, see 4.4.2) corresponding to the intended recipient of the sentence.

If no destination parameter code is present, then all devices that receive this sentence shall process it.

Multiple "d" parameter codes may be specified, if more than one ~~receiver~~ intended recipient exists. All "d" parameter codes in a TAG block group apply collectively to all sentences associated with the TAG block group. Listed recipients shall process and react on the content of the associated sentences.

NOTE This can 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~~ are not intended to take any further action on the contents. 38

If there is a need to specify more "d" parameter codes than can fit into a single TAG block, the list of "d" parameter codes shall be divided over more than one TAG block. If these TAG blocks are in the same TAG block line, there is no need to link them using the "g" parameter code. For example, two TAG blocks, one with 7 and another with 2 "d" parameter codes:

```
\s:IN0001,d:AB0001,d:AB0002,d:AB0003,d:AB0004,d:AB0005,d:AB0006,d:AB0007*hh\\
d:AB0008,d:AB0009*hh\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
```

38

7.2.3.6 Line count parameter – n

(see 8.9.4.1)

The "n" parameter code may be used to assign a sequence number to ~~each~~ selected sentences 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~~ the selected sentences 39 transmitted from this system function block. The parameter value shall be reset to one ("1") ~~when it reaches 1 000, i.e.,~~ after 999 is used, hence the valid range is 1 to 999, inclusive. 40

~~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).~~

EXAMPLE 1 A GPS receiver sends its sentences to everybody. Selected sentences, all sentence or a sub-set of sent sentences, can be supported by a single line counter.

EXAMPLE 2 An equipment implements ECDIS and track control. Selected sentences sent from the track control function to the autopilot can be supported by a line counter. All other sentences sent by the equipment are without the line count parameter code.

EXAMPLE 3 A central display dimming controller sends DDC sentences separately for multiple monitors. Each monitor is identified using the d parameter code. Each flow of DDC sentences can be supported by separate line counters. 41

7.2.3.7 Text string parameter – t (proprietary data)

The "t" parameter code is a free text field. This document 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,s:TI0001,n:334,t:pmmma;MD5;0x12345678*0D\
```

7.2.3.8 General authentication – a

(see 8.9.5)

The authentication parameter code is used to sign a message with a password. Just sending a password with the message would reveal the password to anyone listening to the traffic. Sending a signature digest instead keeps the password secret.

Any kind of messages may be signed using the authentication parameter code. The authentication parameter code does not change the original message in any way. It is always possible to ignore this TAG and use the rest of the message.

EXAMPLE Sign configuration commands for devices or commands to the autopilot.

The authentication parameter code provides a standardized mechanism for passing the digest with the message. Password management is outside of the scope of this document. One way is to use pre-shared keys (PSK) on the participating devices.

NOTE 1 The pre-shared key could be 32 alphanumeric characters, for example "Alea iacta est 1234567890".

This parameter code is optional and should only be used where special safety concerns make it useful. If this TAG is provided, then the manufacturer's documentation shall describe which of the optional types of methods available to calculate a signature are supported by the equipment and shall describe how to share keys.

The format of the TAG block is:

\a:c-h--h*hh\

in which

c is the type of optional method to calculate signature

1) MD5,

2) SHA-256, and **42**

P) proprietary;

h-h is the hexadecimal representation of the signature, for example 32 hexacodes for MD5.

An example of the TAG block is:

\a:1-123456789abcdef67890123456789012*hh\

Types of methods to calculate signature are as follows.

1) MD5

The signature is a MD5 digest of the password plus the message. MD5 is a one-way message-digest algorithm (RFC 1321). The full length of the signature is 128 bits or 32 hexadecimal codes. The MD5 is commonly used for storing passwords in Unix-systems. Revealing the digest does not expose the password.

NOTE 2 See http://tools.ietf.org/html/rfc1321 and http://en.wikipedia.org/wiki/MD5.

The security provided in 2023 by MD5 is weak. For new design, the SHA-256 is recommended. **43**

2) SHA-256

The signature is a SHA-256 digest of the password plus the message. The full length of the signature is 256 bits or 64 hexadecimal codes. Revealing the digest does not expose the password. **42**

P) Proprietary

The signature is a proprietary digest of the password plus the message. This alternative requires that both parties use the same manufacturer specified proprietary method.

The authentication parameter code value is calculated by concatenating a pre-shared key and all TAG blocks and sentences in the message as a single string to be used by the method of the signature calculation to produce the signature digest. "Carriage returns" and "line feeds" from the sentences are not included into the input string.

When the authentication parameter code "a" is used, it shall be in its own authentication TAG block, with no other parameter codes. For a grouped message consisting of several lines of TAG blocks and sentences, the authentication TAG block shall be placed on the first line of the group. Within the first line, the authentication TAG block shall be placed as the last TAG block, and before any sentence on that line. This also applies to a single line TAG block and sentence with no grouping.

An example of use of authentication TAG block:

Message consisting of two grouped sentences to be protected by authentication:

\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Pre-shared key to be used for signature calculation:

Alea iacta est 1234567890

Resulting input string for signature calculation:

Alea iacta est 1234567890\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Message to be sent including signature, method MD5:

\g:1-2-23,s:IN0001*3C\\a:2-851E40CC1CB7E3B39D961D7CF10BD8D3*44\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Messages without authentication parameter codes are accepted unless the set-up parameters of the receiver are explicitly set to require authentication on incoming packets.

If the device is set to require authentication on incoming packets, then packets without valid authentication shall be dropped.

NOTE 3 SNGF are advised to avoid transmitting passwords in the clear from SPW sentences received over a serial connection.

7.2.3.9 Destination cluster identification – x

(see 8.9.4.1 and 8.9.4.2)

The parameter code "x" is optional unless required by an equipment standard (e.g. BAM related communication). See Annex H for cluster identifiers. **44**

7.2.3.10 Source cluster identification – z

(see 8.9.4.1)

The parameter code "z" is optional unless required by an equipment standard. See Annex H for cluster identifiers. **44**

7.2.4 Requirements for processing incoming datagrams

For datagrams intended for processing by the SF, any syntax error in a TAG block or in a sentence shall make the receiving equipment discard the complete datagram without any other further processing than specified in 7.2.5. The exception is a SNGF which ~~shall~~ may retransmit the faulty sentences **45** to the appropriate serial ~~SF~~ port, if it can be determined from a valid destination field, or to all connected serial ~~SFs~~ ports, if no destination field is specified.

7.2.5 Error logging for processing incoming datagrams

(see 8.10)

The equipment shall maintain counts of errors detected in processing datagrams containing IEC 61162-1 sentences. 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 7.2.3.9.

7.3 Binary file transfer using UDP multicast – Single transmitter, multiple receivers

(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 as files, can be transmitted to one or more receivers. This protocol supports the transmission of files from zero bytes up to 4 billion files blocks.

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

- non re-transmittable transfers where sender sends the complete binary file without any feed-back from receiver;
- re-transmittable transfers where limited feed-back from one receiver identified by DestID can be used to re-transmit certain parts of the binary file while other parallel receivers operate as passive receive-only receivers of the binary file.

NOTE The advantage of non-re-transmittable and re-transmittable binary file transfer methods over the TCP/IP is the possibility of multiple parallel receivers of the same transmission.

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 until 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.
WORD	One unsigned 16-bit integer (in range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTES, 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/IEC 8859-1 (ISO Latin 1).

7.3.2 Binary file structure

7.3.2.1 General

The binary files are transmitted over the network in one or more datagrams. The binary file structure is a sequential and unpadded stream of bytes divided into three main groups: header, binary file descriptor and binary file data (see Table 8 and Table 9). The header is needed for synchronisation and data integrity validation. The binary file descriptor is needed for the description of the binary file data and is only used in the first datagram for each binary file transfer.

7.3.2.2 Non re-transmittable and re-transmittable transfers

Table 8 – Binary file structure

61162-450 header (see 7.3.3)
Binary file descriptor (only in first datagram) (see 7.3.4)

Binary file data fragment (see 7.3.5)
61162-450 header (zero or more)
Binary file data fragment (zero or more)

A minimum binary file transmission using non re-transmittable or re-transmittable transfer will consist of the three first blocks where the binary file fragment may have zero length.

The header shall be repeated as the first element of any datagram that contains binary file data fragments.

7.3.3 61162-450 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 binary file transfers, and how much data loss occurs. In addition, the header is used to provide a re-transmission mechanism for re-transmittable binary file transfer.

The 61162-450 header format is defined in Table 9.

Table 9 – 61162-450 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 2 is defined in this document. Extensions and/or modified versions may update this value.
HeaderLength	WORD	Defines the length of the header in bytes. This is at least the length of the header. Future editions of IEC 61162-450 may append additional fields to this header as long as these additional fields are compatible with the definition of the header in this document. Receivers which are not aware of these additional fields shall ignore them.
SrcID	STRING[6]	Define the source system identifier in format "ccxxxx" (see 4.4.2).
DestID	STRING[6]	For re-transmittable, defines the destination system identifier in format "ccxxxx", for example "VR0001" for VDR (see 4.4.2). When Destid = "XXXXXX", then there is no assigned destination.
Type	WORD	Identifies the information in the header.
BlockID	DWORD	Binary file block identifier. The initial value is randomly generated within a range 0 to (2^{32} – 1 = 4294967295) and is incremented by 1 after a whole block is transmitted.
SequenceNum	DWORD	Defines the sequence number of the binary file 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 binary file data block. When SequenceNum is equal to MaxSequence, it means that this datagram is the last datagram of the data block. The ~~Maxseq~~ MaxSequence is used only for DATA type message. For other messages (QUERY,ACK), this field shall be 0.
Device	BYTE	Data source (device) as binary value, 1 for equipment 1, 2 for 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

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

7.3.3.2 Use of header token

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

- "RaUdP" – Simple binary file transfer service with UDP Multicast;
- "RrUdP" – Re-transmittable binary file transfer service with UDP Multicast.

7.3.3.3 Version

Defines the header version. It shall be set to 2 for this document.

7.3.3.4 Destination identifier

For transmissions to one specific receiver, the field shall contain the destination SPI. The field shall be "XXXXXX" for no specific destination.

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 file data including file 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 a binary file sender sends a QUERY message if there is no ACK message for 1 s after a last datagram of the binary file 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 file is received without any error or when errors occurred during the binary file 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 Binary file block identifier

Block identifier is used to identify each binary file block. Since a binary file block is fragmented into several datagrams, the block identifier is used to assemble one or more datagrams into a binary file 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.

7.3.3.8 Identification of separate binary file transfer

Each single binary file transfer shall be identified by a unique combination of SrcID, Device, Channel and BlockID (see Table 9).

NOTE If a single SrcID has multiple needs to send binary files (e.g. ECDIS sending screen image, chart source information and route exchange), then each single binary file 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.

7.3.4 Binary file descriptor structure

The binary file descriptor format is defined in Table 10.

Table 10 – Binary file descriptor format

Data item	TYPE	Description
Length	DWORD	Defines the binary file descriptor length in bytes. This is at least the length of the header including the reserved bytes. Future editions of IEC 61162-450 may append additional fields to this file descriptor as long as these additional fields are compatible with the definition of the file descriptor in this document. Receivers which are not aware of these additional fields shall ignore them.
fileLength	DWORD	Defines the length of the full binary file 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.
AckDestPort	WORD	Port number to be used to acknowledge. Allowed port numbers are within the range from 60006, 60008 to 60016, 60021 to 60030 (see 7.3.8.9).
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.
StatusLength	WORD	The length of the "Status and information text" field in bytes.
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 file header contents as this is handled by the UDP layer. In this document, 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 ISOC RFC 4289.		

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 binary file 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
XML	xml	application/xml

7.3.5 Binary file data fragment

The package data format is defined in Table 12.

Table 12 – Binary file 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 binary file fragment is the length of the UDP datagram (as obtained from the UDP header) minus any headers that are inserted in front of the binary file fragment. All datagrams, except the first datagram of the binary file which requires two headers (Header + binary File Descriptor), carry only one header (Header).

The binary file 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 file transfer

7.3.6.1 Non re-transmittable sender process

The following steps are performed for the basic sending process (see Figure 5):

a) a sender process waits until it gets a binary file block;

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

c) a binary file descriptor is composed according to Table 10;

d) a binary file block is split into datagrams whose size is not more than 1 472 bytes and each datagram is put into the sending buffer;

e) get the first datagram of the binary file block;

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

g) compose a header including token, source ID, destination ID and maximum sequence number according Table 9;

h) send a datagram to the network;

i) if all datagrams of the binary file block are not transmitted, get the next datagram and go to step f);

j) otherwise, then go to step a).

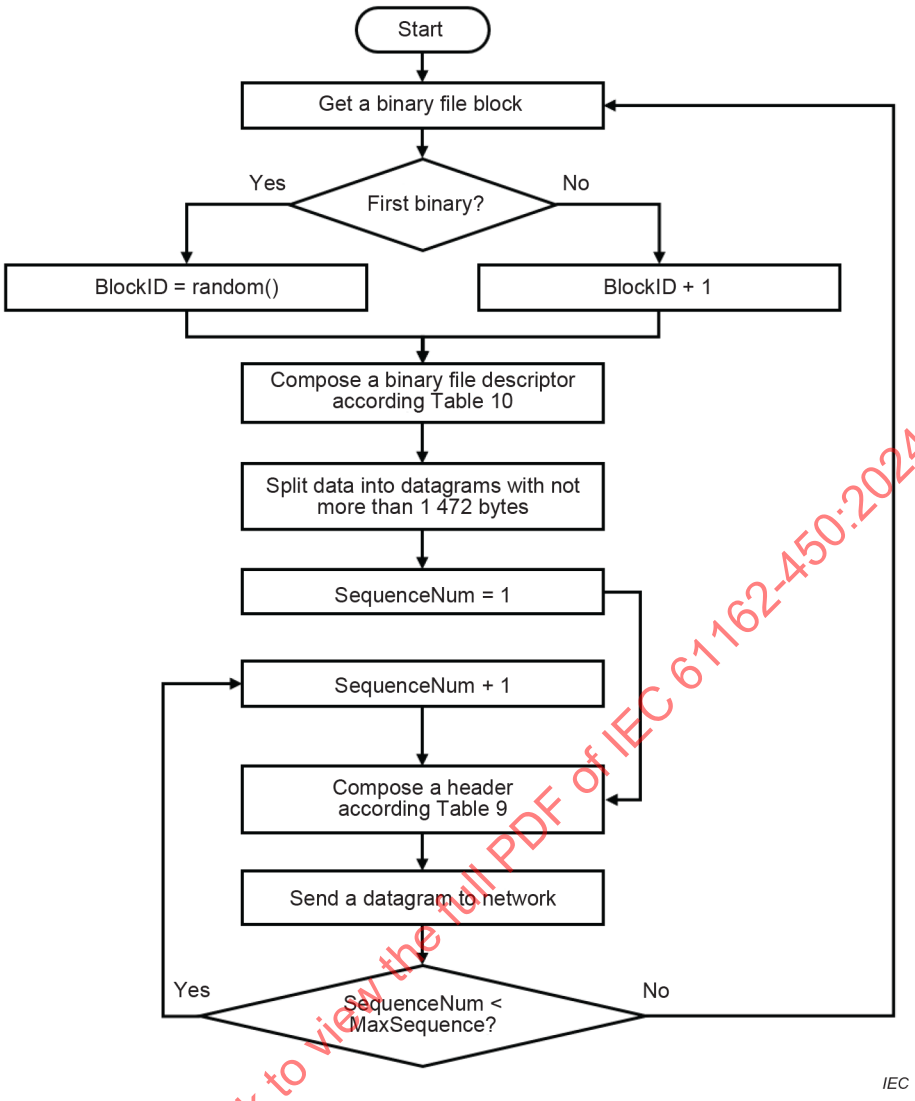


Figure 5 – Non re-transmittable sender process

7.3.6.2 Re-transmittable sender process

The sender processing steps for re-transmittable binary file transfer is as follows (see Figure 6):

a) a sender process waits until it gets a binary file block;

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

c) a binary file descriptor is composed according to Table 10;

d) set re-transmission counter to zero (0), set query counter to zero (0), set query sequence number to 1, set final counter to zero (0);

e) a binary file block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer. Let the maximum number of retransmissions to be as defined in 7.3.8.7; **46**

f) get the first datagram of the binary file;

g) assign a sequence number, which is set to one initially;

h) compose a header according Table 9;

i) send a datagram to the network and set an ACK timer to 500 ms; **47**

j) if the sender receives an ACK message, whose DestID is not equal to own SFI and whose SourceID is not equal to own actual DestID, go to step k);

   1) if the sequence number of ACK message is less than the maximum sequence number and lower than the sequence number of the last transmitted datagram, increase re-transmission count by one;

   2) if re-transmission count is greater than the maximum number of retransmissions (see 7.3.8.7), go to step k);

   3) if sequence number in ACK message is identical to query sequence number, increase query counter with 1, and if query counter is more than 3, set query counter to zero (0) and go to k);

   4) if sequence number in ACK message is not identical to query sequence number, set query counter to 1;

   5) get a datagram whose sequence number is sequence number in ACK message plus one;

   6) set query sequence number to sequence number;

   7) go to step h);

k) if all datagrams of the binary file block have not been transmitted,

   1) get a next datagram and increase sequence number by one,

   2) go to step h);

l) otherwise, wait for an ACK message;

m) if the sender receives an ACK message whose DestID is not equal to own SFI and whose SourceID is not equal to own actual DestID , then go to step (n);

   1) if the sequence number of the ACK message is less than the maximum sequence number, then go to step j);

   2) if the sequence number of the ACK message is equal to the maximum sequence number (i.e. transfer successful), then go to step a);

n) if ACK Timer expires and final counter is not more than three, then

   1) increase the final counter,

   2) compose a QUERY datagram and send it to the network,

   3) set an ACK timer to 500 ms, **47**

   4) go to step l);

o) transfer not successful; **48**

   1) clear the sending buffer,

   2) go to step a).

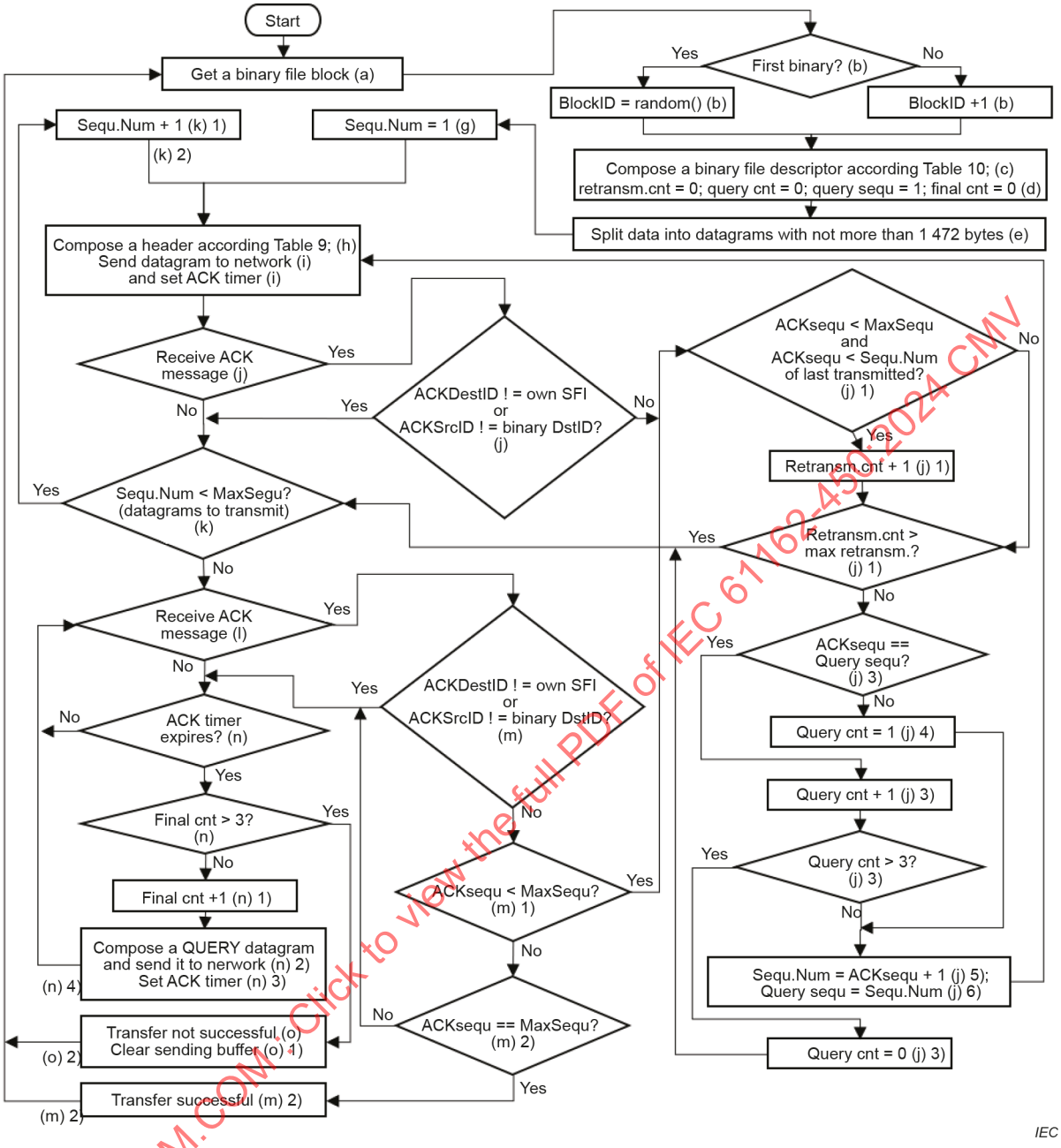


Figure 6 – Re-transmittable sender process

7.3.7 Receiver process for binary file transfer

7.3.7.1 Non re-transmittable receiver process

The receiver process steps of the non re-transmittable binary file transfer, including passive receivers of a re-transmittable binary file 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 the 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 SFI is same as the DestID in the Header as follows (see Figure 7):

a) waits for receiving a new datagram;

b) if the token is not "RrUdP" or if DestID of received datagram is not equal to own SFI or the received datagram is an ACK message **49**, go to step a);

c) if the received datagram is a QUERY message, then

1) if no previous datagram is available, go to step a),
2) if the sequence number of the previous datagram is not equal to maximum sequence number, go to step a),
3) if all sequences flag is false (not all sequences of the previous binary block are received), go to step a),
4) compose a Header with type = ACK, the BlockID and sequence number of the previous datagram,
5) send an acknowledge datagram to the sender,
6) go to step a);

d) if the sequence number is 1,

1) analyse file image descriptor and header,
2) if file image descriptor or header or token is invalid, go to step a),
3) set re-transmission counter and query counter to zero (0), set query sequence number to 1, set all sequences flag to true,
4) go to step g);

e) if no previous datagram is available, go to step g);

f) 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,

1) if there is any data in the receiver buffer, it is delivered to the SF,
2) the receiver buffer is cleared. Set re-transmission counter and query counter to zero (0). Set query sequence number to 1, set all sequences flag to true; **50**

g) if the sequence number is not 1 and not the same as the sequence number of the previous datagram plus one,

1) increase re-transmission count by one,
2) if re-transmission count is greater than the maximum number of retransmissions (see 7.3.8.7), set all sequences flag to false and go to step a),
3) if previous sequence number is identical to query sequence number increase query counter with 1, else go to step g) 6), **51**
4) if query counter is more than 3, set query counter to zero (0) else go to step g) 8), **51**
5) set all sequences flag to false and go to step a),
6) if previous sequence number is not identical to query sequence number, set query counter to 1,
7) set query sequence number to previous sequence number,
8) compose a Header with type = ACK, the block identifier and sequence number of the previous datagram,

9) send an acknowledge datagram to the sender,

10) go to step (a);

h) put a datagram into the receiver buffer;

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

1) all the data in the receive buffer is delivered to the SF,

2) the receiver buffer is cleared,

3) the re-transmission count is set to zero (0);

4) else go to step a); **51**

j) if all sequences flag are true,

1) compose a Header with type = ACK, the block identifier and maximum sequence number,

2) send an acknowledge datagram to the sender;

k) go to step a).

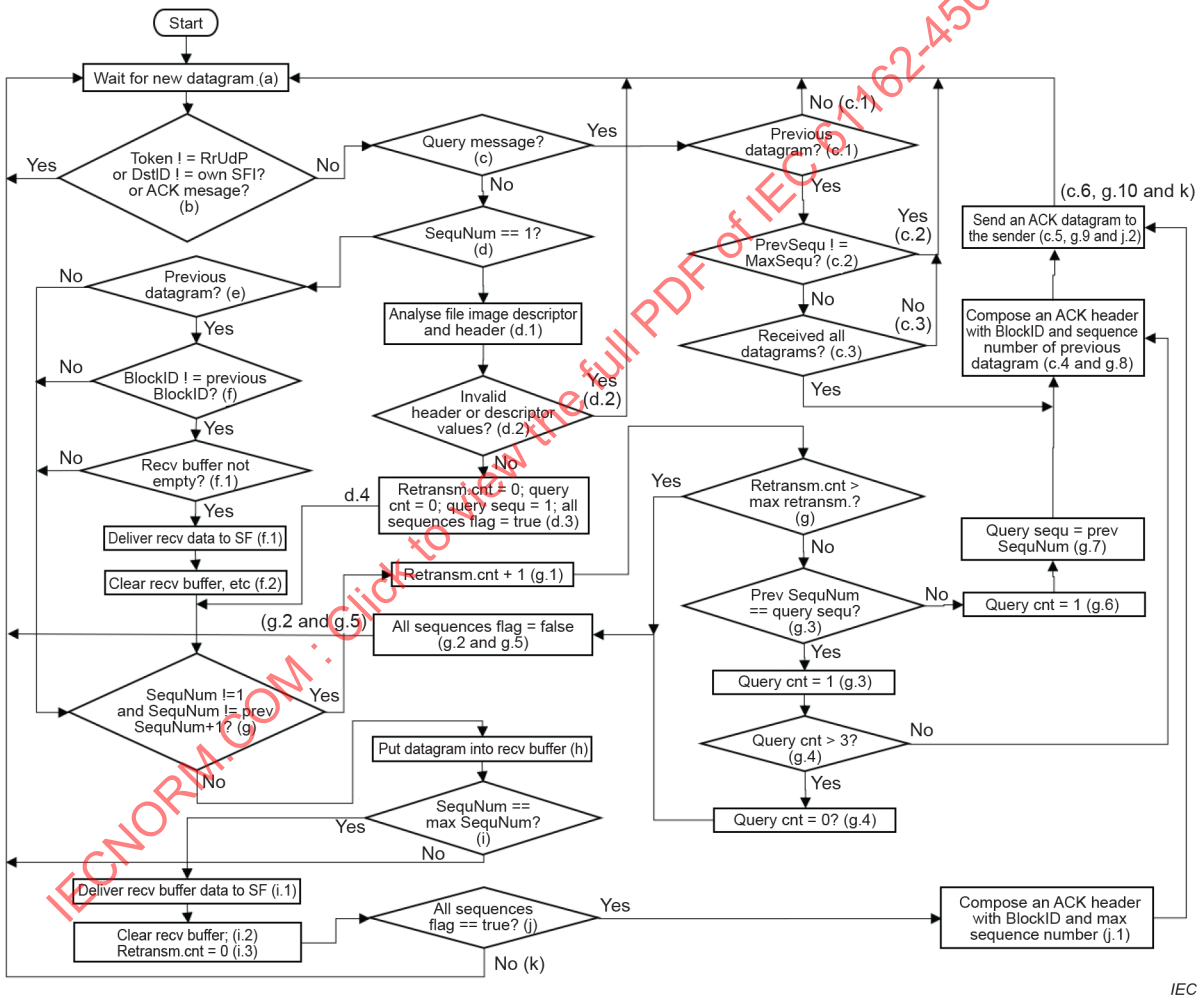


Figure 7 – Re-transmittable receive process

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 file blocks

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

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 file 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 file source shall not exceed 2 MBytes/s.

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

7.3.8.5 End of transmission for non re-transmittable and re-transmittable binary file transfer

The receiver shall assume that a transmission has ended unsuccessfully when it gets a binary file block from the 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 binary file block being received. The transmission shall also be considered finished when the last block is signalled by the SequenceNum from the sender. When a re-transmittable receiver identified by the DestID gets the last block after successful reception of all previous blocks, then it sends an ACK message to the sender to indicate successful transfer and so as to start new binary file block transmission. The receiver of non-re-transmittable binary file transfer and a receiver of re-transmittable binary file transfer not identified by DestID shall not send ACK message to the sender.

The re-transmittable sender assumes that the transmission is successfully finished only if it receives an ACK message with the SequenceNum which is equal to the MaxSequence; otherwise, a transmission has ended unsuccessfully. When a transmission is ended, a sender starts a new transmission if necessary.

7.3.8.6 Gaps between ACK messages for re-transmittable binary file transfer

In general, a receiver shall, immediately after loss detection, transmit an ACK message to the sender if a binary file block has been lost by having a gap in sequence numbers. 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 for ~~the following datagrams~~ another identical datagram **33**. 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 for re-transmittable binary file transfer

The sender shall not retransmit the same datagram identified by sequence number of a binary file more than three times (i.e. totally four transmissions) **52**. After three retransmissions, the sender shall ignore any additional retransmission requests for this datagram identified by sequence number and continue transmitting the next datagram identified by sequence number. The receiver shall not query the same datagram identified by sequence number of a binary file more than three times.

The maximum number of re-transmission requests for a binary file shall be limited to 10 % of the maximum sequence number for the binary file but shall be not lower than three times. If the sender of a binary file receives more re-transmission queries than the maximum number, it shall ignore all further retransmission queries and continue to transmit the binary file until the last datagram identified by sequence number. In the case the receiver did not successfully receive all datagrams identified by sequence numbers of binary file, the receiver shall not acknowledge the last received datagram identified by sequence number with sequence number equal to maximum sequence number. The receiver shall not query datagrams in the same binary file more than the maximum number of retransmissions.

In addition to data message re-transmission, control (Query) 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 for re-transmittable binary file transfer

The re-transmission timer is managed at the sender. A sender sets the re-transmission timer when either a whole binary file 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 for non re-transmittable and re-transmittable binary file transfer

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

The receiver shall reply with ACK to the sender using the incoming datagram's AckDestPort and multicast address corresponding to this port number.

7.3.9 Error logging

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

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

7.4 General IEC 61162-3 PGN message transmissions

(see 8.12)

7.4.1 Message structure

The message structure for transporting IEC 61162-3 PGN messages into IEC 61162-450 networks is illustrated in Table 13.

Table 13 – Structure for PGN message

Header (see Table 9)
PGN message descriptor
IEC 61162-3 message fragment
IEC 61162-3 message fragment (zero or more)

The maximum message size of the PGN is 1 785 bytes. The PGN message shall be transmitted using one or two IEC 61162-450 datagrams. When there is a missing datagram, then the PGN message will be ignored as an error since the re-transmission of the lost datagram is not required.

7.4.2 Message format

The message format for transporting IEC 61162-3 PGN messages into IEC 61162-450 networks is illustrated in Table 14. The PGN message descriptor length for PGN messages is 32 bytes.

Table 14 – PGN message descriptor

Field Name	Size	Description
Source NAME (SNAME)	8 bytes of characters	Name of source. NAME shall be compliant with IEC 61162-3.
Source Device Identifier (SDID) [a]	2 byte of numeric number	Address of source device which is compliant with IEC 61162-3.
Destination NAME (DNAME)	8 bytes of characters	Name of destination. NAME shall be compliant with IEC 61162-3.
Destination Device Identifier (DDID) [a]	2 byte of numeric number	Address of destination device which is compliant with IEC 61162-3.
PGN number	4 byte of numeric number	PGN number of IEC 61162-3.
Priority	1 byte of numeric number	Priority of IEC 61162-3. Bit 0-2 are used and Bit 3 to Bit 7 are reserved.
Reserved (REVD)	7 bytes	Reserved bytes.
[a] Two bytes are specified to allow for future expansion.		

7.4.3 Address translation requirements

7.4.3.1 PGN group identification

A PGN group is defined as a logical group of devices that can share the information and message. Each PNGF shall be assigned a PGN group to communicate with devices in the group. The device address in a PGN group shall be unique in the network.

A PNGF may be registered with more than one PGN group if some of devices are required to communicate with devices in different PGN groups.

Means shall be provided to configure PGN groups at each PNGF.

7.4.3.2 Device identification

The PNGF shall represent all IEC 61162-3 equipment which are uniquely identified in the network.

A virtual device in an IEC 61162-3 network is identified by the source address. Each virtual device shall be identified by SFI of PNGF where it is connected, its PGN group number, its IEC 61162-3 source address and NAME. When there is no address available, then the address cannot be mapped until a new address is available. When a new address is not available, this event shall be recorded as specified in 4.3.3.

7.4.3.3 Address resolution

When a PNGF receives a query (i.e. Address Claim Message) about the device address with NAME and it has the information about the device, it shall respond with the address without forwarding the message to the IEC 61162-3 network.

7.4.4 Message processing

7.4.4.1 From IEC 61162-3 to IEC 61162-450

The PNGF shall have the capability of representing IEC 61162-3 devices as gateway device address and PNGF's SFI except for device address 0 which is always mapped to the device address 256. This is because the PNGF's device address of 0 represents PNGF itself on the IEC 61162-450.

The PNGF shall have the capability to represent it as at least an IEC 61162-3 device by obtaining its corresponding IEC 61162-3 source address from the IEC 61162-3 network.

When a PGN message is received from the IEC 61162-3, the PNGF extracts the information of source address, destination address, priority and PGN and it creates a message and fills up the corresponding fields. It also looks up the field of SFI and NAME of the destination address, and fills it out. When the received PGN message is not valid, then it will be discarded, and this event shall be recorded as specified in 4.3.3.

7.4.4.2 From IEC 61162-450 to IEC 61162-3

The PNGF shall have the capability to map 251 IEC 61162-3 source addresses to IEC 61162-450 device address and vice versa. The value of 251 is based on IEC 61162-3 address where the PNGF consumes 1 for the PNGF itself leaving 251 for mapping.

The address at IEC 61162-3 is source and destination device address. When a PNGF receives a message from an IEC 61162-450 network, it extracts the SDID and DDID information and puts it in the IEC 61162-3 PGN message and transmits into the IEC 61162-3 network. When the received PGN message is not valid, then it will be discarded, and this event shall be recorded as specified in 4.3.3.

7.4.4.3 Address conflicts

When there is a PNGF assigned address conflict in the address translation table of PNGF for mapping IEC 61162-3 network devices available as ~~450~~ nodes in the ~~450~~ network (i.e. when the same device address is assigned to more than one device), it shall be resolved. When a PNGF finds out that there are address conflicts, it re-assigns IEC 61162-3 device address mapping.

The address re-assignment process shall be done within 1 min.

7.4.5 Additional management requirements

7.4.5.1 Field configurable capability

The PNGF may also have the field configurable capability to change this default address so that the address is not claimed for a particular IEC 61162-3 device.

7.4.5.2 Non-volatile memory

The PNGF shall maintain configuration data in non-volatile memory. This ensures that field configurable settings are maintained across power cycles.

7.5 System function ID resolution

(see 8.13)

7.5.1 General

At the construction of a ~~450~~ network of a ship, the assignment of SFI (system function ID) may be clearly defined. However, as the equipment of the ship is amended, replaced, repaired and serviced, the assignment of SFIs may not be as clear. This protocol assists in the detection of SFI collisions.

NOTE The receiver functions are covered in IEC 61162-460.

7.5.2 Transmitter functions

These functions apply to ~~all 450 Nodes~~ nodes which implement SF. **53**

For each SF, including every instance identified by a combination of SFI and instance number **53**, a transmitter in a ~~450~~ network shall, as a minimum after boot up, 1 min after boot up, 5 min after boot up and after reconfiguration which changes any fields in an SRP sentence, send on address 239.192.0.56 port 60056 an SRP sentence to assist detection of collision of the SFI (see Annex F and Annex G). On receiving an SRP sentence with all fields being null fields **33**, equipment shall respond with an SRP sentence with the fields populated.

Multiple sending of SRP is needed as different devices can have faster boot up time than the network monitoring performing the collision detection based on SRP sentences.

A node may periodically send an SRP sentence populated with at least its own MAC address and IP address at a suitable period determined by the manufacturer.

NOTE The usage of the SRP sentence for SFI collision monitoring is specified in IEC 61162-460 – SFI collision monitoring. **54**

7.6 Binary file transfer using TCP point-to-point

(see 8.14)

7.6.1 Definition

This protocol provides a mechanism by which non IEC 61162-1 formatted data can be transmitted from a sender to a single receiver. The protocol emphasizes the reliability of the data transmission between two linked systems by using the TCP protocol.

NOTE The TCP standard is RFC 793. The IP standard is RFC 894. The Ethernet standard is IEEE Std 802.3.

Table 15 describes the terminology used.

Table 15 – Description of terms

Term	Description
BYTE	The lowest level data element consisting of 8 ordered bits (sometimes called an octet). Bit order is as determined by the computer implementation. ~~Note that~~ The implementation shall make any necessary conversion between network bit order and computer bit order.
Data packet	A number of bytes that contains a header, an optional sequence of reserved bytes and the actual message content. The header specifies the length of header itself, of reserved bytes and data and will also contain information that allows a number of data packets to be re-assembled into a presentation.
Data element	One or more bytes that forms a stand-alone information carrier, i.e. a time stamp, an integer or a character.
DWORD	Double word. One unsigned 32-bit integer (in range 0 to 4294967295). The DWORD is constructed from four consecutively transmitted BYTES, where the transmission order on the network is the most significant BYTE first followed by the next most significant BYTE until the least significant BYTE.
File	One group of bytes that forms a stand-alone data set.
Message data	The data contents of a data package.
Reserved bytes	A number of bytes in the data packet 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 the range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTES, 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 BYTES, interpreted as a string of characters. The transmission order on the network is the left-most character first. If the string is shorter than n, additional trailing bytes shall be set to zero. All strings in the header are encoded in ISO/IEC 18859-1 (ISO Latin 1).

7.6.2 Data field structure for transfer of files

7.6.2.1 General

The files are transmitted over the network in packets. The data field is defined as a sequential and unpadded stream of octets divided into two main groups – header and package data, as shown in Table 16. The header is needed for synchronisation and data integrity validation.

Table 16 – Binary file structure

Header (see 7.6.2.2)
Package data (see 7.6.2.3)

7.6.2.2 Elements of the header structure

The header format is defined in the Table 17. The first column specifies the name of the data item inside the header (starting from offset zero). The second column specifies the data type and size. The third column describes the data item and its purpose.

Table 17 – Header structure

Data item	Type	Description
token	STRING[6]	It shall always contain the string "RrTcP" including a trailing NULL character. Identifier as ASCII string with a length of 5 bytes. This token defines the beginning of a new data block.
crcHeader	WORD	Cyclic redundancy check for the header according to CRC-16/CCITT-FALSE. The CRC is calculated from and including headerversion to and including any reserved bytes. The CRC is calculated from the sequence of bytes after formatting into transmission byte order. The CRC polynomial is: $x^{16} + x^{12} + x^5 + 1$.
headerversion	WORD	Defines the header version. The headerversion with value 1 is defined in this document. Extensions and/or modified versions will update this value.
headerlength	DWORD	Defines the binary file descriptor length in bytes. This is at least the length of the header including the reserved bytes. Future editions of IEC 61162-450 may append additional fields to this file descriptor without incrementing the header version as long as these additional fields are compatible with the definition of the file descriptor in this document. Receivers which are not aware of these additional fields shall ignore them.
srcID	STRING[6]	Define the source system identifier in format "ccxxxx" (see 4.4.2).
datalength	DWORD	Defines the data content of this data package in octets. This may be the full (oversized) data in one package or a typical size for network transfer (1 280 octets). In the latter case, maxnum, actnum and streamlength will be used to synchronize data packets into a complete data transfer.
timeSec	DWORD	Seconds part of time stamp. Timestamp is constructed both of time in seconds and nanoseconds at the grabbing instant. If required by the application (e.g. image transmission to the VDR), the timestamp shall be made at the source immediately at data recording. If the application allows the timestamp to be optional and no timestamp is available, the value 0 shall be used for timeSec and timeNsec. The time representation is the number of seconds since January 1st 1970, not including leap seconds (i.e. in astronomic/GMT representation). This information is only needed with the first packet of each file or data stream. Time stamps in the following data packages belonging to the same data transfer shall be discarded by the receiver. It is only practicable to use this value if the synchronization between the destination device (e.g. VDR) and the source device (e.g. Radar unit) is sufficiently precise (in the range of milliseconds). The difftime data item may be used as an alternative method for synchronisation. If difftime is non-zero, this field shall be ignored.
timeNsec	DWORD	Nanosecond part of time stamp. See timeSec for details.
difftime	WORD	Time difference in milliseconds between data recording instant (e.g. grabbing instant) and transmission of the first packet of the file. A timestamp with a resolution of at least in the millisecond range is made immediately before the source generation (e.g. screenshot) and the second timestamp is made immediately before the first packet is transmitted. The difference is entered as "difftime" and the packet is then sent. The destination device (e.g. VDR) uses this difftime value together with its system time to determine the timestamp for the transmitted data. Time tolerances between destination device and source device may be neglected, because the time reference of the destination device is always the system time of the destination device.
maxnum	DWORD	Number of packets needed for transmission of the corresponding file or data stream. The value can be 1 or more.
actnum	DWORD	This packet number (range from 1 to maxnum).
streamlength	DWORD	Defines the length of the (full) stream/presentation content in octets

Data item	Type	Description
device	BYTE	Data source (device) as binary value, 1~~→~~ for equipment 1, 2~~→~~ for 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.
deviceip	DWORD	IP of transmitting device; optionally used. The IP address is entered in Network Byte Order Format (DWORD).
deviceport	WORD	That port the transmitting device has used. It may be used optionally.
typelength	BYTE	The length of the datatype field.
datatype	STRING[~~16~~n]	This string defines the datablock encoding by assigning a MIME content type to the datablock for the server followed by a null character. For example, image/png is used for PNG image files and application/zip is used for zip-files. This document has the datatype specified as STRING[n]. Previous editions had STRING[16]. Transmitters shall have a setup parameter to use the length as "n" or "16" to maintain compatibility with previous editions of IEC 61162-450. In the compatibility instance, receivers may receive padding at the end of datatype string. **55**
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.
StatusLength	WORD	The length of the "Status and information text" field in bytes.
Status and information text	STRING[n]	Status information (e.g. successful operation or error codes). This may be one or more strings terminated by a binary null.

7.6.2.3 Elements of the package data structure

The package data format is defined in Table 18. The first column specifies the name of the data item. The second column specifies the data type and size. The third column describes the data item and its purpose.

The package data structure size is set to zero if only status information is transmitted.

Table 18 – Package data structure

Data item	Type	Description
datablock	BYTE[datalength]	This item is the data either split into pieces or in one block. Size is defined by datalength in the header.

There is no CRC for the data contents as this is partly handled by the TCP/IP layer or by other mechanisms in the contents format. The header has a separate CRC as it is deemed more critical for the correct operation of the system.

7.6.3 Structure of the transfer stream

7.6.3.1 General

The complete binary file is split into a number of datablocks. Each header and datablock is transmitted in increasing order, beginning with the first datablock and ending with the last datablock. Synchronisation is achieved with data items actnum and maxnum.

7.6.3.2 Unknown data types

A receiver that does not understand an incoming data type shall ignore all incoming data without closing the connection if the receiver is a server.

If the receiver is a client and does not understand incoming data, it shall immediately close the connection.

7.6.3.3 Maximum outgoing rate

The data volume for each transmit client of binary file shall not exceed 2 MBytes/s.

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

7.6.4 TCP port and IP addresses

The IP address shall be freely selectable outside the addresses assigned for other purposes in this document and the IP address is depending on the network configuration of the corresponding equipment manufacturer.

The IP address of each file source and the file receiver has to be coordinated and set manually beforehand to be in the same IP address range.

Equipment unable to perform an address look-up service should be configured to the same IP sub-net. A router may be used if the equipment is connected on different IP sub-nets.

The default TCP port between sender and receiver for the transfer shall be 7097. Sender and receiver shall support configuration of the port number and IP address.

7.6.5 Implementation guidance

7.6.5.1 General

In the examples in 7.6.5.2, 7.6.5.3 and 7.6.5.4, it is assumed that the TCP client is the sender and the TCP server is the receiver. In general, both TCP server and TCP client may send or receive data. **33**

7.6.5.2 Receiver as server and sender as client

This setup is used for example for VDRs where the VDR as the file receiver has to be configured as a passive listening device. The file sender is the active transmit client connecting and transferring the data.

Depending on the application, the file receiver may be set up to accept multiple transmit clients on the same input port. This is necessary if more than one transmit client is assumed to send its files to the receiver server.

7.6.5.3 Connection management from sender client

The transmit client shall establish a connection to the receiver server immediately after system initialisation. Once the connection is established, the transmit client is responsible for the connection and streaming of data packet to the receiver server.

If the connection attempt fails or connection is lost, the transmit client shall try to establish the connection again. The interval between attempts shall not exceed 30 s.

7.6.5.4 Connection management from receiver server

The receiver server shall make the listening port available for data transfers during initialisation.

The manufacturer shall specify the maximum number of transmit client connections for the receiver server. The receiver server shall receive data individually from connected transmit clients and detect any loss of connection from transmit clients.

The equipment test and performance standard may require alerts to be raised for loss of connection.

The receiver server may in some cases only detect a failed connection by timeout since data was received last time. The receiver server shall reinitialise the listening port and the receiver software module after timeout for the transmit client.

7.6.5.5 Error handling

The receiver shall ensure data integrity at reception by verification of the header including token, version, consistency of data fields and the header CRC. Erroneous data reception shall be processed and indicated according to individual equipment standard.

NOTE Consistency of data fields can depend on application. However, strings can be checked against containing illegal characters, message sequence numbers can be checked, etc.

7.6.5.6 Transmission of a file

The client transmission of a file may occur at any time when the connection is open. The message header information is sufficient for the server to decode the data stream and reassemble the file and its associated header information data.

7.6.5.7 Device identification

All clients shall be configured with a unique source SFI and device identification (1 to 255) to allow the server to unambiguously identify the source of the received packets.

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 EUT. 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 to be 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;
- if the EUT implements support for PGN, generation of IEC 61162-3 PGN test sentences containing unique and numbered content, syntactically correct and incorrect with variable length and correct, incorrect and missing checksum;
- 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 and reception of non re-transmittable and re-transmittable binary files.

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 EUT has 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)

Confirm by inspection of manufacturer provided information that the EUT does not provide the functions of a repeater hub.

Confirm by inspection of documented evidence that the EUT supports IGMP protocol and that the version of IGMP support is documented.

If the EUT is a switch,

- confirm by inspection of documented evidence that it supports IGMP snooping, and
- confirm by inspection of documented evidence that the IGMP snooping based multicast traffic filtering is supported per each multicast address.

Use a simulation arrangement to generate multicast datagrams with address range of 224.0.0.1 to 224.0.0.255 and confirm by observation that the EUT does not filter out those datagrams.

8.2.3 Documentation

(see 4.4.1, 7.1.1)

Confirm by inspection of manufacture's documentation that all of the implemented datagram types are specified.

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 4.3.2, a) to c).

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 that 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, the output of syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

If reception of syslog message capability is provided, confirm by analytic evaluation that the reception and logging of syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

8.4 System function block (SF)

8.4.1 General

(see 4.4.1)

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

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

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.

Check that manufacturer's documentation include instructions how to select "cc" and "xxxx" part of the SFI so that the SFI is unique at least within the IEC 61162-450 network.

8.4.3 Implementing configurable transmission groups

(see 4.4.2)

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 sources distinguished by different talker mnemonic per each serial port of the device and that the mapping of SFI to sources distinguished by different talker mnemonic per each serial port is correctly implemented by analysing the UDP datagrams.

Check that TAG block source identification “s” is correctly implemented to sources distinguished by different talker mnemonic per each serial port by analysing the UDP datagrams.

Check that TAG block destination identification "d" is correctly implemented for routing from ~~450~~ network to serial ports.

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

- prioritized sentences are correctly replaced, maintaining the FIFO order and not affecting sentence integrity, and
- in case buffer overflow sentences are discarded, the FIFO order is maintained, not affecting sentence integrity, and 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, SFI, source identification "s" and, if required, destination identification "d".

The test sentences should include TAG blocks and grouped messages.

Test configuration should include single source per serial port and multiple sources distinguished by different talker mnemonics per shared serial port.

8.5.4 ~~Datagram output~~ Multi SF serial port

(see 4.5.4)

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, SFI, source identification "s" and, if required, destination identification "d".

Test configuration should be configured for multiple sources distinguished by different talker identifiers and manufacturer mnemonic codes (for proprietary sentences) per shared serial input port. The output should be configured for single destination by talker identifier.

Check the test cases below:

1) received sentences with configured talker identifiers and manufacturer mnemonic codes will transmit datagrams with the configured SFI;
2) received sentences without a configured talker identifier or manufacturer mnemonic code will transmit datagrams for each configured SFI;
3) received datagrams with configured destination SFIs will be transmitted on configured serial port;
4) received datagrams with a valid destination that is an unknown SFI will not be transmitted on any serial port;
5) received datagrams with no destination specified will be transmitted to all serial ports.

In the test cases below, the SNGF ~~serial port default~~ SFI is "SI0001" **56**, the configured SFIs of serial ports **33** are TI0001 (for Talker Identifier "TI") and VD0001 (for Talker Identifier "VD"). A proprietary sentence "PMANMSG" is configured for SFI VD0001. The typical received sentences will then include rate-of-turn ("$TIROT") and speed ("$VDVBW").

- Test case 1: An example of simple SFI conversion:

  "$TIROT,123.45*67<CR><LF>$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  "$PMANMSG,proprietary_contents*hh<CR><LF>"

  will generate three datagrams, one for each SFI:

  "\s:TI0001,n:333*hh\$TIROT,123.45*67<CR><LF>"

  "\s:VD0001,n:111*hh\$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  "\s:VD0001,n:111*hh\>$PMANMSG,proprietary_contents*hh<CR><LF>"

  with the IEC 61162-450 Header("UdPbC'0'").

- Test case 2: An example of un-configured talker identifier:

  "$SDDPT,123.4,,400*hh<CR><LF>"

  will generate one datagram for each configured SFI:

  "\s:TI0001,n:222*hh\$SDDPT,123.4,,400*hh<CR><LF>"

  "\s:VD0001,n:222*hh\$SDDPT,123.4,,400*hh<CR><LF>"

  with the IEC 61162-450 Header("UdPbC'0'").

- Test case 3: An example of simple SFI conversion, no TAG block support:

  Datagram "\s:IN0001,d:TI0001,n:333*hh\$INTIQ,ROT*hh<CR><LF>"

  will generate transmission of the sentence on the serial port configured for the destination SFI TI0001:

  "$INTIQ,ROT*hh<CR><LF>"

- Test case 4: An example of a specified destination but un-configured SFI conversion:

  Datagram "\s:IN0001,d:GN0001,n:333*hh\$INGNQ,ZDA*hh<CR><LF>"

  will not generate transmission on any serial ports.

- Test case 5: An example of no specified destination:

  Datagram "\s:IN0001,n:333*hh\$INGNQ,ZDA*hh<CR><LF>"

  will generate transmission of the sentence on all serial ports.

  "$INGNQ,ZDA*hh<CR><LF>"

8.5.5 Handling malformed data received on serial line

(see 4.5.5)

Verify datagram conversion by feeding the SNGF input ports under test with valid sentences interleaved with malformed data according to 4.5.5.

Confirm that the valid sentences are correctly converted into datagrams.

Each test shall include test cases for all of the start characters. Check that the test cases below will generate a datagram transmission:

1) when data has been received before a start character;
2) when data has been received after a valid start character and the maximum sentence and TAG block length has been exceeded;
3) when data has been received after a valid start character and end of line (<CR><LF>) has not been received within 1 s;
4) when a reserved character has been received and not having been appropriately escaped;

5) when random binary data is sent on serial line.

In the test cases below, ~~the SNGF serial port is configured as SFI TI0001 and default SI0001 is the SFI of the SNGF~~ the SNGF SFI is SI0001, the configured SFI of serial port is TI0001 (for Talker Identifier "TI"). **57**

- Test case 1: An example of data before start character:

  `Serial data "127,333*6B<CR><LF>$TIROT,123.45*67<CR><LF>"`

  will generate two datagrams:

  either

  `"\s:SI0001,n:444*hh\127,333*6B<CR><LF>"` (if SFI for malformed sentences set by configuration to be SI0001)

  or `"\s:TI0001,n:444*hh\127,333*hh<CR><LF>"` (if SFI for malformed sentences set to follow non-malformed sentences)

  and **58**

  `"\s:TI0001,n:445*hh\$TIROT,123.45*hh<CR><LF>"`

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 2: An example of too long line:

  `Serial data "$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>"`

  will generate one datagram, i.e. no change to content:

  either

  `"\s:TI0001,n:446*hh\$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>"` (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)

  or

  `"\s:U20001,n:446*hh\$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>"` (if SFI for malformed sentences set by configuration to be U20001) **58**

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 3: An example of timeout:

  `Serial data "$TIALR,123456,906,A,V,"`

  <1.1 s delay>

  `Serial data "Sensor fault*hh<CR><LF>"`

  will generate two datagrams:

  either

  `"\s:TI0001,n:447*nn\$TIALR,123456,906,A,V,"` (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)

  or

  `"\s:SI0001,n:447*nn\$TIALR,123456,906,A,V,"` (if SFI set by configuration to be SI0001) **58**

  and either

  `"\s:SI0001,n:448*nn\Sensor fault*hh<CR><LF>"` (if SFI for malformed sentences set by configuration to be SI0001)

  or

  `"\s:TI0001,n:448*nn\Sensor fault*hh<CR><LF>"` (if SFI for malformed sentences set to follow non-malformed sentences) **58**

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 4: An example of incorrect escape:

  "$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>"

  will generate a datagram (i.e. no change to content):

  either

  "\s:TI0001,n:449*nn\$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>" (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)

  or

  "\s:SI0001,n:449*nn\$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be SI0001) 58

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 5: An example of random serial data including start characters "$" that will initiate a new ~~buffer~~ datagram:

  ~~This will generate a datagram:~~

  ~~"\s:SI0001,n:449*nn\kfajds...3efbnajfu93hn" followed by~~

  ~~"\s:SI0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.."~~

  "kfajds…3efbnajfu93hn$lkfdajkf98873tq87784((/kfajd.."

  The above random data will generate two datagrams:

  either

  "\s:SI0001,n:449*nn\kfajds...3efbnajfu93hn" (if SFI for malformed sentences set by configuration to be SI0001)

  or

  "\s:TI0001,n:449*nn\kfajds...3efbnajfu93hn" (if SFI for malformed sentences set to follow non-malformed sentences)

  followed by either

  "\s:SI0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." (if SFI for malformed sentences set by configuration to be SI0001)

  or

  "\s:TI0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." (if SFI for malformed sentences set to follow non-malformed sentences)

  or

  "\s:lk0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." if SFI for malformed sentences set based on talker mnemonic)

  and with the IEC 61162-450 Header ("UdPbC'0'").

In the test cases below for Multi SF serial port, the SNGF SFI is SI0001, the configured SFIs of the serial port are TI0001 (for Talker Identifier "TI") and VD0001 (for Talker Identifier "VD"). 59

- Test case 6: An example of data before start character:

  Serial data

  $VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>127,333*6B<CR><LF>$TIROT,123.45*67<CR><LF>

  will generate three datagrams:

  "\s:VD0001,n:443*hh\$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  and either

  "\s:VD0001,n:444*hh\127,333*hh<CR><LF>" (if SFI for malformed sentences set to follow non-malformed sentences, and there were no preceding STN sentence)

  or

  "\s:U20001,n:444*hh\127,333*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be U20001)

and

"\s:TI0001,n:445*hh\$TIROT,123.45*hh<CR><LF>"

and with the IEC 61162-450 Header ("UdPbC'0'"). **60**

8.6 Other network function (ONF)

(see 4.7)

Verify by inspection of the manufacturer's documentation that information for the use of ONF is provided as described in 4.7.

Verify ~~using the test equipment described in 8.1~~ by inspection of the manufacturer's documentation that the ONF does not use any of the multicast IP addresses reserved in 5.4.

~~NOTE The test equipment to confirm the source and destination of general ONF traffic could be a network analyser.~~ **61**

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~~ the EUT does not send packets with IP options set; except for IGMP packets, where IP options are used for the correct functioning of IGMP protocol. **33**

Confirm by generating an example of each relevant (see 5.2) packet and analysing this packet using ~~ping program~~ packet capture software to confirm that ~~each device~~ the EUT supports the network protocols specified. **62**

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 within the ranges reserved for private networks as described in ISOC RFC 1918.

Confirm that any excluded IP ranges reserved for internal sub-nets (internal to the equipment) are documented and those are not in the range given by 5.3.

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~~ datagrams are transmitted and received at each of the appropriate port numbers as defined in Table 4 and Table 5.

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

Verify that each transmitted UDP datagram contains no more than 1 472 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 files,
- "`RrUdP`" for transmission of re-transmittable binary files, and
- "`NkPgN`" for transmission of IEC 61162-3 PGN messages,

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

Check that all TCP/IP datagrams are headed by "`RrTcP`" for transmission of binary files as described in 7.6 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, as part of error logging, the count of received datagrams without valid datagram header (see 7.1) is increased if datagram header is unrecognized or invalid.

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 analyser that

- if provided, **63** all members of group have same group code value,
- if provided, **63** next group code value after 99 is 1,
- the EUT transmits the source identifier (two separate test cases – default and configured),
- if provided, the EUT transmits valid source cluster identification, **64**
- if ~~used~~ provided, the EUT transmits valid destination code,
- if provided, the EUT transmits valid destination cluster identification, **64**
- if provided, **63** line count value increments for each line and resets after 999 to 1,
- if provided, the heartbeat sentence (HBT) is transmitted at least once every 60 s, and
- the EUT 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 analyser, 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\""~~"\b:Y23G81*4E\" **65**) not defined in this document is transparent to normal operation,
- only complete sentence groups are used, and
- TAG block lines with the EUT as destination are processed. Destination is a combination of parameter codes destination code "d" and, if available, destination cluster identification "x".

  NOTE 1 Not available destination cluster identification can mean navigation cluster as destination. **66**

  NOTE 2 Processing can also mean that data is dropped.

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.

8.9.5 General authentication

(see 7.2.3.8)

These tests apply to a EUT that includes transmission of authentication.

Confirm by inspection of manufacturer's documentation which signature methods the EUT provides.

Confirm by analytic evaluation that the EUT transmits sentence or message with correct authentication code as described in 7.2.3.8. Repeat the test for all signature methods supported by the EUT.

Use simulation arrangement to create valid examples of authenticated sentences or messages and confirm by observation that, if the EUT is not set to require authentication, the EUT processes all sentences or messages.

Use simulation arrangement to create same valid examples of authenticated sentences or messages as in previous test, and confirm by observation that, if the EUT is set to require authentication, the EUT processes all sentences or messages. Repeat the test for all signature methods supported by the EUT.

Use simulation arrangement to create same valid examples of sentences or messages as in previous test, but without including authentication parameter code, and confirm by observation that, if the EUT is set to require authentication, the EUT discards all sentences or messages.

Use simulation arrangement to create same valid examples of sentences or messages as in previous test, but with intentionally incorrect value in the authentication parameter code, and confirm by observation that, if the EUT is set to require authentication, the EUT discards all sentences or messages. Repeat the test for all signature methods supported by EUT.

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, and
- 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, and
- incorrect message length.

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

8.11 Binary file transfer using UDP multicast – Single transmitter, multiple receiver

(see 7.3)

8.11.1 Sender process test

8.11.1.1 Non re-transmittable binary file transfer

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

- header token is set correctly,
- header version is set according the Table 9,
- SrcID is set according to Table 9,
- DestID is correctly set according to Table 9,
- 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 file transfer,
- the SequenceNum of first datagram is set to 1, and
- there is no response when a receiver sends any ACK messages.

8.11.1.2 Re-transmittable binary file transfer

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

- header token is set correctly,
- header version is according to Table 9,
- SrcID and DestID are 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, port number and AckDestPort are assigned by one of the addresses for binary file transfer,
- the maximal re-transmission count is calculated correctly according 7.3.8.7,
- the SequenceNum of the first datagram is set to 1,
- ACK messages are received from multicast group, specified from AckDestPort,
- ACK messages are only processed if the DestID of ACK message is equal to own SFI and if the SourceID of ACK message is equal to actual DestID, otherwise the ACK message is ignored,
- the binary transfer is finished and marked as successful after an ACK message is received, whose SequenceNum is equal to the MaxSequence, after all data is transmitted,
- a QUERY message is sent when there is no ACK message received, after all data are transmitted,
- not more than ~~three~~ four QUERY messages at all are sent when there is no ACK message received after a QUERY message is transmitted,
- binary file data from SequenceNum one higher as SequenceNum of ACK is re-transmitted when an ACK message whose SequenceNum is less than the MaxSequence is received,

- the same SequenceNum is retransmitted not more than three times, otherwise the re-transmittable sender continues with normal transfer and ignores ACK message,
- the number of all re-transmissions is not more than the maximal re-transmission count, otherwise the re-transmittable sender continues with normal transfer and ignores ACK messages,
- the binary transfer is finished and marked as not successful after all data is transmitted, if three QUERY messages are sent and no ACK message whose SequenceNum is equal to the MaxSequence is received, and
- log messages are correct.

8.11.2 Receiver process test

8.11.2.1 Non re-transmittable binary file transfer

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

- messages are received correctly on given IP and port address,
- message is only processed if the header token is equal to "RaUdP" or "RrUdP",
- message is only processed with valid header and valid binary ~~image~~ file descriptor,
- each separate binary file 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, and
- log messages are correct.

8.11.2.2 Re-transmittable binary file transfer

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

- messages are received correctly on given IP and port address,
- message is only processed if the header token is equal to "RrUdP",
- message is only processed with valid header and valid binary ~~image~~ file descriptor,
- message is only processed if DestID is equal to own SFI,
- each separate binary file transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- the maximal re-transmission count is calculated correctly according 7.3.8.7,
- ACK messages are generated with the correct token = RrUdP, SrcID = own SFI, DestID = SrcID of received message, BlockID and without binary ~~image~~ file descriptor and without data block,
- ACK messages are transmitted to the multicast group corresponding to the AckDestPort of the actual received binary file block,
- the receive process is marked as successful and an ACK message is transmitted when the received SequenceNum is equal to the MaxSequence with the same instance identifier and if all sequences of the actual binary file block are received,
- an ACK message for a successful received binary file block is not more than three times repeated if query messages are received,
- if no complete binary file block is received, the transfer is marked as not successful and no ACK message after the last received sequence with SequenceNum equal to MaxSequence is transmitted, either directly after received last sequence or after received query messages,

- an ACK message is transmitted with the last received SequenceNum before a gap when the re-transmittable receiver detects that there is a gap in the SequenceNum between two consecutive messages,
- an ACK message for the same requested SequenceNum is not more than three times repeated for the same binary file block,
- the number of all ACK messages for retransmission request is not more than the maximal re-transmission count for the same binary file block,
- 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 re-transmittable receiver does not send any ACK message when a re-transmittable sender sends a binary file block with different DestID, and
- log messages are correct.

8.11.3 Binary file descriptor test

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

- the AckDestPort field is correctly set,
- the Length field, the TypeLength field and the StatusLength field are correctly set,
- binary file length in the descriptor is the same as the size of the received data, and
- the received data format is the same as that of the data type in the descriptor.

8.11.4 Binary file transfer error logging

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

- number of binary file blocks where errors occur;
- missing datagrams;
- unrecognized headers (see 8.9.2).

8.11.5 Maximum outgoing rate

Confirm by inspection of documented evidence that the EUT has an effective method to limit the outgoing rate to be within the given limit of 2 Mbytes/s (see 7.3.8.4). 67

8.12 PGN to network gateway function (PNGF)

(see 7.4)

8.12.1 General

Check that it is possible to enter unique SFIs for all sources distinguished by different devices and that the mapping of SFI to sources distinguished by different device identifier is correctly implemented by analysing the UDP datagrams.

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

8.12.2 Output buffer management

Verify the output routing by feeding the network under test with datagrams containing PGNs for all IEC 61162-3 networks and check that PGNs are routed to the network having the set device identifier.

Check that documentation is available describing the maximum buffer capacity.

Check that the means are provided to configure the maximum buffer capacity.

Check that the overflow is logged as required.

8.12.3 Datagram output

Verify datagram conversion by feeding the input ports of the network under test with PGNs and check if these are transmitted in UDP datagrams as described in 7.4.1.

Verify a single IEC 61162-3 PGN message transmission per each feeding IEC 61162-450 message.

8.12.4 PGN group

Verify PGN group filtering by transmitting four PGN groups and check that the device only receives the PGN group messages to which it belongs.

8.12.5 Address conflicts

Confirm by observation that the EUT assigns new IEC 61162-3 addresses at the address translation table within 1 min when IEC 61162-3 addresses at the EUT conflict with the addresses in IEC 61162-3 Network.

8.13 System function ID resolution

(see 7.5)

Confirm by observation that the EUT sends SRP sentences to address 239.192.0.56 port 60056 when boot up, 1 min after boot up, 5 min after boot up and after reconfiguration, including both reconfiguration of setup parameters and reconfiguration based on a change caused by redundancy arrangements.

NOTE The boundaries of test for redundancy arrangements are the connections from each of its physical interfaces to their immediate switches only. **68**

Confirm by observation that when the EUT receives an SRP sentence with all fields being null fields the EUT responds with an SRP sentence with the fields populated. **69**

8.14 Binary file transfer using TCP point-to-point

(see 7.6)

8.14.1 Test of transmit client

8.14.1.1 Description

The test set-up is a controllable receiver server and the equipment under test. The following tests shall be performed and passed.

8.14.1.2 Connection establishment test

Remove receiver server from the network and power up the transmit client. Confirm by observation that the transmit client performs reconnection attempts as specified.

Connect receiver server and confirm by observation that connection is established.

8.14.1.3 Lost connection test

Power down or physically remove receiver server from the network and confirm by observation that the transmit client detects connection failure. This will normally require the transmission of some data from the transmit client.

Reconnect receiver server and confirm by observation that the transmit client reconnects the receiver server. Confirm by observation that the transmit client sends data as specified. Confirm by observation that the headers are according to the data format specification. Confirm by observation that time stamp is increased.

Break connection in the middle of a transfer. Confirm by observation that the transmit client continues to operate and tries to reconnect.

8.14.2 Test of receiver server

8.14.2.1 Test set-up

The test set-up is a controllable transmit client and the equipment under test. The transmit client shall be able to generate the following, and tests shall be made that check the correct functioning of the receiver server in these cases.

8.14.2.2 Connection establishment test

Remove transmit client(s) from the network and power up receiver server. Confirm by observation that receiver server starts up as specified.

Connect transmit client(s) and confirm by observation that receiver server enters normal operation.

8.14.2.3 Lost connection test

Break connection in the middle of a transfer. Confirm by observation that the receiver server continues to operate.

8.14.2.4 Message transfer test

Transfer at least one file with a content type which is supported by the receiver server, streamed as a sequence of at least 5 datablocks. Confirm by observation that the receiver server correctly processes the file.

8.14.2.5 Multiple transmit client test

If the receiver server supports simultaneous connections from multiple transmit clients, establish the maximum number of connections according to the manufacturer. Send files simultaneously over all connections. Confirm by observation that the receiver server correctly processes all received files.

8.14.2.6 Erroneous input test

Send a file with datalength in the header set to a value which is smaller than the actual size of transmitted data. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

Send a file with an invalid crcHeader value in the header. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

Send a file which is streamed as at least 5 packets. Discard the 3rd packet. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

8.14.2.7 Undefined header test

Send a file with the header version set to a value higher than defined in this document. Confirm by observation that the receiver server ignores the unknown part of the header based on the implemented header version and that the receiver server processes the file.

8.14.3 Maximum outgoing rate

Confirm by inspection of documented evidence that the EUT has an effective method to limit the outgoing rate to be within the given limit.

8.14.4 TCP port and IP addresses

Confirm by inspection of manufacturer's installation documentation that the default port is specified as 7097 and that there are instructions to set both sender and receiver in the same IP address range.

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 gives default classification of each of the IEC 61162-1 sentence formatters as belonging to one of the following three types of message:

- sensor broadcast message (SBM), see 3.22;
- multi-sentence message (MSM), see 3.14;
- command-response pair (CRP), see 3.4.

If provided by the equipment, the default transmission group and classification can be changed by the parameter setup system of the equipment to USR1 to USR8, RCOM, PROP in Table 4 or any in Table 5.

A.2 Talker identifier mnemonic to transmission group mapping

Table A.1 maps the two first characters of the SFI, which 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. ~~For alert communication purposes, an alert source may use transmission group BAM1, BAM2 or transmission group based on Table A.1.~~

For alert communication purposes, an alert source shall use transmission group BAM1 or BAM2 as default or, if in addition optional configuration of transmission groups is provided, any transmission group in Table 4 and Table 5.

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
CAM of BAM	CA	CAM1 or CAM2
Communications: digital selective calling (DSC)	CD	RCOM
data receiver	CR	RCOM
satellite	CS	RCOM
radio-telephone (MF/HF)	CT	RCOM

Type of equipment	Talker identifier	Transmission group
radio-telephone (VHF)	CV	RCOM
scanning receiver	CX	RCOM
Direction finder	DF	NAVD
Duplex repeater station	DU	MISC
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
Network device	ND	NETA
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
Voyage data recorder	VR	MISC
Watertight door controller/monitoring system	WD	VDRD
Water level detection system	WL	VDRD
Transducer	YX	MISC

Type of equipment	Talker identifier	Transmission group
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.~~ 70		

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 CRP 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	X	ABM Sometimes single
ACA	AIS channel assignment message		X		ACA, ACS Sometimes single
ACK	Acknowledge alarm			X	ALR~~, ACK~~
ACN	Alert command	~~X~~		X	AGL 71, ALC, ALF, ARC
ACS	AIS Channel management information source		X		ACA, ACS
AGL 71	Alert group list			X	ALC, ALF
AIR	AIS Interrogation request			X	ABK
AKD	Acknowledge detail alarm condition			X	ALA~~, AKD~~
ALA	Report detailed alarm condition			X	~~ALA,~~ AKD
ALC	Cyclic alert list		X		~~CAN~~ACN
ALF	Alert sentence		X		~~CAN~~ACN
ALR	Set alarm state	X		X	~~ALR,~~ ACK
APB	Heading/track controller (autopilot) sentence B	X			
ARC	Alert command refused	~~X~~		X	~~CAN~~ACN
~~AUC~~	~~Automated procedure control~~	~~X~~			
~~AUQ~~	~~Automated procedure query~~	~~X~~			
~~AUS~~	~~Automated procedure status~~	~~X~~			
BBM	AIS Broadcast binary message		X	X	BBM Sometimes single

	Description	SBM	MSM	CRP	Related sentence formatters
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			
~~CBR~~ 72	~~Configure Broadcast Rates for AIS AtoN Station Message Command~~		~~X~~	~~X~~	~~MEB~~ ~~Sometimes single~~
CUR	Water current layer – multi-layer water current data	X			
~~CYL~~ 72	~~Cyclic procedure list~~		~~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			
~~ECI~~ 72	~~Enhanced selective calling information~~	~~X~~			
EPM 71	Command or report long equipment property value	X			
EPV	Command or report equipment property value	X			
ETL	Engine telegraph operation status	X			
EVE	General event message	X			
FIR	Fire detection		X		FIR
FSI	Frequency set information	X			
~~FSS~~ 72	~~Frequency selection set~~	~~X~~			
GBS	GNSS satellite fault detection	X			
GDC 71	GNSS differential correction	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			
GSN 71	GNSS SBAS navigation message	X			
GST	GNSS pseudorange noise statistics	X			
GSV	GNSS satellites in view	X			
HBT	Heartbeat supervision sentence	X			
HCR	Heading correction report	X			
HDG	Heading, deviation and variation	X			

	Description	SBM	MSM	CRP	Related sentence formatters
HDT	Heading true	X			
HMR	Heading monitor receive			X	HMS
HMS	Heading monitor set			X	HMR
HRM	Heel angle, roll period and roll amplitude measurement device	X			
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	X	LRF, LRI
LR2	AIS long-range reply sentence 2		X	X	LRF, LRI
LR3	AIS long-range reply sentence 3		X	X	LRF, LRI
LRF	AIS long-range function		X	X	LR1, LR2, LR3, LRF
LRI	AIS long-range interrogation		X	X	LR1, LR2, LR3, LRF
~~MEB~~ **72**	~~Message input for broadcast command~~		~~X~~	~~X~~	~~CBR~~ ~~Sometimes single~~
MOB	Man over board notification	X			
MSK	MSK receiver interface	X			
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
NLS **71**	Navigation light status	X			
NRM	NAVTEX receiver mask			X	NRX
NRX	NAVTEX received message		X		
NSR	Navigation status report	X			
~~OCC~~ **72**	~~Occupation control~~	~~X~~			
OSD	Own ship data	X			
POS	Device position and ship dimensions report or configuration command			X	
PRC	Propulsion remote control status	X			
RLM	Return link message	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			
RRT	Report route transfer	X			
RSA	Rudder sensor angle	X			
RSD	Radar system data	X			
RTE	Routes	X			

	Description	SBM	MSM	CRP	Related sentence formatters
SEL 71	Selection report	X			
SFI	Scanning frequency information	X			
~~SSD~~ 72	~~AIS ship static data~~			~~X~~	
SLM 71	Steering location/mode	X			
SM1	SafetyNET message, All ships/NavArea	X			
SM2	SafetyNET message, Coastal warning area	X			
SM3	SafetyNET message, Circular area address	X			
SM4	SafetyNET message, Rectangular area address	X			
SMB	IMO SafetyNET message body	X			
SMV 71	SafetyNET message, Vessel in distress information	X			
SPW	Security password sentence		X		
SRP	System function ID resolution protocol	X			
SSD 71	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
TRL	AIS transmitter-non-functioning log	X			
TTD	Tracked Target Data		X		
TTM	Tracked target message	X			
TUT	Transmission of multi-language text		X		
TXT	Text transmission		X		Sometimes single
UID	User identification code transmission	X			
VBC 71	Water-referenced and ground-referenced docking speed data	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		Sometimes single
VDR	Set and drift	X			
VER	Version		X	X	Sometimes single
VHW	Water speed and heading	X			
VLW	Dual ground/water distance	X			
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			

	Description	SBM	MSM	CRP	Related sentence formatters
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
(normative)

TAG block definitions

B.1 Validity

The material in Annex B is a subset of a definition of a parameter structure from NMEA 0183 intended for adding information to IEC 61162-1 sentences. Conformance with this document on the sending side will guarantee conformance to NMEA 0183, but the description herein is not complete and a receiver that only implements Annex B will not be able to process all valid TAG block structures.

B.2 Valid TAG block characters

The "\" (back-slash) character is designated as the "TAG block delimiter". A TAG block shall begin and end with a TAG block delimiter.

The closing delimiter character is always preceded by the checksum (*hh) of the TAG block content. The TAG block closing "\" appears before a symbol beginning a sentence, either a "$" or "!"; another Tag Block, "\"; or the <CR><LF> symbols.

The beginning TAG block "\" symbol shall follow the "<CR><LF>" symbols at the end of the preceding sentence or before any other character is transmitted.

The maximum number of characters in a TAG block shall be 80 characters including the TAG block delimiters.

IEC 61162-1 requires that the maximum number of characters in a sentence shall be 79 characters between the starting delimiter "$" or "!" and terminating delimiter <CR><LF>. The "$" or "!" is always recognized as the beginning of an IEC 61162-1 sentence. The character content of a TAG block, plus the TAG block delimiters, is not included in the sentence character count.

The contents of the TAG block (valid characters between the two "\" characters) may contain any valid character (see "Valid characters" table in IEC 61162-1~~:2016, Table 2~~ **17**) and some of the reserved characters (see "Reserved characters" table in IEC 61162-1~~:2016, Table 1~~ **17**).

The TAG block shall not contain either the TAG block delimiter, or the start of sentence delimiters, "$" or "!", or characters reserved for future use; the "~" or <del> characters.

The remaining reserved characters (<CR>, <LF>, ",", "*", and "^", found in the "Reserved characters" table in IEC 61162-1~~:2016, Table 1~~ **17**) shall be used as defined in ~~Table 1 of~~ IEC 61162-1~~:2016~~ **17**.

Additional rules are described in Clause B.3. **73**

B.3 TAG block format

Each TAG block may contain one or more parameters consisting of a "parameter-code" and "parameter value." Each parameter value may be either a numeric value or a character string constructed of valid IEC 61162-1 characters as discussed in Clause B.2. The parameter-code consists of alphabetic characters only. Parameter-code and parameter value are separated by a colon (":").

The syntax for a TAG block is described below, in Extended Backus-Naur Form (EBNF) notation. The format is the same as that used in the XML specification and a brief explanation is given below.

parameterCode::= [a-zA-Z0-9]+

numericValue::= '-'? [0-9]+ ('.'[0-9]+)?

characterString::= [-. A-Za-z0-9]+

checksum::= [0-9A-F] [0-9A-F]

parameterPair::= parameterCode ':' (numericValue | characterString)

parameterList::= parameterList ',' parameterPair | parameterPair

TagBlock::= '\' parameterList '*' checkSum '\'

An additional constraint for the TAG block is that it shall be 80 or less characters long. When it appears, it shall be followed by another TAG block, a valid IEC 61162-1 sentence or a carriage return and line feed pair.

Two examples of syntactically valid TAG blocks are listed below:

\a:0.23,b:All the kings men – but jack.,c:-23*hh\

\d:A*hh\

A brief description of the EBNF notation follows below. The complete description can be found in W3C XML.

Any character in single quotes is itself, i.e., ':' is just a colon.

The square brackets denote exactly one character from the set of characters listed within. The dash ("-"), unless appearing as the first character, defines a range of characters, i.e. "[0-9A-F]", is one character in the range zero to nine or A to F. A dash as the first character represents itself in the selection.

The plus sign means that the immediately preceding character can be repeated one or more times. Thus, "[0-9]+" specifies a integer number, possibly with leading zeros.

The vertical bar ("|") specifies a selection. Either the left or right hand side expression is valid.

Ordinary parentheses group an expression and can be used in conjunction with the plus sign or the horizontal bar.

B.4 TAG block "hexadecimal checksum" (*hh)

In order to improve the integrity of the parameters in a TAG block, the "Exclusive OR" hexadecimal checksum (*hh), that is calculated for every IEC 61162-1 sentence shall also be used for the content of each TAG block ~~(see examples below)~~. The checksum is the 8-bit Exclusive OR (no start or stop bits) of all characters in the TAG block, including the "," and "^" delimiters, between but not including the beginning "\" character and the "*" checksum delimiter.

B.5 TAG block "line"

A TAG block "line" can be formed in three ways.

1) The TAG block can appear alone to form a "line".
2) The TAG block may precede a sentence to form a "line" with an associated IEC 61162-1 sentence.

3) Multiple TAG blocks may appear one after another to form a "line" or they may precede a sentence to form a "line" with an associated IEC 61162-1 sentence.

A TAG block "line" is only valid when either a <CR><LF> immediately follows the last TAG block closing "\" symbol, or when a valid IEC 61162-1 sentence immediately follows the TAG block closing "\" symbol. TAG blocks are linked with a sentence when no <CR><LF> or any characters separate the TAG block and sentence.

B.6 TAG block parameter-code dictionary

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

Table B.1 – Defined parameter-codes

Parameter-code	Description	Form of parameter value
a	General authentication	Alphanumeric string (32 char. maximum)
c	POSIX time	Positive integer
d	Destination-identification	Alphanumeric string (15 char. maximum)
g	Sentence-grouping	Grouped numeric string (alphanumeric)
n	Line-count	Positive integer
r	Relative time	Positive integer
s	Source-identification	Alphanumeric string (15 char. maximum)
t	Text	Free text, including proprietary information
~~a~~	~~General authentication~~	~~Alphanumeric string (32 char. maximum)~~
x	Destination cluster identification	Alphanumeric string (3 char.)
z	Source cluster identification	Alphanumeric string (3 char.) **74**

Annex C
(normative)

Reliable transmission of command-response pair messages

C.1 Purpose

The rules that are listed in Annex C 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.

The requirements of Annex C are not applicable for SNGF and PNGF as they only act as converter between original sender and original receiver(s).

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, and
- 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.

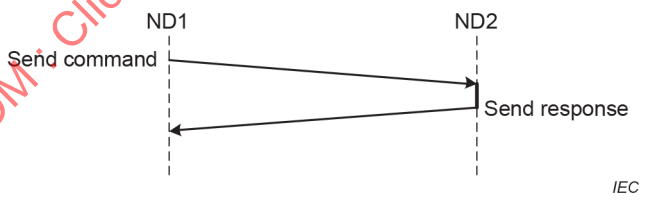


Figure C.1 – Command response communications

C.4 Requirements

The requirements for reliable communication are the following:

- 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;
- optionally, TAG block parameter "n" ~~shall~~ may 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. It shall be sent by each ~~450~~ node 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>
```

Annex D
(informative)

Compatibility between ~~IEC 61162-450~~ nodes based on IEC 61162-450:2011 connected to a network which uses methods based on later editions of IEC 61162-450~~:2018~~

D.1 General

The hosts (i.e. ~~450-~~nodes) in IEC 61162-450:2011 are not required to implement IGMP protocol. When the IGMP snooping introduced in IEC 61162-450:2018 is enabled, a switch snoops IGMP join message for multicast groups and maintains per port information of multicast groups into which the port belongs. When a multicast message is received, the IGMP enabled switch forwards the message only to ports which belong to this multicast group. Since the multicast traffic filtering at the switch is based on the snooping of IGMP join messages, the ~~450-~~nodes of IEC 61162-450:2011, which do not implement IGMP protocol, will not receive the IEC 61162-450 traffic. The IGMP snooping prevents only reception of the messages. It does not cause any problem for the transmission of the messages by the ~~450-~~node.

D.2 Alternative methods for compatibility

D.2.1 Use of IGMP proxy node

One method for a ~~450-~~node based on IEC 61162-450:2011, which is non-IGMP capable, to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is IGMP proxy node.

When switches are enabled to do IGMP snooping, there is no way to receive multicasting messages without sending an IGMP join message from the ~~450-~~node to the switch. A special node, an IGMP proxy node, which sends an IGMP join (and IGMP leave) message instead of the non-IGMP capable ~~450-~~node is required to be between the ~~450-~~node and the switch. This means that all non-IGMP capable ~~450-~~nodes should be connected to an IGMP snooping enabled switch through a virtual IGMP agent. An IGMP proxy node collects the multicast membership information from the non-IGMP capable network (automatically or by configuration), and sends IGMP join (and maybe IGMP leave) messages periodically for the detected multicast groups. The IGMP proxy node also replies to IGMP membership report requests from the switch.

D.2.2 Use of virtual LAN (VLAN)

D.2.2.1 Method

Another method for a ~~450-~~node based on IEC 61162-450:2011, which is non-IGMP capable, to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is VLAN.

IGMP snooping could be configured with per VLAN at a switch. This is only related with the setup of the switch and requires nothing to do with the ~~450-~~node. When a port at a switch is connected directly or indirectly to nodes with non-IGMP capable nodes, then the ports are allocated the specific VLAN ID(s), which is configured to disable the IGMP snooping. The system designer or integrator may assign a special VLAN ID for the non-IGMP capable ~~450-~~nodes in the networks.

VLAN can be used to avoid the burden of receiving all binary file transfers from ports in Table 5. A VLAN ID can be assigned to each binary file transfer port or some ports of the binary file transfer. This means that the system integrator could plan the system so that binary file transfers are not shared by all users who are not interested in the binary file transfers.

D.2.2.2 Requirements for switches

The following are required at a switch to support IGMP snooping compatibility based on VLAN:

a) means to configure VLAN for each Ethernet port;

b) means to enable or to disable IGMP snooping per each VLAN.

D.2.3 Use of static multicast switch configuration

A third method for a ~~450~~ node based on IEC 61162-450:2011 which is non-IGMP capable to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is to use static multicast switch configuration.

Managed switches typically provide the ability to define at switch port level which ports will receive data from multicast groups. This is often referred to as static multicast or static multicast routing and involves configuring the IP/MAC address of a multicast group to which a non-IGMP capable device wishes to receive data from and associating it with the network port of the device on the switch. As multicast data is received at the IP/MAC address on the switch, it is provided to the device without any explicit IGMP join requests.

Annex E
(informative)

Use of switch setup configuration to filter network traffic

Typically, a simple network consisting of only IEC 61162-1 sentences and screen capture images from radars and ECDIS to VDR, and ECDIS route exchange transmitted over LAN using IEC 61162-450 protocol would not need any filtering of the network traffic. Often, there is a need to share the same LAN infrastructure for things like raw radar video, CCTV pictures, transfer of SENC databases, etc. Such additional traffic is defined as ONF by this document. The issue is that such additional traffic may cause too high a CPU load for some of the simple ~~450~~ nodes connected to the shared network infrastructure. There are many possibilities to address the issue of the filtering of the network traffic.

Annex E explains one family of methods. This family of methods uses network infrastructure elements, namely switches, to perform the filtering. ~~This document is for 450 Nodes and therefore it includes "shall" requirements only for the 450 Nodes. Annex E is informative because it describes the use of network infrastructure elements.~~ **75**

One method to filter or control network traffic is to use setup configuration of the managed switches. Such setup would typically allow traffic filtering based on any combination of

- the physical port,
- the logical port number,
- the protocol type,
- the source IP address,
- the source MAC address,
- the destination IP address,
- the destination MAC address, and
- the VLAN.

There are no international standards by IEEE, IETF, etc. to do this setup, but there is a de facto method called Access Control List (ACL). Typical of all methods used to control the setup is that the setup configuration can be stored as a simple text file which could be fed by a computer into the switch. Therefore, such methods offer a high level of manageability for an organization that makes system design or service and support (for example a company could create an environment in which experts prepare setup configurations as files, the setup files are centrally stored to be available in a cloud and the service and support persons can utilize these setup files while performing service and support).

Annex F
(normative)

Sentence to support SFI collision detection

F.1 General

Annex F describes details of a ~~new~~ sentence used to support implementation of a ~~450~~ network.

NOTE Refer to IEC 61162-1 for possible later versions of this sentence.

F.2 SRP – System function ID resolution protocol

This sentence is used to assist detection of possible system function ID (SFI) ~~conflicts~~ collision.

This sentence is transmitted as specified in this document (see 7.5). This sentence cannot be queried.

~~\s:ccxxxx*hh\$--SRP,x,hhhhhhhhhhhh,c--c*hh<CR><LF>~~
~~IP address [4]~~
~~MAC address [3]~~
~~Instance number of redundant alternative [2]~~
~~SFI of the transmitter [1]~~

```
\s:ccxxxx*hh\$--SRP,x,hhhhhhhhhhhh,c--c*hh<CR><LF>
     |                |       |       |
     |                |       |       └─ IP address [4]
     |                |       └──MAC address [3]
     |                └─ Instance number [2]
     └─ SFI of the transmitter [1]
```

Comments:

1) Reported SFI of the transmitter.

2) ~~Instance number for interface redundancy (i.e. number of physical port for identical SFI), null if interface redundancy not in use. The instance numbers shall be ordinal with no skipping (1, 2, 3,...).~~ Instance number for available interfaces with the same SFI (i.e. number of physical port for identical SFI), null field if there is only one interface with identical SFI available. In case there is more than one interface using intentionally the identical SFI, the numbering starts with 1. The instance numbers shall be ordinal with no skipping (1, 2, 3, etc.). **33**

3) Reported MAC address used by SFI, 48bit hexadecimal number, for example 32613C4EB605.

4) Reported IP address used by SFI as text string, for example ~~239.192.0.1~~ 192.168.0.10. **59**

Annex G 76
(informative)

Examples for SRP sentences and SFI collision detection

G.1 SFI collision detection

For the case where, in two SRP messages, the pair of SFI and instance number is equal and the pair of MAC address and the IP address is deviating, there is a (potential) conflict of SFI numbering in the system.

There could be at least three kinds of redundancy:

a) redundancy based on multiple SF available in a single network for the same purpose;

b) redundancy based on reuse of SFI but using separate MAC addresses;

c) redundancy based on multiple isolated networks.

The SFI collision detection is intended to detect conflicts within a single network. Multiple isolated networks may or may not reuse the same SFI value, see 4.4.2.

A potential SFI collision is detected within a single network when in two SRP messages the pair of SFI and instance number is equal and the MAC address or the IP address is not equal.

There could be also a need to use separate physical interfaces for different but related purposes for which there is a need to use a common SFI. For example, traffic related to the functionality of the equipment and traffic related to alert management could be available from separate physical interfaces. This could be the case for all physical interface types, but it is assumed that this is more common in the case of physical interfaces based on serial lines, for example IEC 61162-1 or IEC 61162-2.

G.2 Examples for SRP sentences

G.2.1 Redundancy on network level only

G.2.1.1 Two network interfaces provide the same information

In this use case there are two separate network interfaces connected to the same single network, see Figure G.1.

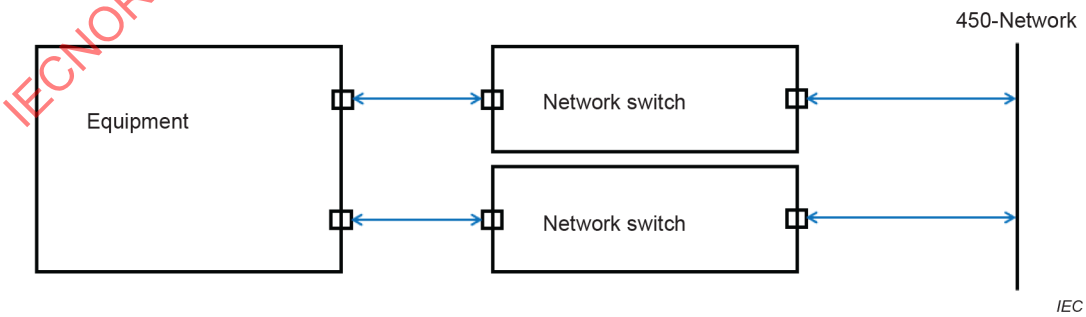


Figure G.1 – Two separate network interfaces connected to the same single network

Two active physical network interfaces with identical payload in data transfer. No link aggregation (also known as teaming/bonding, see G.2.1.3) is present. The EUT sends the same packet but either with the same source IP address or a different source IP address or a different source parameter code or some combination from each connected network interface to the same multicast group. The receiving device decides which of two identical packets to process and which should be discarded.

The data is transmitted on the same IEC 61162-450 network.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.1) both reporting using two physical interface, see Figure G.2. No SFI collision.

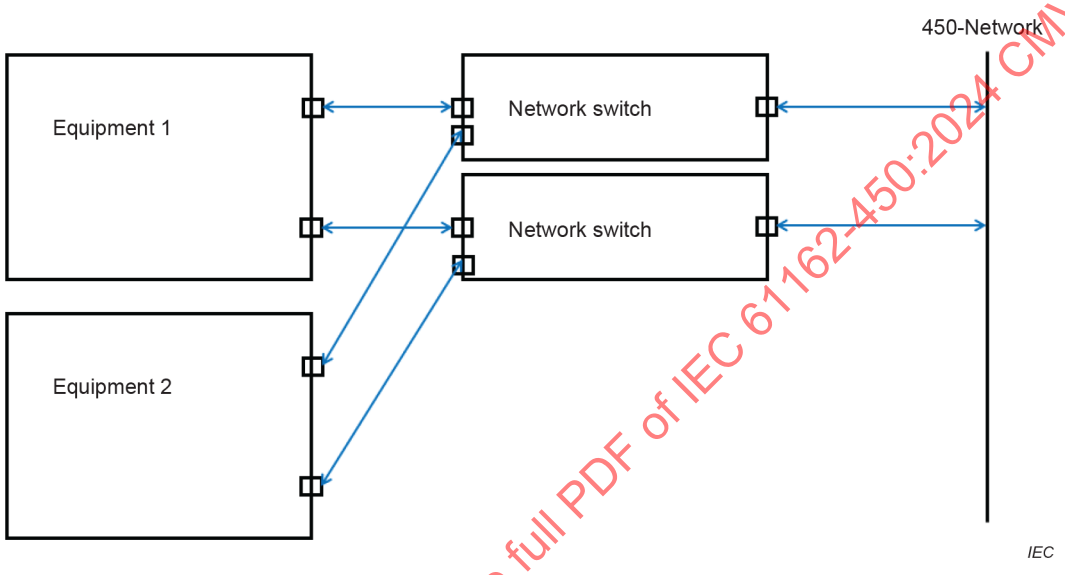


Figure G.2 – An example of two equipment

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0002*5C\$GPSRP,1,02004F68901C,192.168.0.21*46<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0002*5C\$GPSRP,2,02003D41FCB3,192.168.0.22*47<CR><LF>
```

- Example 2: two equipment both reporting using two physical interface, see Figure G.2. SFI collision as same SFI is shared by two separate equipment:

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0001*5F\$GPSRP,1,05A3CE170137,192.168.0.53*34<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0001*5F\$GPSRP,2,86FD61AC2802,192.168.0.30*41<CR><LF>
```

G.2.1.2 Two network interfaces provide the same information

This style may be called link, teaming, etc.

In this use case, there are two separate networks interfaces connected to the same single network but only one of the network interfaces is sending at any one time (this sending is controlled by the equipment), see Figure G.3.

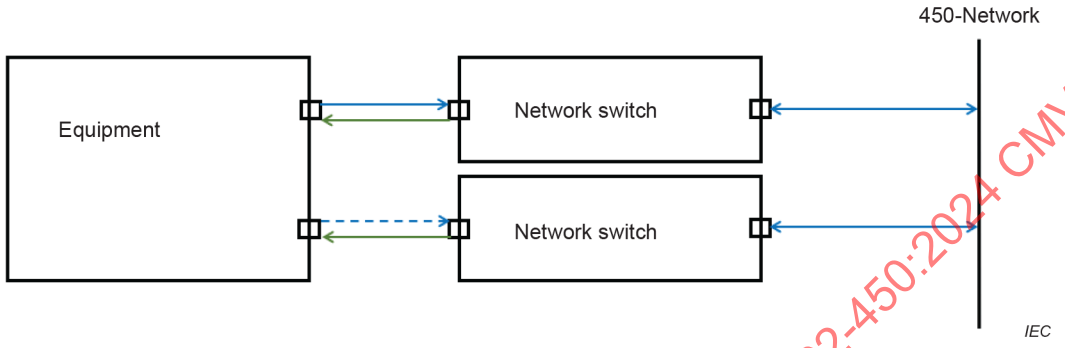


Figure G.3 – Two separate networks interfaces connected to the same single network, but only one of the network interfaces is sending at any one time

Both physical interfaces of the equipment provides/processes identical information. To the receiving equipment in the network, the equipment is identified as only "one connection". A switching over between the separate physical interfaces to be sender is managed by the equipment based on missing traffic from one of the physical interfaces.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.3) both reporting using two physical interface, see Figure G.4. No SFI collision.

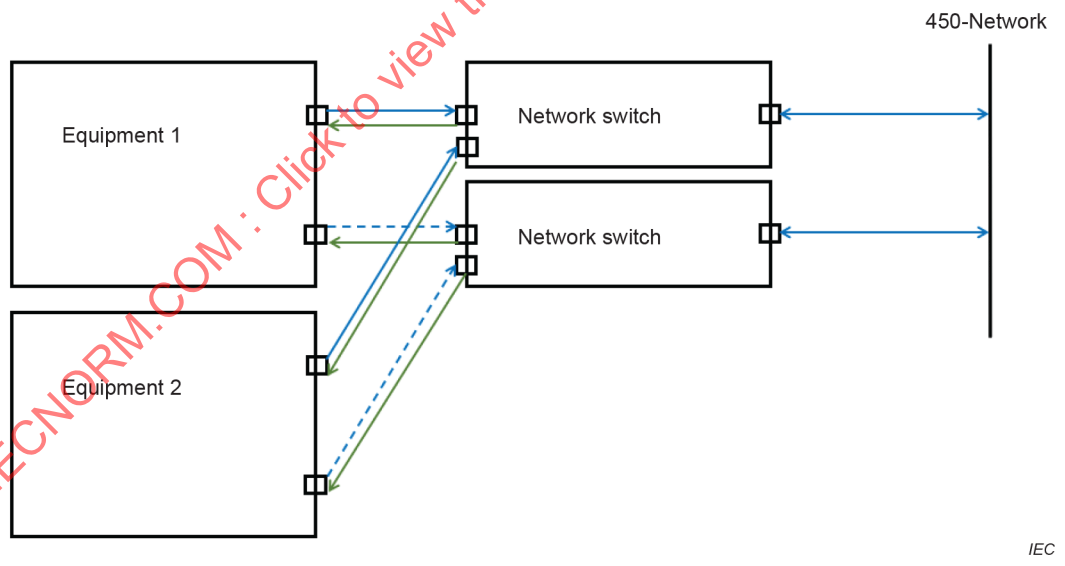


Figure G.4 – An example of two equipment

SRP equipment 1, interface 1. Note that, if this is sent, then interface 2 is not sending.

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2. Note that, if this is sent, then interface 1 is not sending

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1. Note that, if this is sent, then interface 2 is not sending

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

SRP equipment 2, interface 2. Note that, if this is sent, then interface 1 is not sending

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

- Example 2: two equipment (i.e. two sets of the cases in Figure G.3) both reporting using two physical interface, see Figure G.4. SFI collision occurs as the same SFI is shared by two separate equipment.

  Equal SFI on all interfaces, for equipment 2 deviating pair of MAC address and IP address

  SRP equipment 1, interface 1

  ```
  \s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
  ```

  SRP equipment 1, interface 2

  ```
  \s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
  ```

  SRP equipment 2, interface 1

  ```
  \s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
  ```

  SRP equipment 2, interface 2

  ```
  \s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
  ```

G.2.1.3 Link aggregation/teaming mode

In this use case, there are two separate network interfaces connected to the same single network, but a network switch controls the traffic so that the equipment is seen as one interface, see Figure G.5.

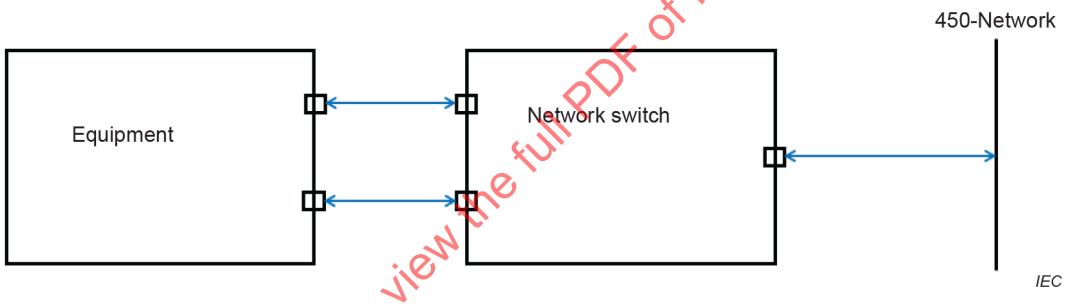


Figure G.5 – Two separate network interfaces connected to the same single network but a network switch makes the equipment to be seen as one

Both physical interfaces of the equipment provide/process identical information. To the equipment in the network, the equipment is identified as only "one connection". A network switch manages that the equipment is seen as one logical interface. Note that traffic from both physical interfaces of the equipment is available in the network.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.5) both reporting using two physical interfaces, see Figure G.6. No SFI collision.

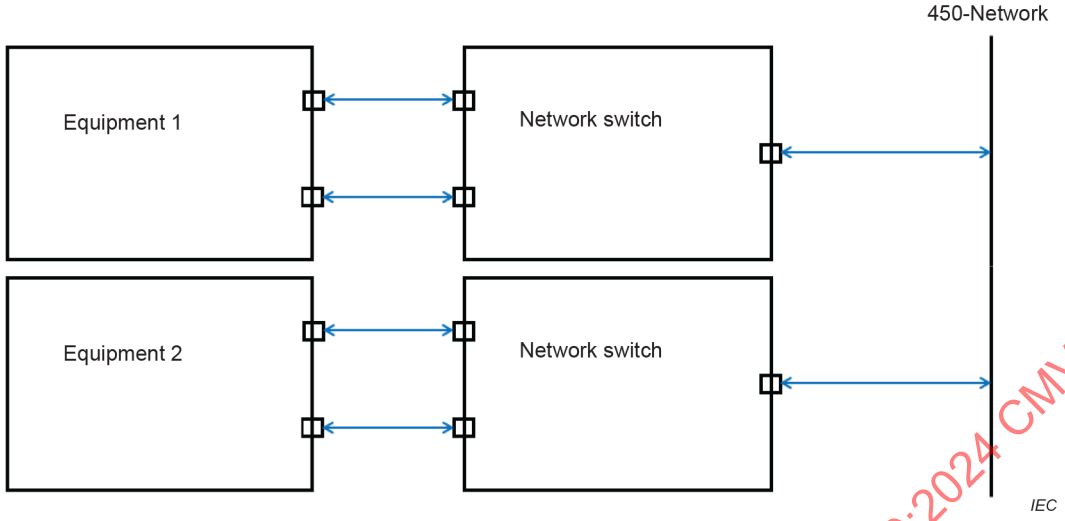


Figure G.6 – An example of two equipment

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

- Example 2: two equipment (i.e. two sets of the cases in Figure G.5) both reporting using two physical interface, see Figure G.6. SFI collision occurs as the same SFI is shared by two separate equipment.

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

G.2.2 Examples for redundancy on network and serial (to network) level

G.2.2.1 One equipment with redundant serial interfaces is connected to two different SNGFs

In this use case, there are two separate serial interfaces connected through two separate SNGF to the same single network, see Figure G.7.

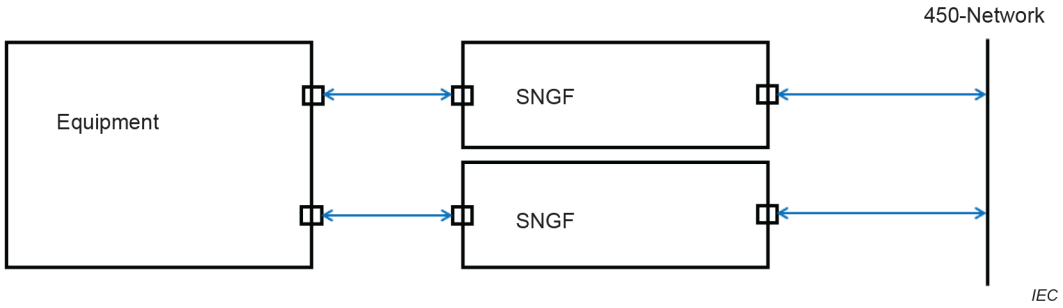


Figure G.7 – One equipment with two separate serial interfaces connected through separate SNGFs to the network

Two active physical serial interfaces with identical data transfer. The recipient can decide which channel he would like to process. For redundancy reasons, it is connected to two SNGFs. The two SNGFs distribute the identical information with the same SFI to the network. The combination of two source parameter codes "s" is unique within the 450-Network.

- EXAMPLE 1: one equipment reporting using two physical interfaces, see Figure G.7. No SFI collision:

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\\s:SI0001*hh\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\\s:SI0002*hh\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>`

  NOTE Although the second interface is providing the same serial line information, it is important that the instance number on SNGF 2 for the second serial interface is increased. Otherwise, the SFI failure detection will detect a SFI configuration error. The processing of redundant serial line information needs to be handled on system integration level by the recipient.

- Example 2: one equipment reporting using two physical interfaces, see Figure G.7. SFI collision as instance numbers of the SFI are not available (instance number-field is null):

  Correctly equal SFI on all interfaces and deviating pair of MAC address and IP address for the SNGFs, but null fields in the instance fields.

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\$GPSRP,,0091A5814187,192.168.0.12*0D<CR><LF>`

G.2.2.2 One data source has two different serial interfaces on which it provides different information to different SNGFs

In this use case, there are two separate serial interfaces connected through two separate SNGF to the same single network, see Figure G.7.

Two active physical serial interfaces with different information, e.g., one for data and another for BAM. Both are connected to different SNGFs.

NOTE 1 The case that one data source (device) provides different information on separate serial lines to one SNGF needs to be handled by this SNGF.

- Example 1: one equipment reporting using two physical interfaces, see Figure G.7. No SFI collision:

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>`

NOTE 2 It is important that the instance number on SNGF 2 for the second serial interface is increased. Otherwise, the SFI failure detection will detect a SFI configuration error. The processing of redundant serial line information needs to be handled on system integration level.

- Example 2: one equipment reporting using two physical interfaces, see Figure G.7. SFI collision as instance numbers of the SFI are not available (instance number-field is null):

  SRP SNGF 1, (serial interface 1)

  ```
  \s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
  ```

  SRP SNGF 2, (serial interface 2)

  ```
  \s:GP0001*5F\$GPSRP,,0091A5814187,192.168.0.12*0D<CR><LF>
  ```

G.3 Other uses of SRP sentence

When a source is redundantly available and redundant traffic is identified by the instance numbers. It is possible to monitor the correct configuration or healthy of the source.

If in this case, there is a SRP message with a SFI and instance ‘1’ and a corresponding SRP message with an instance ‘2’ is missing:

- the device with instance ‘2’ is switched off, is defective (i.e. unhealthy); or
- the device transmitting instance ‘1’ is wrongly configured and has to send a null field in the instance field.

If in this case, there is a SRP message with a SFI and instance ‘2’ and a corresponding SRP message with an instance ‘1’ is missing:

- the device with instance ‘1’ is switched off, is defective (i.e. unhealthy); or
- the device transmitting instance ‘2’ is wrongly configured and has to send a null field in the instance field.

Annex H 77
(normative)

Reserved cluster identifiers

The reserved cluster identifiers are specified in Table H.1.

Table H.1 – List of reserved cluster identifiers

Identifier	Cluster name	Description	Operator (example)
Nav	Navigation	Navigation bridge	Navigator
Com	Communication	Ship's communication	Radio operator
Aut	Automation	Engine room domain	Engineer
Cgo	Cargo	Regarding the payload of the ship	Chief officer/Supercargo
Htl	Hotel	Passenger related services	Hotel manager (passenger vessels)
ICT	ICT	Office network	ICT manager
SSe	Safety/Security	Access monitoring	Ship security officer
Pos	Position control	Dynamic position or mooring control	DP/mooring operator
ROV	Remote operated vehicle	ROV control centre	ROV operator

Bibliography

IEC 60603-7:2020, *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 61162-450:2011, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*[2]

IEC 61162-460, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security*

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 interconnecting devices and passive components – 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: Performance requirements, methods of testing and required test results*

IEC 62388~~:2007~~, *Maritime navigation and radiocommunication equipment and systems – Shipborne radar – Performance requirements, methods of testing and required test results*~~3~~

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

ISO/IEC 8859-1, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*

ITU-R Recommendation M.1371, *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile band*

IEEE 802, *IEEE standard for local and metropolitan area networks: Overview and architecture*

ISOC RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)* **78**

ISOC RFC 793, *Transmission control protocol*

---

2 This publication has been withdrawn.

~~3 This document has been withdrawn, but for the purpose of this document, it is given as a reference.~~

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

ISOC RFC 966, *Host Groups: A Multicast Extension to the Internet Protocol* **78**

ISOC RFC 1321, *The MD5 Message-Digest Algorithm*

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 4: Registration Procedures*

ISOC RFC 4541, *Internet Group Management Protocol (IGMP) and Multicast listener discovery (MLD) snooping switches*

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

NMEA 0183:2008, *Standard for interfacing marine electronic devices, Version 4.00* **78**

ANSI/TIA~~/EIA~~-568, *Generic telecommunications cabling for customer premises*

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

W3C Recommendation, *Extensive markup language (XML)*, 1.0 (fifth edition). Available at: http://www.w3.org/TR/REC-xml/

List of comments

1 Dated reference not needed by IEC rules

2 Updated to newer edition

3 Moved to Bibliography

4 Added new alternative how to group

5 Clarify that one physical equipment may contain more than one SNGF function

6 The compatibility issue is: For a network to work with IGMP snooping, all equipment in the network will need to incorporate the same version of IGMP

7 Manufacturer is not allowed to specify below the applicable equipment standards

8 Clarify use of italics in this table

9 Specify how interface redundancy is implemented

10 Clarification: Previous short specification has been replaced by figures and longer text

11 Simplification of the content: Before two paragraphs in the end of this subclause, now a few words

12 Clarification: More detailed description how to handle proprietary sentences

13 Not needed

14 There is no “default SFI”, just “SFI used for administrative purposes”

15 More examples of “administrative purposes”

16 Simplification of the content: Before two paragraphs in the end of this subclause, now a few words, see 5th paragraph of this subclause

17 Amended style to avoid dated reference by IEC rules

18 Agreed to remove these installation related requirements

19 Updated to the latest editions

20 First two bullet points are applicable for all use cases of this standard. Five bullet points below are optional depending of the use case

21 Explains when UDP may not be needed

22 Explains when UDP multicast may not be needed

23 Explains when TCP may not be needed

24 Explains when ICMP may not be needed

25 Explains when IGMP may not be needed

26 Clarification of existing requirement

27 Explanatory note is improved for the most common industry practice

28 Clarification: Clearer version of the requirement

29 Clarification: Change single line into separate lines

30 Clarification: Clearer version of the description

31 Clarification: Longer description including examples

32 Clarification: What is detailed content of the requirement in the first paragraph of this subclause

33 Clarification of the use case

34 Clarification: More detailed description of how to use “g” parameter code

35 New requirement

36 Clarification for the case that a message contains more than one “s” parameter code
37 New requirement is that command (CRP type sentences) shall use “d” parameter code
38 Clarification for the case that a message contains more than one “d” parameter code
39 Change: Use of “n” is totally free, not so that if used once then shall be used by every
40 Clarify that value “1000” is newer used
41 Removed hard requirement replaced by example of optional use cases
42 Added alternative
43 Explains why use of MD5 may not be sufficient
44 New parameter codes to identify “cluster”
45 Change in requirement: SNGF may or may not retransmit faulty sentences
46 Existing requirement, but added to be available in the relevant process step
47 New standardized value for timeout
48 Figure 6 has always had this. It was just missing from the related textual description
49 Clarify the role of ACK message
50 Clarify what is clearing of receiver buffer
51 Clarify the textual description
52 Clarify that 1 + 3 = 4
53 Clarify the applicable use case
54 Guidance for the case that IEC 61162-450 compliant equipment is also intended to be IEC 61162-460 compliant
55 A change in specification. Note how to be downward compatible
56 There is no “default”, just the given value “SI0001”
57 There are no “defaults”, just used values “SI0001” and “TI0001”
58 Example improved for alternative ways to handle this case
59 Improved example
60 Added new example
61 Requirement change: Verification by documentation instead of test using physical equipment
62 Requirement change
63 Added as the use case is optional
64 Added test of a new option
65 Fix
66 Clarify use case of destination
67 Value added into the test for more easy reading
68 Added guidance for testing
69 Test of clarified requirement
70 This talker has been included into the 6th edition of IEC 61162-1
71 Added new sentence
72 Removed as not applicable
73 Clarification
74 Added new parameters codes

75 Change, for all nodes, not limited to those officially called “450-Nodes”

76 New annex providing guidance

77 New annex to standardize cluster identifiers for the new “cluster” feature added into this edition

78 Useful reference

_____

IEC 61162-450

Edition 3.0 2024-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques –
Partie 450: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet

IEC 61162-450:2024-04(en-fr)

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

a) clarification of serial to network gateway function (SNGF) in 4.5 with the addition of two new figures;

b) addition of further destination multicast addresses and port numbers in 6.2;

c) clarification of TAG block parameters in 7.2 together with Annex B, a new Annex H and associated tests in 8.9.4;

d) clarification of the sender process for binary files in 7.3.6 and the receiver process for binary files in 7.3.7 with updated Figure 6 and Figure 7;

e) clarifications of SFI collision detection and use of SRP sentence in 7.5 together with a new Annex G;

f) revision of tests for handling malformed data received on the serial line in 8.5.5.

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

Draft	Report on voting
80/1094/FDIS	80/1098/RVD

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

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

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

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

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

- reconfirmed,
- withdrawn, or
- revised.

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 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 document 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 document specifies an Ethernet based bus type network where any listener can receive messages from any sender with the following properties.

- This document 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 file), for example between radar and VDR, and also includes provisions for multicast distribution of information formatted according to IEC 61162-3, for example position fixes and other measurements.
- This document 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 document provides requirements only for equipment interfaces. By specifying protocols for transmission of IEC 61162-1 sentences, IEC 61162-3 PGN messages and general binary file data, these requirements will guarantee interoperability between equipment implementing this document as well as a certain level of safe behaviour of the equipment itself.
- This document permits equipment using other protocols than those specified in this document to share a network infrastructure, provided that it is supplied with interfaces which satisfy the requirements described for ONF.
- This document includes provisions for filtering of the network traffic in order to limit the amount of traffic to manageable level for each individual equipment.

This document does not contain any system requirements other than the ones that can be inferred from the sum of individual equipment requirements. An associated standard, IEC 61162-460, further addresses system requirements.

2 Normative references

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

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

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

IEEE Std 802.3-2022, *IEEE Standard for Ethernet*

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

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

ISOC RFC 826, *An ethernet Address Resolution Protocol*

ISOC RFC 1112, *Host Extensions for IP Multicasting, Standard STD0005 (and updates),* (include IGMP version 1)

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

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

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

ISOC RFC 3376, *Internet Group Management Protocol, Version 3*

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

ISOC RFC 5227, *IPv4 Address Conflict Detection*

ISOC RFC 5424, *The Syslog Protocol*

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.

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

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

3.1
ASCII
printable 7 bit character encoded in one byte

3.2
binary file
data block without formatting known to this protocol, i.e., non IEC 61162-1 formatted data, which can be transmitted with the protocol defined in 7.3 or in 7.5

Note 1 to entry: The term "binary file" 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

Note 1 to entry: 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 to entry: CRP are defined in Annex A.

Note 2 to entry: 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
atomic UDP transmission unit on the Ethernet as defined in ISOC RFC 768 and as constrained elsewhere in this document

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

Note 1 to entry: The types of Ethernet media that can be used for implementation of this document are defined in Clause 5.

3.7
function block
specified functionality implemented by equipment

Note 1 to entry: 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.

3.8
Internet Group Management Protocol
IGMP
communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships

Note 1 to entry: The IGMP is an integral part of IP multicast.

3.9
IGMP snooping
process of listening to Internet Group Management Protocol (IGMP) network traffic

3.10
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 1 to entry: The currently assigned numbers are listed in http://www.iana.org/assignments/port-numbers.

3.11
Internet protocol
IP
signalling protocol used and defined in ISOC RFC 791 (and updates)

3.12
message
collection of one or more sentences that are grouped by use of the TAG block grouping protocol or mechanisms internal to the sentence, for instance by sequence numbers as in the TXT sentence

Note 1 to entry: A stand-alone sentence is a message.

3.13
message type
classification of IEC 61162-1 sentence formatters into SBM, MSM and CRP types

Note 1 to entry: SBM, MSM and CRP types are defined in Annex A.

Note 2 to entry: This document defines different requirements to the transmission of different message types.

3.14
multi-sentence message
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 to entry: Multi-sentence messages that are grouped together with a TAG construct are also a sentence group.

Note 2 to entry: MSM are defined in Annex A.

3.15
network
physical Ethernet network with one Internet address space, consisting only of the network nodes, switches, cables and supporting equipment such as power supply units

3.16
network function block
NF
function block responsible for physical connectivity to the network and connectivity to the transport layer as described in 4.3

3.17
network infrastructure
part of the network that provides a transmission path between network nodes

Note 1 to entry: The network nodes are not part of the network infrastructure.

3.18
network node
physical device connected to the network and which have an Internet address

Note 1 to entry: A network node is also called an "Internet host".

Note 2 to entry: A network node will normally correspond to equipment. "Equipment" is used in this document.

3.19
other network function block
ONF
function block that interfaces to the network, but which is not using the protocol definition in Clause 5, Clause 6 and Clause 7

EXAMPLE Real time streaming of radar and CCTV image transfer, or VDR sound transfer.

Note 1 to entry: Requirements as defined in 4.7 ensure that an ONF can co-reside with SF network nodes and function blocks that make use of this document's protocol.

3.20
PGN to network gateway function block
PNGF
function block that enables transfer of sentences between the network and devices that are compliant with the IEC 61162-3 serial data instrument network interface

3.21
PGN message
parameter group number message
message consisting of an 8-bit or 16-bit number that identifies each parameter group

Note 1 to entry: The parameter group number (PGN) is analogous to the three-character sentence formatter in IEC 61162-1. By definition, parameter groups identified by 16-bit parameter group numbers are broadcast to all addresses on the network. Parameter groups identified by 8-bit parameter group numbers may be used to direct data for use by a specific address.

[SOURCE: IEC 61162-3:2008, 3.1.21, modified – The word "message" has been added to the term, and the definition has been rephrased.]

3.22
sensor broadcast message
SBM
message consisting of only one sentence

Note 1 to entry: SBMs 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 to entry: SBMs are defined in Annex A.

3.23
sentence
standard information carrying unit as described in IEC 61162-1

3.24
sentence group
logical group of sentences that need to be processed together to give full meaning to the information contained in the sentence(s)

Note 1 to entry: A sentence group may consist of only one sentence.

Note 2 to entry: The grouping of sentences into sentence group is done by TAG block mechanisms.

Note 3 to entry: This document allows the explicit grouping of sentences by using coding in a datagram. This document 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.

3.25
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

Note 1 to entry: One SNGF may contain several system function blocks which each have their own SFI. Furthermore, the SNGF itself has an SFI for administrative purposes.

3.26
system function block
SF
function block, identified by a unique system function ID (SFI), which is the only function block that can send information in a datagram format as defined in Clause 7

3.27
system function ID
SFI
parameter string as defined in 4.4.2

3.28
transmission group
pair of a multicast address and a port number that are used by an SF to transmit sentences

Note 1 to entry: The transmission groups are defined in Table 4, and Annex A defines default transmission groups for the SF.

3.29
transport annotate and group
TAG
formatted block of data, defined in NMEA 0183, which adds parameters to IEC 61162-1 sentences

Note 1 to entry: Annex B gives an overview of the TAG blocks used in this document.

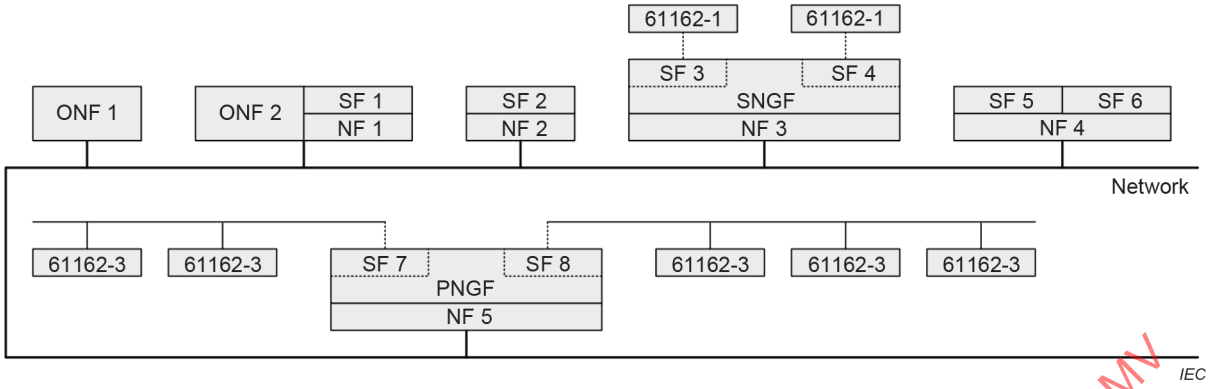
3.30
user datagram protocol
UDP
connection-less datagram protocol defined by ISOC RFC 768

Note 1 to entry: ISOC RFC 768 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 Clause 4.



Key

SF	system function block
NF	network function block
SNGF	serial to network gateway function block
ONF	other network function block
PNGF	PGN to network gateway function block

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 file) 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 document (SF3, SF4, SNGF and NF3);
- a system device function block presented by an IEC 61162-3 compliant equipment connected to network gateway function (PNGF); in this case, the PNGF will format outgoing sentences according to requirements of this document (SF7, SF8, PNGF and NF5);
- a device that does not send or receive IEC 61162-450 compliant data (sentences and/or binary file), 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), 4.5 (SNGF) and 4.6 (PNGF).
- 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 4.7.
- 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.

  NOTE This requirement applies only to devices on the network when the network is in normal operation. During commissioning or maintenance, when the system is not being used for safety-related navigation, other equipment can be temporarily connected to the network that does not comply with 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)

To avoid potential problems with certain network infrastructure equipment, repeater hubs shall not be used to interconnect components of an IEC 61162-450 network.

NOTE 1 Repeater hubs are network infrastructure devices without internal storage that repeat incoming datagrams onto all outgoing connections.

NOTE 2 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.

Switches used in an IEC 61162-450 network shall have means to filter network traffic using IGMP snooping. When the IGMP snooping is enabled and when a multicast datagram is received, the switch shall forward it only to the ports which have joined the same multicast group. The means which shall be provided to support multicast data filtering using IGMP snooping are the following:

- IGMP snooping shall be provided based on IGMPv1, IGMPv2 or IGMPv3; the selection of the IGMP version shall be based on highest version supported by all the connected nodes;
- multicast traffic filtering shall be provided based on IP multicast address;
- multicast data filtering shall not be enabled for the address range of 224.0.0.1 to 224.0.0.255 as recommended in RFC 4541.

In addition to or instead of multicast filtering techniques, such as IGMP snooping, it is also permitted to configure manually individual ports of the switches to block unnecessary traffic flow (for example to isolate simple sensors from ECDIS and radar).

See Annex D for IGMP snooping compatibility issues of nodes based on IEC 61162-450:2011[1].

Another possible method to filter and control network traffic is described in Annex E.

4.3 Network function (NF) requirements

4.3.1 General requirements

All equipment that implements a NF shall satisfy the requirements in Clause 5 and Clause 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 except for the equipment applicable standards or functions otherwise specified by the manufacturer.

1 This publication has been withdrawn.

Maximum input rate shall be specified as:

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

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

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

NOTE 1 "Received by" means datagrams that are received on all transmission groups that the equipment listens to.

NOTE 2 "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, for example by trained service engineer. It is allowed that the inspection is done through a simple network mechanism, such as a terminal emulator, as defined in this document 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 document 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 document, 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 document.
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 h 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 document, 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.
Italicised words are place-holders for data explained in the right hand column.	

A "syslog" packet shall not exceed 480 bytes and shall be sent as a single UDP datagram. The "syslog" packet for multiple occurrences of same message identity shall not be reported more often than once per minute. The "syslog" packet for any occurrence of message identity shall not be delayed more than 10 min.

This document does not specify requirements for equipment receiving syslog messages. This type of equipment would fall into the category of ONF. As Table 1 is a subset of the full ISOC RFC 5424 specification, implementers of such equipment shall 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 document have been assigned a message identity as defined in Table 2.

Table 2 – Syslog error message codes

Message identity	Description	Subclause
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 file error	7.3.9
201	PNGF buffer overflow	4.6.2
202	PGN message errors	7.4.2 and 7.4.4
203	No available address for devices	7.4.3.2

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

4.3.4 Provisions for network traffic filtering – IGMP

NOTE The purpose of the IGMP for this document is to provide the possibility to perform network traffic filtering based on IGMP snooping.

The manufacturer shall specify the version of IGMP as defined in ISOC RFC 1112, RFC 2236 and RFC 3376 that the NF supports. At least version 1 as defined in ISOC RFC 1112 shall be implemented.

See Annex D for compatibility issues of nodes based on IEC 61162-450:2011.

4.4 System function block (SF) requirements

4.4.1 General requirements

(see 8.4.1 and 8.2.3)

Equipment that implements an SF shall satisfy the following requirements:

- requirements in 6.2 shall be satisfied for all equipment implementing SF;
- implements at least one of the datagram types defined in Clause 7, but does not have to implement all of them;
- implemented datagram types shall be specified in the manufacture's documentation (see 7.1.1);
- requirements in 7.2 shall be satisfied for all equipment implementing IEC 61162-1 sentence transmitting or receiving function blocks;
- requirements in 7.3 shall be satisfied for equipment that implements an SF that can transmit or receive binary file data;
- requirements in 7.4 shall be satisfied for all equipment implementing IEC 61162-3 PGN message transmitting or receiving function blocks.

4.4.2 Implementing configurable transmission groups

(see 8.4.3)

As default, each SF shall be assigned a single transmission group/multicast address 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 and the SFs which are assigned to them within the valid range of multicast addresses defined in 5.4. A system integrator may, for example, split an SF into different transmission groups to support optimal load balancing for a given system. Where non-default configurations of SF and transmission groups are utilised, the details should be documented by the system integrator.

4.4.3 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. If the talker mnemonic is proprietary (i.e. consists of character "P" followed by a three-character manufacturer's mnemonic code), then two first characters are used as the "cc" characters in the SFI.

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 shall be avoided.

The numeric character string "xxxx" will be an instance number in the range "0001" to "9999". The numeric character string "9999" is reserved for an unconfigured 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. For implementation of interface redundancy (i.e. a single device is available through multiple paths in the network), the SF and related SFI shall be the same. The combination of source parameter codes "s" shall be unique for each path (see 7.2.3.4).

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.

There may be multiple SF, each communication with their own SFI, assigned to a single IP address or MAC address.

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

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.

The SNGF may support one or more serial ports (see Figure 2).

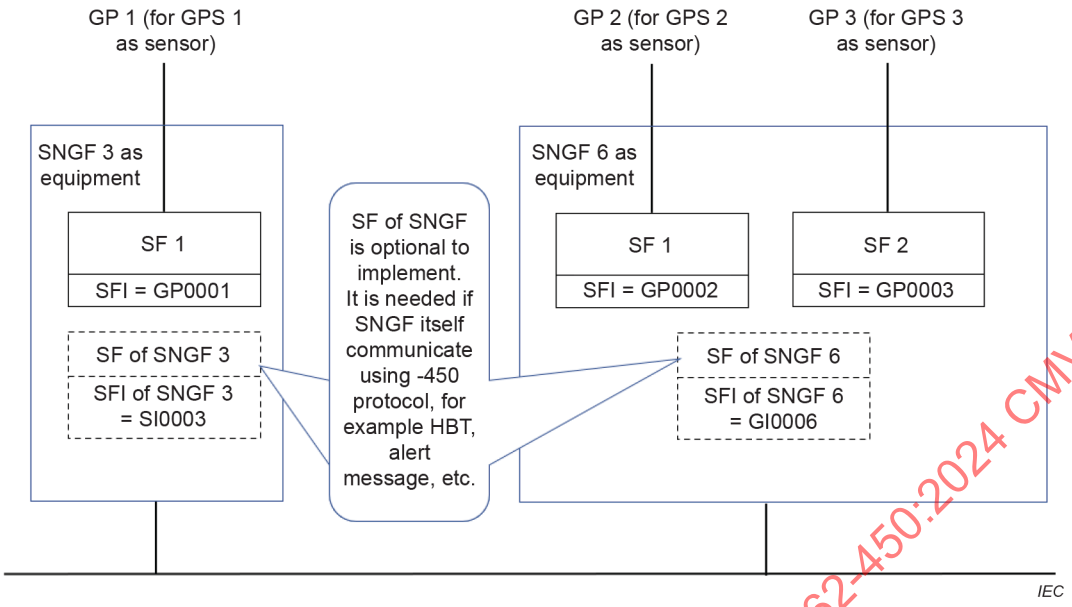


Figure 2 – SNGF examples

Each serial port shall be implemented as a separate SF and assigned a separate SFI, unless the SNGF implements multi-SF serial port (see 4.5.4 and Figure 3) or the SNGF implements interface redundancy. If practical, the "cc" part of the SFI shall be based on the talker identifier in use by the serial port; otherwise, an appropriate Talker Identifier shall be used.

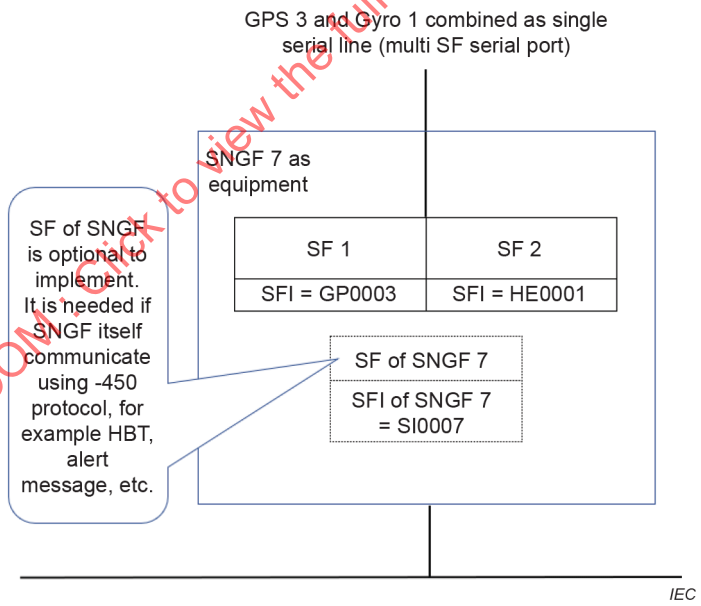


Figure 3 – SNGF example, multi SF serial port

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 the installation manual.

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

All sentences, including those with unidentified or illegal content, as well as proprietary sentences shall be transmitted, unless subject to filtering, from the SF associated with the serial port. Sentences with unidentified or illegal content shall be sent with a legal transport annotate and group (TAG) block as defined in 7.2.3, but with the raw received serial data following the TAG block.

As a destination, each serial port shall be associated with the corresponding SFI. Outgoing sentences shall be transmitted exactly as received in the datagram.

The SNGF may support one or more sources distinguished by different talker mnemonics at each serial port. Each source in a shared serial port shall be implemented as a separate SF and assigned a separate SFI. If practical, the "cc" part of the SFI shall be based on the talker mnemonic in use by each source in a shared serial port. As a destination, each source in a shared serial port shall be based on the SFI. Proprietary sentences include no talker identifier and, based on setup parameters, they shall use the same SFI as standardized sentences from the same source. The STN sentence is an additional qualifier for the following sentence. The STN sentence and the following sentence belong to the same SF and shall use the same SFI.

Proprietary sentences received from serial port shall be associated with the SF of the serial port based on

- talker mnemonic used by non-proprietary sentences (see above paragraph), or
- the SF determined by the preceding STN sentence, or
- optionally, the SF set by the configuration for the serial port.

Malformed sentences (see 4.5.5) received from a serial port shall be associated with the SF either

- of the talker mnemonics, if available, of the malformed sentence, or
- of the talker mnemonic used by non-malformed sentences for the serial port, or
- set by the configuration for the malformed sentences.

The manufacturer shall declare in the installation manual which alternatives have been used for association with the SF for malformed sentences.

The TAG block for source identification "s" shall be based on the SFI. If available, routing from a network to serial ports shall be based on the TAG block for destination identification "d".

The SFI of a SNGF used for administrative purposes, such as syslog, heartbeat (HBT) of SNGF itself, etc., shall use the talker mnemonic "SI".

4.5.2 Serial line output buffer management

(see 8.5.2)

An SNGF function block shall provide an independent buffer for each separate SF implemented 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. Exception is a multi-sentence message or a TAG block group of sentences: they shall only be replaced in their entirety.

  NOTE When prioritizing AIS VDM and VDO sentences, the string beginning with the "!" character and ending with the 7th character of the encapsulation field is 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 single sentence, multi sentence message 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 or sentences at its position in the queue. This replacing shall not cause logging of an error nor sending anything to syslog.

  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 either transmit one IEC 61162-1 sentence or, if part of a multi sentence sequence, may transmit multiple IEC 61162-1 sentences per outgoing IEC 61162-450 datagram. The multi sentence sequence includes the case described in IEC 61162-1 Multi-sentence messages, and the cases for which IEC 61162-1 requires a sentence sent prior sending another sentence. The datagram shall include the correct SFI, source identification (s:) and, if required, destination identification (d:).

4.5.4 Multi SF serial port

(see 8.5.4)

The SNGF is allowed to implement more than one SFs for any single serial line. Received sentences on this serial line with a valid talker mnemonic will be transmitted from one of the associated SFs dependent on the talker mnemonics. Each SF shall be assigned a separate SFI and, as a destination, transmit outgoing sentences on the serial line according to the rules in 4.5.1.

Proprietary sentences received on the serial line include no talker identifier. It shall be determined by setup parameters from what SF they shall be transmitted.

Unidentified data from the serial line shall be sent from all SFs associated with the serial port. This sending of unidentified data shall not cause logging of an error nor sending anything to syslog.

4.5.5 Handling malformed data received on serial line

(see 8.5.5)

The SNGF is intended as a remote serial data converter with minimum data processing. For each of the cases below, the SNGF shall send a datagram with the malformed data as required by 4.5.1 and 4.5.4. If the formatted message exceeds the maximum datagram length (see 6.2.4), the data shall be truncated from the end. The following cases shall cause a message containing the malformed data to be sent:

1) if data has been received before a start character;
2) if data has been received after a valid start character and the maximum sentence and TAG block length has been exceeded;
3) if data has been received after a valid start character and end of line (CR,LF) has not been received after 1 s;
4) if a reserved character has been received and not having been appropriately escaped;
5) if random binary data is received on the serial line.

"Start character" is a valid start of sentence ("$", "!") or TAG block start character.

4.6 PGN to network gateway function (PNGF) requirements

(see 8.12)

4.6.1 General requirements

(see 8.12)

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

The SFI of a PNGF used for administrative purposes, such as syslog, heartbeat (HBT) of PNGF itself, etc., shall use the talker mnemonic "SI".

The PNGF may implement different types of filtering based on the PGN messages from and to IEC 61162-3 network. Any filtering methods shall be described in the manufacturer's documentation.

NOTE The accurate timing between PGN messages available in the IEC 61162-3 network is not supported when the same is converted into IEC 61162-450 network.

4.6.2 Output buffer management from IEC 61162-450 network to IEC 61162-3 network

(see 8.12)

A PNGF function block shall provide an independent buffer for each IEC 61162-3 network it can send into. The manufacturer shall specify the maximum buffer capacity for each port. The maximum capacity may be configurable at installation.

PNGF buffer management shall be based on the IEC 61162-3 priority included into each message. The manufacturer shall describe the method in documentation.

If the buffer is full and a PGN message is discarded, it shall be recorded as specified in 4.3.3.

4.6.3 Datagram output requirements

(see 8.12)

The PNGF shall format outgoing messages as defined in 7.4.1.

The PNGF shall transmit one IEC 61162-3 PGN message per outgoing IEC 61162-450 datagram to minimise delays.

4.6.4 PGN group number

(see 8.12)

A PGN group is defined as a logical group of devices that can share the information and message. A message from a device is broadcasted to all devices that belong to the same PGN group. A device may belong to more than one PGN groups. The maximum number of PGN groups is no more than four. The PGN group may be used for filtering of messages (see 4.6.1).

4.7 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 document 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 describing the impact of the ONF 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.

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

The physical layer requirement for IEC 61162-3 ports of the PNGF shall be compliant with IEC 61162-3:2008, Clause 4.

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-TX IEEE Std 802.3-2022 Clauses 24 and 25	100 m	IEC 60603-7-3, 8-way shielded modular connector Refer to IEC 60603-7:2020, Figures 1 through 5, and IEEE Std 802.3:2022, Clause 25	[b]	CAT5 STP Two shielded twisted pairs ANSI/TIA-568-A, ANSI/TIA-568-B or ISO/IEC 11801 (class D).
(not specified)	[a]	Terminal block	[b]	CAT5 STP Two shielded twisted pairs
100BASE-SX IEEE Std 802.3-2022, 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 Std 802.3:2022, Clause 40	100 m	IEC 60603-7-7, 8-way shielded modular connector Refer to IEC 60603-7:2020, Figures 1 through 5.	[c]	CAT5 STP Four shielded twisted pairs ANSI/TIA-568-A, ANSI/TIA-568-B or ISO/IEC 11801 (Class D).
1000BASE-SX IEEE Std 802.3-2022, Clause 38	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 for copper network cable. And similar rugged connector should be considered for external fibre optic connections.				

[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 8 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 Std 802.3-2022, 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 8 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 Std 802.3-2022, 40.8.1, and IEC 60603-7-7.

[d] See TIA-604-10.

5.2 Network protocol requirements

(see 8.7.2)

Equipment shall implement IPv4 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;

The following protocols may be supported depending upon the requirements of the equipment:

- UDP – User datagram Protocol as described in ISOC RFC 768;

  NOTE 1 For equipment that is purely an ONF (neither SF nor SNGF), this is not necessarily required. Such an ONF device can communicate only over TCP or only over UDP, or perhaps even with raw IP or ICMP packets.

- UDP Multicast – Host groups as described in ISOC RFC 966 and Host extensions as described in ISOC RFC 1112;

  NOTE 2 For equipment that is purely an ONF (neither SF nor SNGF), this is not necessarily required. Such an ONF device can communicate only over TCP or only over UDP, or perhaps even with raw IP or ICMP packets.

- TCP – Transmission Control Protocol as described in ISOC RFC 793;

  NOTE 3 TCP is generally not required for SF and SNGF functions. Whilst it can make sense for some equipment to support TCP, this document does not require TCP to be used.

- ICMP – Internet Control Message Protocol as described in ISOC RFC 792;

  NOTE 4 There is no requirement in this document relating to ICMP.

- IGMP – Internet Group Management Protocol as described in ISOC RFC 1112, RFC 2236 or RFC 3376;

  NOTE 5 It is sensible to support IGMP snooping particularly for SF and SNGF devices, but it is not strictly required within this document. See D.2.1.

5.3 IP address assignment for equipment

(see 8.7.3)

Means shall be provided to configure the equipment to any of the addresses reserved for use in private networks as described in ISOC RFC 1918 with any valid network address mask. The default sub-net mask shall be set appropriately for 192.168.0.0/24 (legacy class C). The assigned IP address shall remain fixed during normal operation of the equipment, including powering the equipment down and up.

A 450-Node may reserve sub-nets for non-450 use, for example, for internal use (internal to the equipment) or for other interfaces. All reserved sub-nets shall be documented. The following sub-nets shall always be available to the IEC 61162-450 network: 192.168.0.0/24 – 192.168.10.0/24 and 172.16.0.0/16 (class B).

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).

The multicast address range 239.192.0.57 to 239.192.0.64 is used for interconnection with IEC 61162-3 networks.

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

NOTE 1 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 allocates sub-ranges when defining scopes for private use.

NOTE 2 The multicast time to live (TTL i.e. number of hops) is adaptable to allow transmission over multiple network routers. The default TTL value is 64. The sub-net mask is set appropriately for a class C (local area network).

5.5 Device address for instrument networks

Means shall be provided to assign a device address range from 0 to 251 when the PNGF transmits to an IEC 61162-3 network. The device address may be set automatically.

6 Transport layer specification

(see 8.8)

6.1 General

Clause 6 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 of Clause 6 applies to both, but shall be tested independently as described in 7.6.

An example of the structure of an Ethernet frame with a IEC 61162-450 sentence is given in Figure 4. 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).

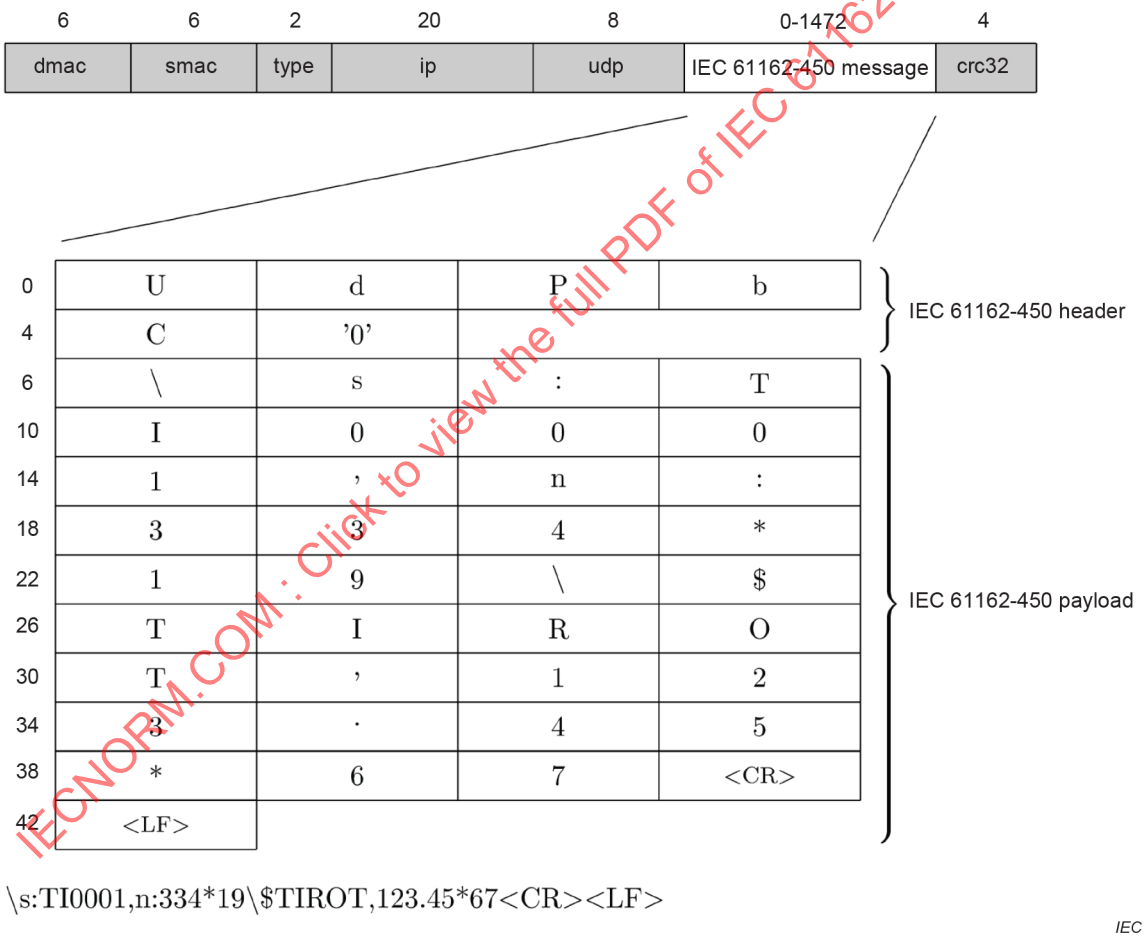


Figure 4 – Ethernet frame example for a SBM from a rate of turn sensor

6.2 UDP messages

6.2.1 UDP multicast protocol

UDP Multicast – IP multicast is a technique for many-to-many communication over an IP infrastructure in a network. The destination nodes send join and may send leave messages. IP multicast scales to a larger receiver population by not requiring prior knowledge of who or how many receivers there are. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers only when necessary. The most common transport layer protocol to use multicast addressing is User Datagram Protocol (UDP).

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

6.2.2 Use of multicast addresses and port numbers

Port numbers shall be allocated from the dynamic port range that the internet assigned number authority (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. If provided by the equipment, the default transmission group can be changed by the parameter setup system of the equipment to any transmission group in Table 4 or any in Table 5 (for example to support use of same transmission group for both "binary file" and related sentences, for example ECDIS route exchange and RRT-sentence).

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 61996-1	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	User defined transmission group 1	239.192.0.9	60009
USR2	User defined transmission group 2	239.192.0.10	60010
USR3	User defined transmission group 3	239.192.0.11	60011
USR4	User defined transmission group 4	239.192.0.12	60012
USR5	User defined transmission group 5	239.192.0.13	60013
USR6	User defined transmission group 6	239.192.0.14	60014
USR7	User defined transmission group 7	239.192.0.15	60015
USR8	User defined transmission group 8	239.192.0.16	60016
BAM1	BAM compliant alert source reporting to CAM group 1	239.192.0.17	60017

Transmission group	Category	Multicast address	Destination port
BAM2	BAM compliant alert source reporting to CAM group 2	239.192.0.18	60018
CAM1	CAM of the BAM group 1	239.192.0.19	60019
CAM2	CAM of the BAM group 2	239.192.0.20	60020
NETA	Network administration, e.g. SFI collision detection	239.192.0.56	60056
PGP1	PGN Group 1	239.192.0.57	60057
PGP2	PGN Group 2	239.192.0.58	60058
PGP3	PGN Group 3	239.192.0.59	60059
PGP4	PGN Group 4	239.192.0.60	60060
PGB1	Backup PGN group 1	239.192.0.61	60061
PGB2	Backup PGN group 2	239.192.0.62	60062
PGB3	Backup PGN group 3	239.192.0.63	60063
PGB4	Backup PGN group 4	239.192.0.64	60064
NOTE 1 The USR1 to USR8 transmission groups can be used, for example, for proprietary data in binary format. NOTE 2 To balance the traffic or to provide backward compatibility, in addition to the implementation of mandatory use of BAM1/BAM2 and CAM1/CAM2, BAM related communication can be configured to use e.g. SATD or NAVD transmission groups.			

Table 5 defines multicast addresses and destination port numbers that shall be used when transmitting binary file data. If provided by the equipment, the default multicast address or destination port number can be changed by the parameter setup system of the equipment to the multicast addresses or destination port numbers of the transmission groups USR1 to USR8, RCOM, PROP in Table 4 or any in Table 5 (for example to support use of same transmission group for both "binary file" and related sentences).

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

Category	Multicast address	Destination port
Non re-transmittable binary file transfer group 1 [a]	239.192.0.21	60021
Non re-transmittable binary file transfer group 2 [a]	239.192.0.22	60022
Non re-transmittable binary file transfer group 3 [a]	239.192.0.23	60023
Non re-transmittable binary file transfer group 4 [a]	239.192.0.24	60024
Non re-transmittable binary file transfer group 5 [a]	239.192.0.25	60025
Re-transmittable binary file transfer group 1 [b]	239.192.0.26	60026
Re-transmittable binary file transfer group 2 [b]	239.192.0.27	60027
Re-transmittable binary file transfer group 3 [b]	239.192.0.28	60028
Re-transmittable binary file transfer group 4 [b]	239.192.0.29	60029
Re-transmittable binary file transfer group 5 [b]	239.192.0.30	60030
[a] Address 239.192.0.25, port 60025 is the default for ECDIS route transfer (see IEC 61174). [b] Address 239.192.0.26, port 60026 is the default for VDR image transfer (see IEC 61996-1). Address 239.192.0.30, port 60030 is the default for ECDIS re-transmittable data blocks for route transfer (see IEC 61174).		

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

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

Category	Multicast address	Destination port
Syslog	239.192.0.254	514
Sending to syslog can use multicast or UDP unicast. Some switches can support only UDP unicast.		

The addresses 239.192.0.31 to 239.192.0.55 are reserved for future expansion.

IANA has defined that port range 49152 to 65535 is reserved for dynamic and private use. The specific ports for this document are within this IANA range. Operating systems also use this IANA range for their internal use as ephemeral ports. This double use may cause port number conflicts resulting for lost communication of IEC 61162-450 messages. It is recommended to consider limiting the ephemeral port range of the operating system of equipment connected to an IEC 61162-450 network to avoid port number conflicts.

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 kB 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 datagrams 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 files as described in 7.3;
- "`RrUdP`" for transmission of re-transmittable binary files as described in 7.3;
- "`NkPgN`" for transmission of IEC 61162-3 PGN messages as described in 7.4;

All TCP/IP datagrams shall contain the following string, followed by a null character (all bits set to zero) as the first six bytes of the datagram:

- "`RrTcP`" for transmission of binary files as described in 7.6.

NOTE 1 Datagram means packet in this context.

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

NOTE 2 Future editions of IEC 61162-450 can 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 Annex B, containing one or more of the parameter codes described in 7.2.3.3 to 7.2.3.8. Adding of TAG blocks with parameter codes happens after the last existing TAG block.

An example of applying one and more parameter code "s" is as follows.

Original source = GP0001

```
\s:GP0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\\s:TT0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A
*27<CR><LF>
```

If a parameter code is assigned a value more than once in all TAG blocks and only one value is expected, the parameter code value closest to the start of the IEC 61162-1 sentence and IEC 61162-450 conformant (see 7.2.3.4) shall be used.

NOTE The IEC 61162-450 conformant parameter code "s" can be added by SNGF or ONF.

In case of multiple source parameter codes "s", the original source is the right most “s” parameter in the left most TAG block from the start of the IEC 61162-1 sentence and IEC 61162-450 conformant (see 7.2.3.4).

If a device modifies the content of a received IEC 61162-1 sentence, then the TAG blocks containing source parameter codes "s" shall be removed and replaced by a TAG block containing a source parameter code "s" based upon the SFI of the device which did the modification.

It is possible that a TAG block, or a group with two or more TAG blocks, may contain multiple destinations. Each listener is responsible for recognizing its own identifier, and each listener would treat the TAG block line (see Clause B.5) or group of TAG block lines as addressed to that unit.

- First example

  Two valid datagrams are shown below. The second datagram shows two occurrences of parameter code "s", where the first occurrence (AC1000) is the original source and the second occurrence closest to the sentence (BC1000) identifies the device that this sentence passed through.

  ```
  \d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,
  0*7C

  \s:AC1000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,
  3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
  ```

- Second example

  The datagram below shows the case when one parameter code "s" (002300000) is from a non IEC 61162-450 conformant source. A receiver can use or ignore this non IEC 61162-450 conformant source. Note that parameter code "s" (BC1000) closest to the sentence is IEC 61162-450 conformant.

  ```
  \s:002300000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,
  ,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
  ```

For compliance with this document, all TAG block parameter codes are set at the time of installation and shall not be dynamically configurable during normal operation.

NOTE The control sentences for changing parameter codes in NMEA 0183 are not 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.

A TAG block may contain parameter codes and their values known and/or not known by the receiver. Further there may be multiple occurrences of a parameter code. The examples below assist in correct interpretation.

If the value of the "s" parameter code is not understood by the receiver, for example not encoded as in this document (see 7.2.3.4), then the message shall be ignored, for example:

```
\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
```

If the "s" parameter code is available twice, the first instance encoded as in this document (see 7.2.3.4) and the second instance not understood by the receiver, then the message shall be accepted based on the parameter code understood by the receiver and the existence of the not understood parameter code is ignored, for example

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R
=23BTB3F00Uh,0*7C
```

NOTE The above example could be the result of a node adding its TAG block in front of existing TAG blocks instead of in front of the start of the sentence (see 7.3.2.1).

When the "s" parameter code is available twice, only the closest to the start of the IEC 61162-1 sentence is used (in the example below s:AI0001) and the other is ignored, for example.

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:AI0001*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23
BTB3F00Uh,0*7C
```

If the message contains known (for instance "s") and unknown parameter codes (for instance "c" defined in this document, but not implemented by the receiver), then the message shall be accepted and the unknown parameter code shall be ignored, for example:

```
\s:BC1000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
```

If all parameter codes are unknown for the receiver (for instance "h" is not defined in this standard and "c" is not implemented by the receiver), then the message shall be ignored, for example:

```
\h:002300000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*
37
```

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.

NOTE An example of optional use is to associate or link related sentences together, for example GGA and VTG sentences from a GNSS receiver could be grouped together.

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

A valid MSM type sentence where internal data fields specify 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 value of the "g" parameter code is divided into three fields. The fields within the "g" parameters are separated using "-".as delimiter. The uses 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. This is used to differentiate between different groups of TAG blocks and sentences.

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 99 is used, hence the valid range is 1 to 99, inclusive. The receiver shall make no assumption about the initial value of the group code.

When used, the "g" parameter code shall be the first parameter code in the TAG block.

All grouped sentence of type MSM of a message shall be included in the same group of linked lines, but the group of linked lines may include also other than the MSM type sentences.

It is recommended that grouped sentences are sent in as few datagrams as possible to minimise the probability of out of order packets being received.

Below is an example of compliant use. In this example, four VDM sentences are grouped (first 2 are individual and last 2 are part of MSM).

```
\g:1-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
\g:2-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
\g:3-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\g:4-4-45*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

Below is an example of non-compliant use of grouping. In this example, the grouping of the first three lines does not include the second part of the MSM message.

```
\g:1-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F 00Uh,0*7C
\g:2-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD 8@Ip,0*37
\g:3-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\d:AB0001, d:AB0002,s:BC1000*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

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,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-46,s:IN0001*3F\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D
\g:2-2-46,s:IN0001*3C\$ABVSI,r3669962,1,013538.05654921,1427,101,,*20
```

Additional requirements for use of "g" parameter code are:

1) all grouped TAG block lines shall be sent in increasing sequence as indicated by the first numeric value in the “g” parameter code;
2) grouped TAG block lines shall not be sent with more than one second delay between each TAG block line.

Receivers may ignore the complete group if the above two requirements are not met.

An example of non-compliant use of the first requirement is a variant of the previous example with an incorrect sequence (two lines are sent in the wrong order):

```
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-34,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
```

7.2.3.4 Source identification – s

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

Received messages without any known "s" parameter code shall be ignored.

Multiple "s" parameter codes may be used to indicate the path a message takes. The first or right-most “s” parameter code is the SFI of the device which creates the message. Subsequent equipment SFIs for source parameter codes may be added to the left to indicate the path the message takes.

For example, a SNGF may add its SFI as a source parameter to a message to indicate that the message originates from a particular SNGF, see Figure 2 and Figure 3 for an example for the configuration of sensor SFI and SNGF SFI.

7.2.3.5 Destination identification – d

The "d" parameter code shall be provided for CRP type sentences and optional for other types and shall, if used, contain the system function ID (SFI, see 4.4.2) corresponding to the intended recipient of the sentence.

If no destination parameter code is present, then all devices that receive this sentence shall process it.

Multiple "d" parameter codes may be specified, if more than one intended recipient exists. All "d" parameter codes in a TAG block group apply collectively to all sentences associated with the TAG block group. Listed recipients shall process and react on the content of the associated sentences.

NOTE This can be the case for redundant control functions. Other receivers also read the message, for example for voyage data recording purposes, but are not intended to take any further action on the contents.

If there is a need to specify more "d" parameter codes than can fit into a single TAG block, the list of "d" parameter codes shall be divided over more than one TAG block. If these TAG blocks are in the same TAG block line, there is no need to link them using the "g" parameter code. For example, two TAG blocks, one with 7 and another with 2 "d" parameter codes:

```
\s:IN0001,d:AB0001,d:AB0002,d:AB0003,d:AB0004,d:AB0005,d:AB0006,d:AB0007*hh\\
d:AB0008,d:AB0009*hh\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
```

7.2.3.6 Line count parameter – n

(see 8.9.4.1)

The "n" parameter code may be used to assign a sequence number to selected sentences 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 the selected sentences transmitted from this system function block. The parameter value shall be reset to one ("1") after 999 is used, hence the valid range is 1 to 999, inclusive.

EXAMPLE 1 A GPS receiver sends its sentences to everybody. Selected sentences, all sentence or a sub-set of sent sentences, can be supported by a single line counter.

EXAMPLE 2 An equipment implements ECDIS and track control. Selected sentences sent from the track control function to the autopilot can be supported by a line counter. All other sentences sent by the equipment are without the line count parameter code.

EXAMPLE 3 A central display dimming controller sends DDC sentences separately for multiple monitors. Each monitor is identified using the d parameter code. Each flow of DDC sentences can be supported by separate line counters.

7.2.3.7 Text string parameter – t (proprietary data)

The "t" parameter code is a free text field. This document 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,s:TI0001,n:334,t:pmmma;MD5;0x12345678*0D\
```

7.2.3.8 General authentication – a

(see 8.9.5)

The authentication parameter code is used to sign a message with a password. Just sending a password with the message would reveal the password to anyone listening to the traffic. Sending a signature digest instead keeps the password secret.

Any kind of messages may be signed using the authentication parameter code. The authentication parameter code does not change the original message in any way. It is always possible to ignore this TAG and use the rest of the message.

EXAMPLE Sign configuration commands for devices or commands to the autopilot.

The authentication parameter code provides a standardized mechanism for passing the digest with the message. Password management is outside of the scope of this document. One way is to use pre-shared keys (PSK) on the participating devices.

NOTE 1 The pre-shared key could be 32 alphanumeric characters, for example "Alea iacta est 1234567890".

This parameter code is optional and should only be used where special safety concerns make it useful. If this TAG is provided, then the manufacturer's documentation shall describe which of the optional types of methods available to calculate a signature are supported by the equipment and shall describe how to share keys.

The format of the TAG block is:

\a:c-h--h*hh\

in which

c is the type of optional method to calculate signature

1) MD5,

2) SHA-256, and

P) proprietary;

h-h is the hexadecimal representation of the signature, for example 32 hexacodes for MD5.

An example of the TAG block is:

\a:1-123456789abcdef67890123456789012*hh\

Types of methods to calculate signature are as follows.

1) MD5

The signature is a MD5 digest of the password plus the message. MD5 is a one-way message-digest algorithm (RFC 1321). The full length of the signature is 128 bits or 32 hexadecimal codes. The MD5 is commonly used for storing passwords in Unix-systems. Revealing the digest does not expose the password.

NOTE 2 See http://tools.ietf.org/html/rfc1321 and http://en.wikipedia.org/wiki/MD5.

The security provided in 2023 by MD5 is weak. For new design, the SHA-256 is recommended.

2) SHA-256

The signature is a SHA-256 digest of the password plus the message. The full length of the signature is 256 bits or 64 hexadecimal codes. Revealing the digest does not expose the password.

P) Proprietary

The signature is a proprietary digest of the password plus the message. This alternative requires that both parties use the same manufacturer specified proprietary method.

The authentication parameter code value is calculated by concatenating a pre-shared key and all TAG blocks and sentences in the message as a single string to be used by the method of the signature calculation to produce the signature digest. "Carriage returns" and "line feeds" from the sentences are not included into the input string.

When the authentication parameter code "a" is used, it shall be in its own authentication TAG block, with no other parameter codes. For a grouped message consisting of several lines of TAG blocks and sentences, the authentication TAG block shall be placed on the first line of the group. Within the first line, the authentication TAG block shall be placed as the last TAG block, and before any sentence on that line. This also applies to a single line TAG block and sentence with no grouping.

An example of use of authentication TAG block:

Message consisting of two grouped sentences to be protected by authentication:

\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Pre-shared key to be used for signature calculation:

Alea iacta est 1234567890

Resulting input string for signature calculation:

Alea iacta est 1234567890\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Message to be sent including signature, method MD5:

\g:1-2-23,s:IN0001*3C\\a:2-851E40CC1CB7E3B39D961D7CF10BD8D3*44\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Messages without authentication parameter codes are accepted unless the set-up parameters of the receiver are explicitly set to require authentication on incoming packets.

If the device is set to require authentication on incoming packets, then packets without valid authentication shall be dropped.

NOTE 3 SNGF are advised to avoid transmitting passwords in the clear from SPW sentences received over a serial connection.

7.2.3.9 Destination cluster identification – x

(see 8.9.4.1 and 8.9.4.2)

The parameter code "x" is optional unless required by an equipment standard (e.g. BAM related communication). See Annex H for cluster identifiers.

7.2.3.10 Source cluster identification – z

(see 8.9.4.1)

The parameter code "z" is optional unless required by an equipment standard. See Annex H for cluster identifiers.

7.2.4 Requirements for processing incoming datagrams

For datagrams intended for processing by the SF, any syntax error in a TAG block or in a sentence shall make the receiving equipment discard the complete datagram without any other further processing than specified in 7.2.5. The exception is a SNGF which may retransmit the faulty sentences to the appropriate serial port, if it can be determined from a valid destination field, or to all connected serial ports, if no destination field is specified.

7.2.5 Error logging for processing incoming datagrams

(see 8.10)

The equipment shall maintain counts of errors detected in processing datagrams containing IEC 61162-1 sentences. 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 7.2.3.9.

7.3 Binary file transfer using UDP multicast – Single transmitter, multiple receivers

(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 as files, can be transmitted to one or more receivers. This protocol supports the transmission of files from zero bytes up to 4 billion files blocks.

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

- non re-transmittable transfers where sender sends the complete binary file without any feed-back from receiver;
- re-transmittable transfers where limited feed-back from one receiver identified by DestID can be used to re-transmit certain parts of the binary file while other parallel receivers operate as passive receive-only receivers of the binary file.

NOTE The advantage of non-re-transmittable and re-transmittable binary file transfer methods over the TCP/IP is the possibility of multiple parallel receivers of the same transmission.

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 until 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.
WORD	One unsigned 16-bit integer (in range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTES, 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/IEC 8859-1 (ISO Latin 1).

7.3.2 Binary file structure

7.3.2.1 General

The binary files are transmitted over the network in one or more datagrams. The binary file structure is a sequential and unpadded stream of bytes divided into three main groups: header, binary file descriptor and binary file data (see Table 8 and Table 9). The header is needed for synchronisation and data integrity validation. The binary file descriptor is needed for the description of the binary file data and is only used in the first datagram for each binary file transfer.

7.3.2.2 Non re-transmittable and re-transmittable transfers

Table 8 – Binary file structure

61162-450 header (see 7.3.3)
Binary file descriptor (only in first datagram) (see 7.3.4)
Binary file data fragment (see 7.3.5)
61162-450 header (zero or more)
Binary file data fragment (zero or more)

A minimum binary file transmission using non re-transmittable or re-transmittable transfer will consist of the three first blocks where the binary file fragment may have zero length.

The header shall be repeated as the first element of any datagram that contains binary file data fragments.

7.3.3 61162-450 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 binary file transfers, and how much data loss occurs. In addition, the header is used to provide a re-transmission mechanism for re-transmittable binary file transfer.

The 61162-450 header format is defined in Table 9.

Table 9 – 61162-450 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 2 is defined in this document. Extensions and/or modified versions may update this value.
HeaderLength	WORD	Defines the length of the header in bytes. This is at least the length of the header. Future editions of IEC 61162-450 may append additional fields to this header as long as these additional fields are compatible with the definition of the header in this document. Receivers which are not aware of these additional fields shall ignore them.
SrcID	STRING[6]	Define the source system identifier in format "ccxxxx" (see 4.4.2).
DestID	STRING[6]	For re-transmittable, defines the destination system identifier in format "ccxxxx", for example "VR0001" for VDR (see 4.4.2). When Destid = "XXXXXX", then there is no assigned destination.
Type	WORD	Identifies the information in the header.
BlockID	DWORD	Binary file block identifier. The initial value is randomly generated within a range 0 to (2^{32} – 1 = 4294967295) and is incremented by 1 after a whole block is transmitted.
SequenceNum	DWORD	Defines the sequence number of the binary file 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 binary file data block. When SequenceNum is equal to MaxSequence, it means that this datagram is the last datagram of the data block. The MaxSequence is used only for DATA type message. For other messages (QUERY,ACK), this field shall be 0.
Device	BYTE	Data source (device) as binary value, 1 for equipment 1, 2 for 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

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

7.3.3.2 Use of header token

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

- "RaUdP" – Simple binary file transfer service with UDP Multicast;
- "RrUdP" – Re-transmittable binary file transfer service with UDP Multicast.

7.3.3.3 Version

Defines the header version. It shall be set to 2 for this document.

7.3.3.4 Destination identifier

For transmissions to one specific receiver, the field shall contain the destination SFI. The field shall be "XXXXXX" for no specific destination.

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 file data including file 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 a binary file sender sends a QUERY message if there is no ACK message for 1 s after a last datagram of the binary file 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 file is received without any error or when errors occurred during the binary file 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 Binary file block identifier

Block identifier is used to identify each binary file block. Since a binary file block is fragmented into several datagrams, the block identifier is used to assemble one or more datagrams into a binary file 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.

7.3.3.8 Identification of separate binary file transfer

Each single binary file transfer shall be identified by a unique combination of SrcID, Device, Channel and BlockID (see Table 9).

NOTE If a single SrcID has multiple needs to send binary files (e.g. ECDIS sending screen image, chart source information and route exchange), then each single binary file 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.

7.3.4 Binary file descriptor structure

The binary file descriptor format is defined in Table 10.

Table 10 – Binary file descriptor format

Data item	TYPE	Description
Length	DWORD	Defines the binary file descriptor length in bytes. This is at least the length of the header including the reserved bytes. Future editions of IEC 61162-450 may append additional fields to this file descriptor as long as these additional fields are compatible with the definition of the file descriptor in this document. Receivers which are not aware of these additional fields shall ignore them.
fileLength	DWORD	Defines the length of the full binary file 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.
AckDestPort	WORD	Port number to be used to acknowledge. Allowed port numbers are within the range from 60006, 60008 to 60016, 60021 to 60030 (see 7.3.8.9).
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.
StatusLength	WORD	The length of the "Status and information text" field in bytes.
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 file header contents as this is handled by the UDP layer. In this document, 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 ISOC RFC 4289.		

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 binary file 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
XML	xml	application/xml

7.3.5 Binary file data fragment

The package data format is defined in Table 12.

Table 12 – Binary file 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 binary file fragment is the length of the UDP datagram (as obtained from the UDP header) minus any headers that are inserted in front of the binary file fragment. All datagrams, except the first datagram of the binary file which requires two headers (Header + binary File Descriptor), carry only one header (Header).

The binary file 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 file transfer

7.3.6.1 Non re-transmittable sender process

The following steps are performed for the basic sending process (see Figure 5):

a) a sender process waits until it gets a binary file block;

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

c) a binary file descriptor is composed according to Table 10;

d) a binary file block is split into datagrams whose size is not more than 1 472 bytes and each datagram is put into the sending buffer;

e) get the first datagram of the binary file block;

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

g) compose a header including token, source ID, destination ID and maximum sequence number according Table 9;

h) send a datagram to the network;

i) if all datagrams of the binary file block are not transmitted, get the next datagram and go to step f);

j) otherwise, then go to step a).

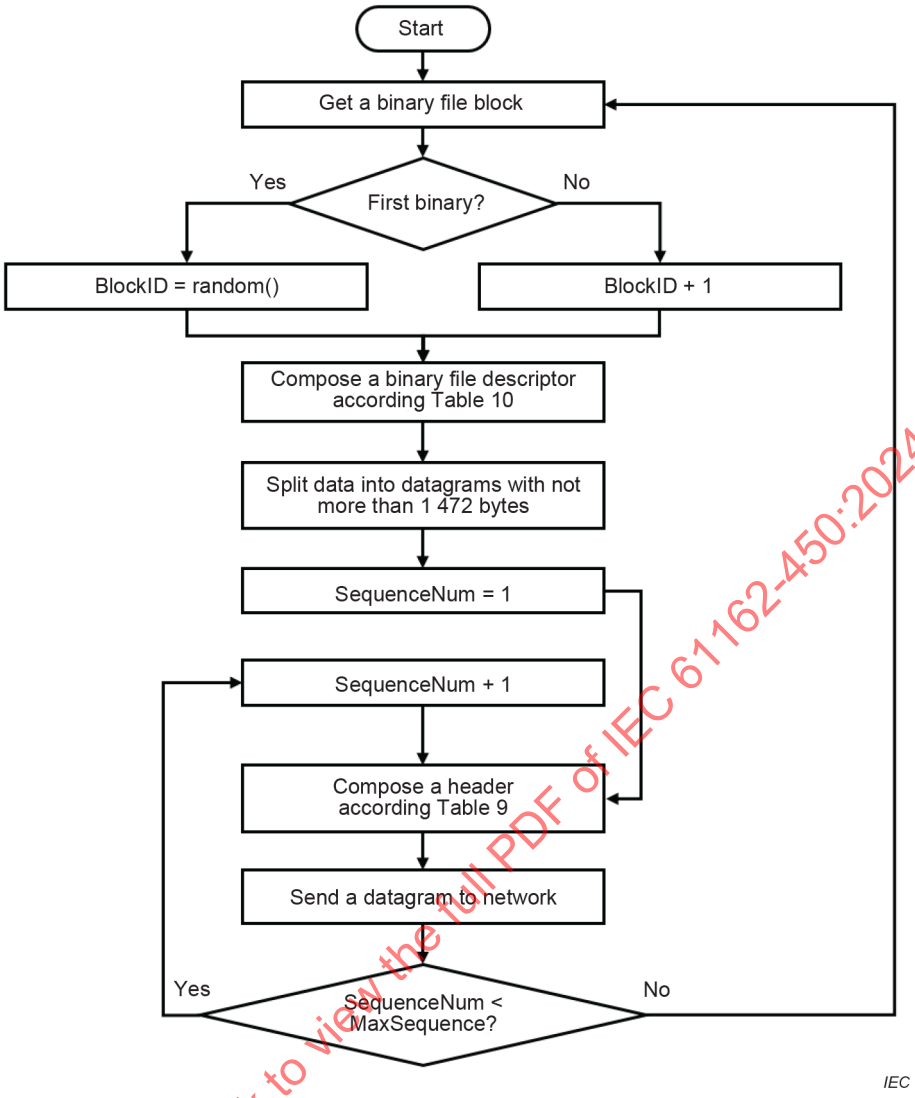


Figure 5 – Non re-transmittable sender process

7.3.6.2 Re-transmittable sender process

The sender processing steps for re-transmittable binary file transfer is as follows (see Figure 6):

a) a sender process waits until it gets a binary file block;

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

c) a binary file descriptor is composed according to Table 10;

d) set re-transmission counter to zero (0), set query counter to zero (0), set query sequence number to 1, set final counter to zero (0);

e) a binary file block is split into datagrams whose size is less than 1 472 bytes and each datagram is put into the sending buffer. Let the maximum number of retransmissions to be as defined in 7.3.8.7;

f) get the first datagram of the binary file;

g) assign a sequence number, which is set to one initially;

h) compose a header according Table 9;

i) send a datagram to the network and set an ACK timer to 500 ms;

j) if the sender receives an ACK message, whose DestID is not equal to own SFI and whose SourceID is not equal to own actual DestID, go to step k);

   1) if the sequence number of ACK message is less than the maximum sequence number and lower than the sequence number of the last transmitted datagram, increase re-transmission count by one;

   2) if re-transmission count is greater than the maximum number of retransmissions (see 7.3.8.7), go to step k);

   3) if sequence number in ACK message is identical to query sequence number, increase query counter with 1, and if query counter is more than 3, set query counter to zero (0) and go to k);

   4) if sequence number in ACK message is not identical to query sequence number, set query counter to 1;

   5) get a datagram whose sequence number is sequence number in ACK message plus one;

   6) set query sequence number to sequence number;

   7) go to step h);

k) if all datagrams of the binary file block have not been transmitted,

   1) get a next datagram and increase sequence number by one,

   2) go to step h);

l) otherwise, wait for an ACK message;

m) if the sender receives an ACK message whose DestID is not equal to own SFI and whose SourceID is not equal to own actual DestID , then go to step (n);

   1) if the sequence number of the ACK message is less than the maximum sequence number, then go to step j);

   2) if the sequence number of the ACK message is equal to the maximum sequence number (i.e. transfer successful), then go to step a);

n) if ACK Timer expires and final counter is not more than three, then

   1) increase the final counter,

   2) compose a QUERY datagram and send it to the network,

   3) set an ACK timer to 500 ms,

   4) go to step l);

o) transfer not successful;

   1) clear the sending buffer,

   2) go to step a).

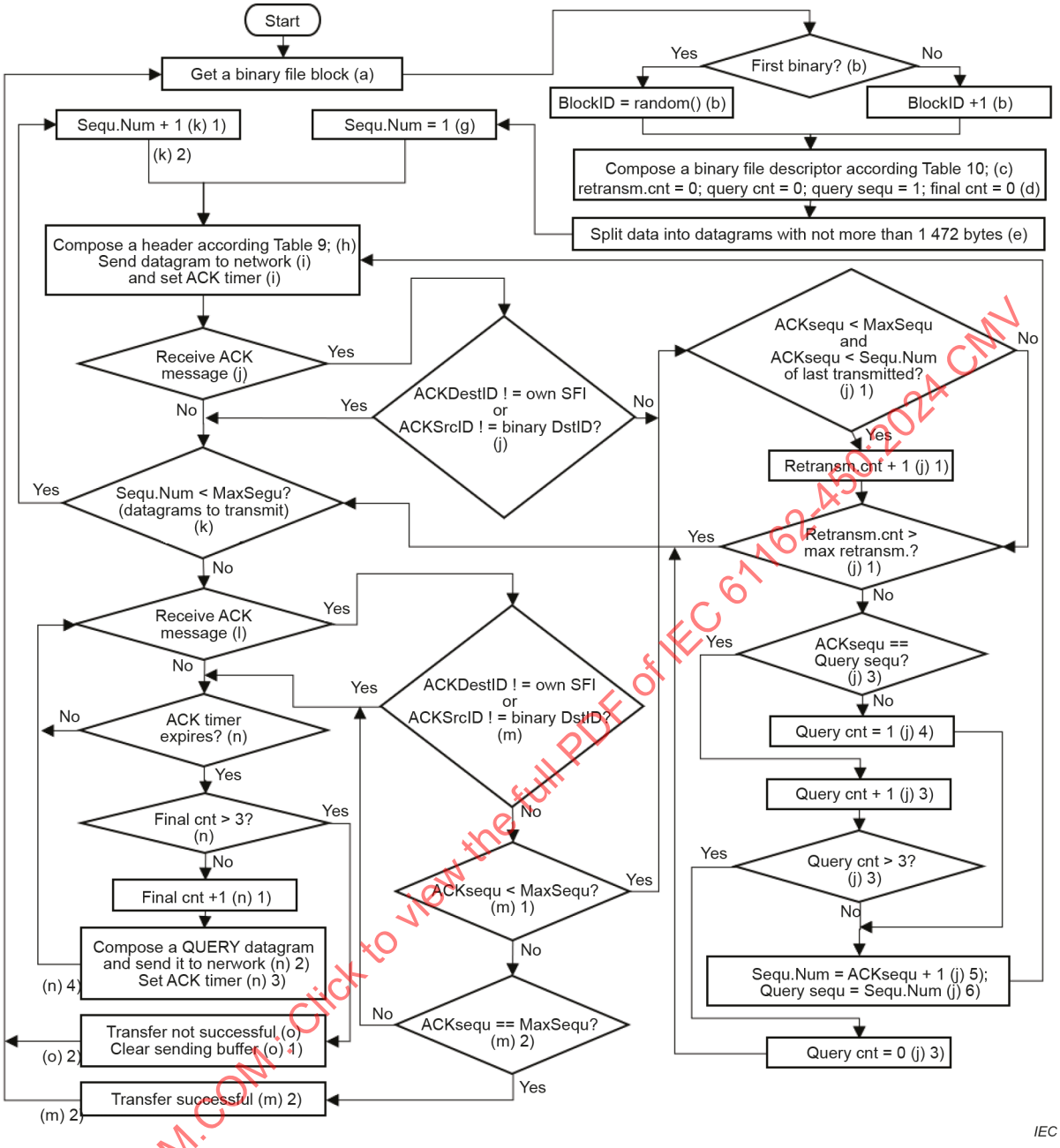


Figure 6 – Re-transmittable sender process

7.3.7 Receiver process for binary file transfer

7.3.7.1 Non re-transmittable receiver process

The receiver process steps of the non re-transmittable binary file transfer, including passive receivers of a re-transmittable binary file 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 the same as the maximum sequence number,
   - the 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 SFI is same as the DestID in the Header as follows (see Figure 7):

a) waits for receiving a new datagram;

b) if the token is not "RrUdP" or if DestID of received datagram is not equal to own SFI or the received datagram is an ACK message, go to step a);

c) if the received datagram is a QUERY message, then
   1) if no previous datagram is available, go to step a),
   2) if the sequence number of the previous datagram is not equal to maximum sequence number, go to step a),
   3) if all sequences flag is false (not all sequences of the previous binary block are received), go to step a),
   4) compose a Header with type = ACK, the BlockID and sequence number of the previous datagram,
   5) send an acknowledge datagram to the sender,
   6) go to step a);

d) if the sequence number is 1,
   1) analyse file image descriptor and header,
   2) if file image descriptor or header or token is invalid, go to step a),
   3) set re-transmission counter and query counter to zero (0), set query sequence number to 1, set all sequences flag to true,
   4) go to step g);

e) if no previous datagram is available, go to step g);

f) 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,
   1) if there is any data in the receiver buffer, it is delivered to the SF,
   2) the receiver buffer is cleared. Set re-transmission counter and query counter to zero (0). Set query sequence number to 1, set all sequences flag to true;

g) if the sequence number is not 1 and not the same as the sequence number of the previous datagram plus one,
   1) increase re-transmission count by one,
   2) if re-transmission count is greater than the maximum number of retransmissions (see 7.3.8.7), set all sequences flag to false and go to step a),
   3) if previous sequence number is identical to query sequence number increase query counter with 1, else go to step g) 6),
   4) if query counter is more than 3, set query counter to zero (0) else go to step g) 8),
   5) set all sequences flag to false and go to step a),
   6) if previous sequence number is not identical to query sequence number, set query counter to 1,
   7) set query sequence number to previous sequence number,
   8) compose a Header with type = ACK, the block identifier and sequence number of the previous datagram,

9) send an acknowledge datagram to the sender,

10) go to step (a);

h) put a datagram into the receiver buffer;

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

1) all the data in the receive buffer is delivered to the SF,

2) the receiver buffer is cleared,

3) the re-transmission count is set to zero (0);

4) else go to step a);

j) if all sequences flag are true,

1) compose a Header with type = ACK, the block identifier and maximum sequence number,

2) send an acknowledge datagram to the sender;

k) go to step a).

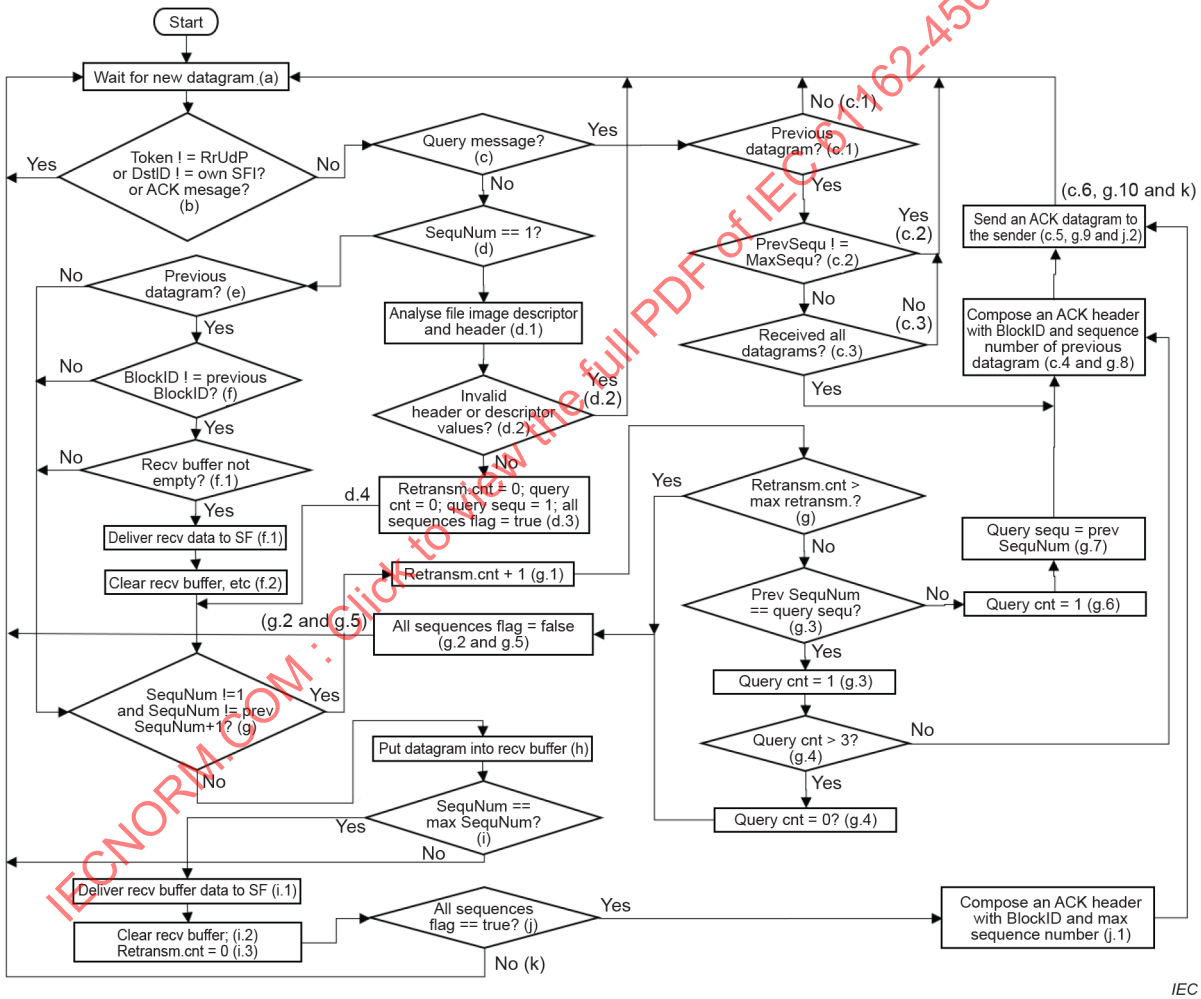


Figure 7 – Re-transmittable receive process

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 file blocks

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

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 file 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 file source shall not exceed 2 MBytes/s.

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

7.3.8.5 End of transmission for non re-transmittable and re-transmittable binary file transfer

The receiver shall assume that a transmission has ended unsuccessfully when it gets a binary file block from the 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 binary file block being received. The transmission shall also be considered finished when the last block is signalled by the SequenceNum from the sender. When a re-transmittable receiver identified by the DestID gets the last block after successful reception of all previous blocks, then it sends an ACK message to the sender to indicate successful transfer and so as to start new binary file block transmission. The receiver of non-re-transmittable binary file transfer and a receiver of re-transmittable binary file transfer not identified by DestID shall not send ACK message to the sender.

The re-transmittable sender assumes that the transmission is successfully finished only if it receives an ACK message with the SequenceNum which is equal to the MaxSequence; otherwise, a transmission has ended unsuccessfully. When a transmission is ended, a sender starts a new transmission if necessary.

7.3.8.6 Gaps between ACK messages for re-transmittable binary file transfer

In general, a receiver shall, immediately after loss detection, transmit an ACK message to the sender if a binary file block has been lost by having a gap in sequence numbers. 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 for another identical datagram. 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 for re-transmittable binary file transfer

The sender shall not retransmit the same datagram identified by sequence number of a binary file more than three times (i.e. totally four transmissions). After three retransmissions, the sender shall ignore any additional retransmission requests for this datagram identified by sequence number and continue transmitting the next datagram identified by sequence number. The receiver shall not query the same datagram identified by sequence number of a binary file more than three times.

The maximum number of re-transmission requests for a binary file shall be limited to 10 % of the maximum sequence number for the binary file but shall be not lower than three times. If the sender of a binary file receives more re-transmission queries than the maximum number, it shall ignore all further retransmission queries and continue to transmit the binary file until the last datagram identified by sequence number. In the case the receiver did not successfully receive all datagrams identified by sequence numbers of binary file, the receiver shall not acknowledge the last received datagram identified by sequence number with sequence number equal to maximum sequence number. The receiver shall not query datagrams in the same binary file more than the maximum number of retransmissions.

In addition to data message re-transmission, control (Query) 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 for re-transmittable binary file transfer

The re-transmission timer is managed at the sender. A sender sets the re-transmission timer when either a whole binary file 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 for non re-transmittable and re-transmittable binary file transfer

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

The receiver shall reply with ACK to the sender using the incoming datagram's AckDestPort and multicast address corresponding to this port number.

7.3.9 Error logging

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

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

7.4 General IEC 61162-3 PGN message transmissions

(see 8.12)

7.4.1 Message structure

The message structure for transporting IEC 61162-3 PGN messages into IEC 61162-450 networks is illustrated in Table 13.

Table 13 – Structure for PGN message

Header (see Table 9)
PGN message descriptor
IEC 61162-3 message fragment
IEC 61162-3 message fragment (zero or more)

The maximum message size of the PGN is 1 785 bytes. The PGN message shall be transmitted using one or two IEC 61162-450 datagrams. When there is a missing datagram, then the PGN message will be ignored as an error since the re-transmission of the lost datagram is not required.

7.4.2 Message format

The message format for transporting IEC 61162-3 PGN messages into IEC 61162-450 networks is illustrated in Table 14. The PGN message descriptor length for PGN messages is 32 bytes.

Table 14 – PGN message descriptor

Field Name	Size	Description
Source NAME (SNAME)	8 bytes of characters	Name of source. NAME shall be compliant with IEC 61162-3.
Source Device Identifier (SDID) [a]	2 byte of numeric number	Address of source device which is compliant with IEC 61162-3.
Destination NAME (DNAME)	8 bytes of characters	Name of destination. NAME shall be compliant with IEC 61162-3.
Destination Device Identifier (DDID) [a]	2 byte of numeric number	Address of destination device which is compliant with IEC 61162-3.
PGN number	4 byte of numeric number	PGN number of IEC 61162-3.
Priority	1 byte of numeric number	Priority of IEC 61162-3. Bit 0-2 are used and Bit 3 to Bit 7 are reserved.
Reserved (REVD)	7 bytes	Reserved bytes.
[a] Two bytes are specified to allow for future expansion.		

7.4.3 Address translation requirements

7.4.3.1 PGN group identification

A PGN group is defined as a logical group of devices that can share the information and message. Each PNGF shall be assigned a PGN group to communicate with devices in the group. The device address in a PGN group shall be unique in the network.

A PNGF may be registered with more than one PGN group if some of devices are required to communicate with devices in different PGN groups.

Means shall be provided to configure PGN groups at each PNGF.

7.4.3.2 Device identification

The PNGF shall represent all IEC 61162-3 equipment which are uniquely identified in the network.

A virtual device in an IEC 61162-3 network is identified by the source address. Each virtual device shall be identified by SFI of PNGF where it is connected, its PGN group number, its IEC 61162-3 source address and NAME. When there is no address available, then the address cannot be mapped until a new address is available. When a new address is not available, this event shall be recorded as specified in 4.3.3.

7.4.3.3 Address resolution

When a PNGF receives a query (i.e. Address Claim Message) about the device address with NAME and it has the information about the device, it shall respond with the address without forwarding the message to the IEC 61162-3 network.

7.4.4 Message processing

7.4.4.1 From IEC 61162-3 to IEC 61162-450

The PNGF shall have the capability of representing IEC 61162-3 devices as gateway device address and PNGF's SFI except for device address 0 which is always mapped to the device address 256. This is because the PNGF's device address of 0 represents PNGF itself on the IEC 61162-450.

The PNGF shall have the capability to represent it as at least an IEC 61162-3 device by obtaining its corresponding IEC 61162-3 source address from the IEC 61162-3 network.

When a PGN message is received from the IEC 61162-3, the PNGF extracts the information of source address, destination address, priority and PGN and it creates a message and fills up the corresponding fields. It also looks up the field of SFI and NAME of the destination address, and fills it out. When the received PGN message is not valid, then it will be discarded, and this event shall be recorded as specified in 4.3.3.

7.4.4.2 From IEC 61162-450 to IEC 61162-3

The PNGF shall have the capability to map 251 IEC 61162-3 source addresses to IEC 61162-450 device address and vice versa. The value of 251 is based on IEC 61162-3 address where the PNGF consumes 1 for the PNGF itself leaving 251 for mapping.

The address at IEC 61162-3 is source and destination device address. When a PNGF receives a message from an IEC 61162-450 network, it extracts the SDID and DDID information and puts it in the IEC 61162-3 PGN message and transmits into the IEC 61162-3 network. When the received PGN message is not valid, then it will be discarded, and this event shall be recorded as specified in 4.3.3.

7.4.4.3 Address conflicts

When there is a PNGF assigned address conflict in the address translation table of PNGF for mapping IEC 61162-3 network devices available as nodes in the network (i.e. when the same device address is assigned to more than one device), it shall be resolved. When a PNGF finds out that there are address conflicts, it re-assigns IEC 61162-3 device address mapping.

The address re-assignment process shall be done within 1 min.

7.4.5 Additional management requirements

7.4.5.1 Field configurable capability

The PNGF may also have the field configurable capability to change this default address so that the address is not claimed for a particular IEC 61162-3 device.

7.4.5.2 Non-volatile memory

The PNGF shall maintain configuration data in non-volatile memory. This ensures that field configurable settings are maintained across power cycles.

7.5 System function ID resolution

(see 8.13)

7.5.1 General

At the construction of a network of a ship, the assignment of SFI (system function ID) may be clearly defined. However, as the equipment of the ship is amended, replaced, repaired and serviced, the assignment of SFIs may not be as clear. This protocol assists in the detection of SFI collisions.

NOTE The receiver functions are covered in IEC 61162-460.

7.5.2 Transmitter functions

These functions apply to nodes which implement SF.

For each SF, including every instance identified by a combination of SFI and instance number, a transmitter in a network shall, as a minimum after boot up, 1 min after boot up, 5 min after boot up and after reconfiguration which changes any fields in an SRP sentence, send on address 239.192.0.56 port 60056 an SRP sentence to assist detection of collision of the SFI (see Annex F and Annex G). On receiving an SRP sentence with all fields being null fields, equipment shall respond with an SRP sentence with the fields populated.

Multiple sending of SRP is needed as different devices can have faster boot up time than the network monitoring performing the collision detection based on SRP sentences.

A node may periodically send an SRP sentence populated with at least its own MAC address and IP address at a suitable period determined by the manufacturer.

NOTE The usage of the SRP sentence for SFI collision monitoring is specified in IEC 61162-460 – SFI collision monitoring.

7.6 Binary file transfer using TCP point-to-point

(see 8.14)

7.6.1 Definition

This protocol provides a mechanism by which non IEC 61162-1 formatted data can be transmitted from a sender to a single receiver. The protocol emphasizes the reliability of the data transmission between two linked systems by using the TCP protocol.

NOTE The TCP standard is RFC 793. The IP standard is RFC 894. The Ethernet standard is IEEE Std 802.3.

Table 15 describes the terminology used.

Table 15 – Description of terms

Term	Description
BYTE	The lowest level data element consisting of 8 ordered bits (sometimes called an octet). Bit order is as determined by the computer implementation. The implementation shall make any necessary conversion between network bit order and computer bit order.
Data packet	A number of bytes that contains a header, an optional sequence of reserved bytes and the actual message content. The header specifies the length of header itself, of reserved bytes and data and will also contain information that allows a number of data packets to be re-assembled into a presentation.
Data element	One or more bytes that forms a stand-alone information carrier, i.e. a time stamp, an integer or a character.
DWORD	Double word. One unsigned 32-bit integer (in range 0 to 4294967295). The DWORD is constructed from four consecutively transmitted BYTES, where the transmission order on the network is the most significant BYTE first followed by the next most significant BYTE until the least significant BYTE.
File	One group of bytes that forms a stand-alone data set.
Message data	The data contents of a data package.
Reserved bytes	A number of bytes in the data packet 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 the range 0 to 65535). The WORD is constructed from two consecutively transmitted BYTES, 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 BYTES, interpreted as a string of characters. The transmission order on the network is the left-most character first. If the string is shorter than n, additional trailing bytes shall be set to zero. All strings in the header are encoded in ISO/IEC 18859-1 (ISO Latin 1).

7.6.2 Data field structure for transfer of files

7.6.2.1 General

The files are transmitted over the network in packets. The data field is defined as a sequential and unpadded stream of octets divided into two main groups – header and package data, as shown in Table 16. The header is needed for synchronisation and data integrity validation.

Table 16 – Binary file structure

Header (see 7.6.2.2)
Package data (see 7.6.2.3)

7.6.2.2 Elements of the header structure

The header format is defined in the Table 17. The first column specifies the name of the data item inside the header (starting from offset zero). The second column specifies the data type and size. The third column describes the data item and its purpose.

Table 17 – Header structure

Data item	Type	Description
token	STRING[6]	It shall always contain the string "RrTcP" including a trailing NULL character. Identifier as ASCII string with a length of 5 bytes. This token defines the beginning of a new data block.
crcHeader	WORD	Cyclic redundancy check for the header according to CRC-16/CCITT-FALSE. The CRC is calculated from and including headerversion to and including any reserved bytes. The CRC is calculated from the sequence of bytes after formatting into transmission byte order. The CRC polynomial is: $x^{16} + x^{12} + x^5 + 1$.
headerversion	WORD	Defines the header version. The headerversion with value 1 is defined in this document. Extensions and/or modified versions will update this value.
headerlength	DWORD	Defines the binary file descriptor length in bytes. This is at least the length of the header including the reserved bytes. Future editions of IEC 61162-450 may append additional fields to this file descriptor without incrementing the header version as long as these additional fields are compatible with the definition of the file descriptor in this document. Receivers which are not aware of these additional fields shall ignore them.
srcID	STRING[6]	Define the source system identifier in format "ccxxxx" (see 4.4.2).
datalength	DWORD	Defines the data content of this data package in octets. This may be the full (oversized) data in one package or a typical size for network transfer (1 280 octets). In the latter case, maxnum, actnum and streamlength will be used to synchronize data packets into a complete data transfer.
timeSec	DWORD	Seconds part of time stamp. Timestamp is constructed both of time in seconds and nanoseconds at the grabbing instant. If required by the application (e.g. image transmission to the VDR), the timestamp shall be made at the source immediately at data recording. If the application allows the timestamp to be optional and no timestamp is available, the value 0 shall be used for timeSec and timeNsec. The time representation is the number of seconds since January 1st 1970, not including leap seconds (i.e. in astronomic/GMT representation). This information is only needed with the first packet of each file or data stream. Time stamps in the following data packages belonging to the same data transfer shall be discarded by the receiver. It is only practicable to use this value if the synchronization between the destination device (e.g. VDR) and the source device (e.g. Radar unit) is sufficiently precise (in the range of milliseconds). The difftime data item may be used as an alternative method for synchronisation. If difftime is non-zero, this field shall be ignored.
timeNsec	DWORD	Nanosecond part of time stamp. See timeSec for details.
difftime	WORD	Time difference in milliseconds between data recording instant (e.g. grabbing instant) and transmission of the first packet of the file. A timestamp with a resolution of at least in the millisecond range is made immediately before the source generation (e.g. screenshot) and the second timestamp is made immediately before the first packet is transmitted. The difference is entered as "difftime" and the packet is then sent. The destination device (e.g. VDR) uses this difftime value together with its system time to determine the timestamp for the transmitted data. Time tolerances between destination device and source device may be neglected, because the time reference of the destination device is always the system time of the destination device.
maxnum	DWORD	Number of packets needed for transmission of the corresponding file or data stream. The value can be 1 or more.
actnum	DWORD	This packet number (range from 1 to maxnum).
streamlength	DWORD	Defines the length of the (full) stream/presentation content in octets

Data item	Type	Description
device	BYTE	Data source (device) as binary value, 1 for equipment 1, 2 for 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.
deviceip	DWORD	IP of transmitting device; optionally used. The IP address is entered in Network Byte Order Format (DWORD).
deviceport	WORD	That port the transmitting device has used. It may be used optionally.
typelength	BYTE	The length of the datatype field.
datatype	STRING[n]	This string defines the datablock encoding by assigning a MIME content type to the datablock for the server followed by a null character. For example, image/png is used for PNG image files and application/zip is used for zip-files. This document has the datatype specified as STRING[n]. Previous editions had STRING[16]. Transmitters shall have a setup parameter to use the length as "n" or "16" to maintain compatibility with previous editions of IEC 61162-450. In the compatibility instance, receivers may receive padding at the end of datatype string.
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.
StatusLength	WORD	The length of the "Status and information text" field in bytes.
Status and information text	STRING[n]	Status information (e.g. successful operation or error codes). This may be one or more strings terminated by a binary null.

7.6.2.3 Elements of the package data structure

The package data format is defined in Table 18. The first column specifies the name of the data item. The second column specifies the data type and size. The third column describes the data item and its purpose.

The package data structure size is set to zero if only status information is transmitted.

Table 18 – Package data structure

Data item	Type	Description
datablock	BYTE[datalength]	This item is the data either split into pieces or in one block. Size is defined by datalength in the header.

There is no CRC for the data contents as this is partly handled by the TCP/IP layer or by other mechanisms in the contents format. The header has a separate CRC as it is deemed more critical for the correct operation of the system.

7.6.3 Structure of the transfer stream

7.6.3.1 General

The complete binary file is split into a number of datablocks. Each header and datablock is transmitted in increasing order, beginning with the first datablock and ending with the last datablock. Synchronisation is achieved with data items actnum and maxnum.

7.6.3.2 Unknown data types

A receiver that does not understand an incoming data type shall ignore all incoming data without closing the connection if the receiver is a server.

If the receiver is a client and does not understand incoming data, it shall immediately close the connection.

7.6.3.3 Maximum outgoing rate

The data volume for each transmit client of binary file shall not exceed 2 MBytes/s.

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

7.6.4 TCP port and IP addresses

The IP address shall be freely selectable outside the addresses assigned for other purposes in this document and the IP address is depending on the network configuration of the corresponding equipment manufacturer.

The IP address of each file source and the file receiver has to be coordinated and set manually beforehand to be in the same IP address range.

Equipment unable to perform an address look-up service should be configured to the same IP sub-net. A router may be used if the equipment is connected on different IP sub-nets.

The default TCP port between sender and receiver for the transfer shall be 7097. Sender and receiver shall support configuration of the port number and IP address.

7.6.5 Implementation guidance

7.6.5.1 General

In the examples in 7.6.5.2, 7.6.5.3 and 7.6.5.4, it is assumed that the TCP client is the sender and the TCP server is the receiver. In general, both TCP server and TCP client may send or receive data.

7.6.5.2 Receiver as server and sender as client

This setup is used for example for VDRs where the VDR as the file receiver has to be configured as a passive listening device. The file sender is the active transmit client connecting and transferring the data.

Depending on the application, the file receiver may be set up to accept multiple transmit clients on the same input port. This is necessary if more than one transmit client is assumed to send its files to the receiver server.

7.6.5.3 Connection management from sender client

The transmit client shall establish a connection to the receiver server immediately after system initialisation. Once the connection is established, the transmit client is responsible for the connection and streaming of data packet to the receiver server.

If the connection attempt fails or connection is lost, the transmit client shall try to establish the connection again. The interval between attempts shall not exceed 30 s.

7.6.5.4 Connection management from receiver server

The receiver server shall make the listening port available for data transfers during initialisation.

The manufacturer shall specify the maximum number of transmit client connections for the receiver server. The receiver server shall receive data individually from connected transmit clients and detect any loss of connection from transmit clients.

The equipment test and performance standard may require alerts to be raised for loss of connection.

The receiver server may in some cases only detect a failed connection by timeout since data was received last time. The receiver server shall reinitialise the listening port and the receiver software module after timeout for the transmit client.

7.6.5.5 Error handling

The receiver shall ensure data integrity at reception by verification of the header including token, version, consistency of data fields and the header CRC. Erroneous data reception shall be processed and indicated according to individual equipment standard.

NOTE Consistency of data fields can depend on application. However, strings can be checked against containing illegal characters, message sequence numbers can be checked, etc.

7.6.5.6 Transmission of a file

The client transmission of a file may occur at any time when the connection is open. The message header information is sufficient for the server to decode the data stream and reassemble the file and its associated header information data.

7.6.5.7 Device identification

All clients shall be configured with a unique source SFI and device identification (1 to 255) to allow the server to unambiguously identify the source of the received packets.

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 EUT. 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 to be 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;
- if the EUT implements support for PGN, generation of IEC 61162-3 PGN test sentences containing unique and numbered content, syntactically correct and incorrect with variable length and correct, incorrect and missing checksum;
- 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 and reception of non re-transmittable and re-transmittable binary files.

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 EUT has 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)

Confirm by inspection of manufacturer provided information that the EUT does not provide the functions of a repeater hub.

Confirm by inspection of documented evidence that the EUT supports IGMP protocol and that the version of IGMP support is documented.

If the EUT is a switch,

- confirm by inspection of documented evidence that it supports IGMP snooping, and
- confirm by inspection of documented evidence that the IGMP snooping based multicast traffic filtering is supported per each multicast address.

Use a simulation arrangement to generate multicast datagrams with address range of 224.0.0.1 to 224.0.0.255 and confirm by observation that the EUT does not filter out those datagrams.

8.2.3 Documentation

(see 4.4.1, 7.1.1)

Confirm by inspection of manufacture's documentation that all of the implemented datagram types are specified.

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 4.3.2, a) to c).

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 that 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, the output of syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

If reception of syslog message capability is provided, confirm by analytic evaluation that the reception and logging of syslog messages conforms to the manufacturer's documentation and the requirements of 4.3.3.2.

8.4 System function block (SF)

8.4.1 General

(see 4.4.1)

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

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

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.

Check that manufacturer's documentation include instructions how to select "cc" and "xxxx" part of the SFI so that the SFI is unique at least within the IEC 61162-450 network.

8.4.3 Implementing configurable transmission groups

(see 4.4.2)

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 sources distinguished by different talker mnemonic per each serial port of the device and that the mapping of SFI to sources distinguished by different talker mnemonic per each serial port is correctly implemented by analysing the UDP datagrams.

Check that TAG block source identification “s” is correctly implemented to sources distinguished by different talker mnemonic per each serial port by analysing the UDP datagrams.

Check that TAG block destination identification "d" is correctly implemented for routing from network to serial ports.

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

- prioritized sentences are correctly replaced, maintaining the FIFO order and not affecting sentence integrity, and
- in case buffer overflow sentences are discarded, the FIFO order is maintained, not affecting sentence integrity, and 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, SFI, source identification "s" and, if required, destination identification "d".

The test sentences should include TAG blocks and grouped messages.

Test configuration should include single source per serial port and multiple sources distinguished by different talker mnemonics per shared serial port.

8.5.4 Multi SF serial port

(see 4.5.4)

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, SFI, source identification "s" and, if required, destination identification "d".

Test configuration should be configured for multiple sources distinguished by different talker identifiers and manufacturer mnemonic codes (for proprietary sentences) per shared serial input port. The output should be configured for single destination by talker identifier.

Check the test cases below:

1) received sentences with configured talker identifiers and manufacturer mnemonic codes will transmit datagrams with the configured SFI;
2) received sentences without a configured talker identifier or manufacturer mnemonic code will transmit datagrams for each configured SFI;
3) received datagrams with configured destination SFIs will be transmitted on configured serial port;
4) received datagrams with a valid destination that is an unknown SFI will not be transmitted on any serial port;
5) received datagrams with no destination specified will be transmitted to all serial ports.

In the test cases below, the SNGF SFI is "SI0001", the configured SFIs of serial ports are TI0001 (for Talker Identifier "TI") and VD0001 (for Talker Identifier "VD"). A proprietary sentence "PMANMSG" is configured for SFI VD0001. The typical received sentences will then include rate-of-turn ("$TIROT") and speed ("$VDVBW").

- Test case 1: An example of simple SFI conversion:

  "$TIROT,123.45*67<CR><LF>$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  "$PMANMSG,proprietary_contents*hh<CR><LF>"

  will generate three datagrams, one for each SFI:

  "\s:TI0001,n:333*hh\$TIROT,123.45*67<CR><LF>"

  "\s:VD0001,n:111*hh\$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  "\s:VD0001,n:111*hh\>$PMANMSG,proprietary_contents*hh<CR><LF>"

  with the IEC 61162-450 Header("UdPbC'0'").

- Test case 2: An example of un-configured talker identifier:

  "$SDDPT,123.4,,400*hh<CR><LF>"

  will generate one datagram for each configured SFI:

  "\s:TI0001,n:222*hh\$SDDPT,123.4,,400*hh<CR><LF>"

  "\s:VD0001,n:222*hh\$SDDPT,123.4,,400*hh<CR><LF>"

  with the IEC 61162-450 Header("UdPbC'0'").

- Test case 3: An example of simple SFI conversion, no TAG block support:

  Datagram "\s:IN0001,d:TI0001,n:333*hh\$INTIQ,ROT*hh<CR><LF>"

  will generate transmission of the sentence on the serial port configured for the destination SFI TI0001:

  "$INTIQ,ROT*hh<CR><LF>"

- Test case 4: An example of a specified destination but un-configured SFI conversion:

  Datagram "\s:IN0001,d:GN0001,n:333*hh\$INGNQ,ZDA*hh<CR><LF>"

  will not generate transmission on any serial ports.

- Test case 5: An example of no specified destination:

  Datagram "\s:IN0001,n:333*hh\$INGNQ,ZDA*hh<CR><LF>"

  will generate transmission of the sentence on all serial ports.

  "$INGNQ,ZDA*hh<CR><LF>"

8.5.5 Handling malformed data received on serial line

(see 4.5.5)

Verify datagram conversion by feeding the SNGF input ports under test with valid sentences interleaved with malformed data according to 4.5.5.

Confirm that the valid sentences are correctly converted into datagrams.

Each test shall include test cases for all of the start characters. Check that the test cases below will generate a datagram transmission:

1) when data has been received before a start character;
2) when data has been received after a valid start character and the maximum sentence and TAG block length has been exceeded;
3) when data has been received after a valid start character and end of line (<CR><LF>) has not been received within 1 s;
4) when a reserved character has been received and not having been appropriately escaped;

5) when random binary data is sent on serial line.

In the test cases below, the SNGF SFI is SI0001, the configured SFI of serial port is TI0001 (for Talker Identifier "TI").

- Test case 1: An example of data before start character:

  `Serial data "127,333*6B<CR><LF>$TIROT,123.45*67<CR><LF>"`

  will generate two datagrams:

  `either`

  `"\s:SI0001,n:444*hh\127,333*6B<CR><LF>" (if SFI for malformed sentences set by configuration to be SI0001)`

  `or "\s:TI0001,n:444*hh\127,333*hh<CR><LF>" (if SFI for malformed sentences set to follow non-malformed sentences)`

  `and`

  `"\s:TI0001,n:445*hh\$TIROT,123.45*hh<CR><LF>"`

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 2: An example of too long line:

  `Serial data "$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>"`

  will generate one datagram, i.e. no change to content:

  either

  `"\s:TI0001,n:446*hh\$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>" (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)`

  or

  `"\s:U20001,n:446*hh\$TIALR,123456,906,A,V,Sensor fault with a too long description to violate serial data maximum line length limitation*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be U20001)`

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 3: An example of timeout:

  `Serial data "$TIALR,123456,906,A,V,"`

  <1.1 s delay>

  `Serial data "Sensor fault*hh<CR><LF>"`

  will generate two datagrams:

  either

  `"\s:TI0001,n:447*nn\$TIALR,123456,906,A,V," (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)`

  or

  `"\s:SI0001,n:447*nn\$TIALR,123456,906,A,V," (if SFI set by configuration to be SI0001)`

  and either

  `"\s:SI0001,n:448*nn\Sensor fault*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be SI0001)`

  or

  `"\s:TI0001,n:448*nn\Sensor fault*hh<CR><LF>" (if SFI for malformed sentences set to follow non-malformed sentences)`

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 4: An example of incorrect escape:

  "$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>"

  will generate a datagram (i.e. no change to content):

  either

  "\s:TI0001,n:449*nn\$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>" (if SFI for malformed sentences set based on talker mnemonic or set to follow non-malformed sentences)

  or

  "\s:SI0001,n:449*nn\$TITXT,01,01,01,Incorrect * escape*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be SI0001)

  and with the IEC 61162-450 Header ("UdPbC'0'").

- Test case 5: An example of random serial data including start characters "$" that will initiate a new datagram:

  "kfajds…3efbnajfu93hn$lkfdajkf98873tq87784((/kfajd..”

  The above random data will generate two datagrams:

  either

  "\s:SI0001,n:449*nn\kfajds...3efbnajfu93hn" if SFI for malformed sentences set by configuration to be SI0001)

  or

  "\s:TI0001,n:449*nn\kfajds...3efbnajfu93hn" (if SFI for malformed sentences set to follow non-malformed sentences)

  followed by either

  "\s:SI0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." (if SFI for malformed sentences set by configuration to be SI0001)

  or

  "\s:TI0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." (if SFI for malformed sentences set to follow non-malformed sentences)

  or

  "\s:lk0001,n:450*nn\$lkfdajkf98873tq87784((/kfajd.." if SFI for malformed sentences set based on talker mnemonic)

  and with the IEC 61162-450 Header ("UdPbC'0'").

In the test cases below for Multi SF serial port, the SNGF SFI is SI0001, the configured SFIs of the serial port are TI0001 (for Talker Identifier "TI”) and VD0001 (for Talker Identifier "VD").

- Test case 6: An example of data before start character:

  Serial data

  $VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>127,333*6B<CR><LF>$TIROT,123.45*67<CR><LF>

  will generate three datagrams:

  "\s:VD0001,n:443*hh\$VDVBW,10.00,,A,,,V,,V,,V*hh<CR><LF>"

  and either

  "\s:VD0001,n:444*hh\127,333*hh<CR><LF>" (if SFI for malformed sentences set to follow non-malformed sentences, and there were no preceding STN sentence)

  or

  "\s:U20001,n:444*hh\127,333*hh<CR><LF>" (if SFI for malformed sentences set by configuration to be U20001)

  and

  "\s:TI0001,n:445*hh\$TIROT,123.45*hh<CR><LF>"

  and with the IEC 61162-450 Header ("UdPbC'0'").

8.6 Other network function (ONF)

(see 4.7)

Verify by inspection of the manufacturer's documentation that information for the use of ONF is provided as described in 4.7.

Verify by inspection of the manufacturer's documentation 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 the EUT does not send packets with IP options set; except for IGMP packets, where IP options are used for the correct functioning of IGMP protocol.

Confirm by generating an example of each relevant (see 5.2) packet and analysing this packet using packet capture software to confirm that the EUT 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 within the ranges reserved for private networks as described in ISOC RFC 1918.

Confirm that any excluded IP ranges reserved for internal sub-nets (internal to the equipment) are documented and those are not in the range given by 5.3.

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 datagrams are transmitted and received at each of the appropriate port numbers as defined in Table 4 and Table 5.

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

Verify that each transmitted UDP datagram contains no more than 1 472 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 files,
- "`RrUdP`" for transmission of re-transmittable binary files, and
- "`NkPgN`" for transmission of IEC 61162-3 PGN messages,

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

Check that all TCP/IP datagrams are headed by "`RrTcP`" for transmission of binary files as described in 7.6 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, as part of error logging, the count of received datagrams without valid datagram header (see 7.1) is increased if datagram header is unrecognized or invalid.

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 analyser that

- if provided, all members of group have same group code value,
- if provided, next group code value after 99 is 1,
- the EUT transmits the source identifier (two separate test cases – default and configured),
- if provided, the EUT transmits valid source cluster identification,
- if provided, the EUT transmits valid destination code,
- if provided, the EUT transmits valid destination cluster identification,
- if provided, line count value increments for each line and resets after 999 to 1,
- if provided, the heartbeat sentence (HBT) is transmitted at least once every 60 s, and
- the EUT 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 analyser, 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 "\b:Y23G81*4E\") not defined in this document is transparent to normal operation,
- only complete sentence groups are used, and
- TAG block lines with the EUT as destination are processed. Destination is a combination of parameter codes destination code "d" and, if available, destination cluster identification "x".

NOTE 1 Not available destination cluster identification can mean navigation cluster as destination.

NOTE 2 Processing can also mean that data is dropped.

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.

8.9.5 General authentication

(see 7.2.3.8)

These tests apply to a EUT that includes transmission of authentication.

Confirm by inspection of manufacturer's documentation which signature methods the EUT provides.

Confirm by analytic evaluation that the EUT transmits sentence or message with correct authentication code as described in 7.2.3.8. Repeat the test for all signature methods supported by the EUT.

Use simulation arrangement to create valid examples of authenticated sentences or messages and confirm by observation that, if the EUT is not set to require authentication, the EUT processes all sentences or messages.

Use simulation arrangement to create same valid examples of authenticated sentences or messages as in previous test, and confirm by observation that, if the EUT is set to require authentication, the EUT processes all sentences or messages. Repeat the test for all signature methods supported by the EUT.

Use simulation arrangement to create same valid examples of sentences or messages as in previous test, but without including authentication parameter code, and confirm by observation that, if the EUT is set to require authentication, the EUT discards all sentences or messages.

Use simulation arrangement to create same valid examples of sentences or messages as in previous test, but with intentionally incorrect value in the authentication parameter code, and confirm by observation that, if the EUT is set to require authentication, the EUT discards all sentences or messages. Repeat the test for all signature methods supported by EUT.

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, and
- 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, and
- incorrect message length.

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

8.11 Binary file transfer using UDP multicast – Single transmitter, multiple receiver

(see 7.3)

8.11.1 Sender process test

8.11.1.1 Non re-transmittable binary file transfer

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

- header token is set correctly,
- header version is set according the Table 9,
- SrcID is set according to Table 9,
- DestID is correctly set according to Table 9,
- 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 file transfer,
- the SequenceNum of first datagram is set to 1, and
- there is no response when a receiver sends any ACK messages.

8.11.1.2 Re-transmittable binary file transfer

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

- header token is set correctly,
- header version is according to Table 9,
- SrcID and DestID are 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, port number and AckDestPort are assigned by one of the addresses for binary file transfer,
- the maximal re-transmission count is calculated correctly according 7.3.8.7,
- the SequenceNum of the first datagram is set to 1,
- ACK messages are received from multicast group, specified from AckDestPort,
- ACK messages are only processed if the DestID of ACK message is equal to own SFI and if the SourceID of ACK message is equal to actual DestID, otherwise the ACK message is ignored,
- the binary transfer is finished and marked as successful after an ACK message is received, whose SequenceNum is equal to the MaxSequence, after all data is transmitted,
- a QUERY message is sent when there is no ACK message received, after all data are transmitted,
- not more than four QUERY messages at all are sent when there is no ACK message received after a QUERY message is transmitted,
- binary file data from SequenceNum one higher as SequenceNum of ACK is re-transmitted when an ACK message whose SequenceNum is less than the MaxSequence is received,

- the same SequenceNum is retransmitted not more than three times, otherwise the re-transmittable sender continues with normal transfer and ignores ACK message,
- the number of all re-transmissions is not more than the maximal re-transmission count, otherwise the re-transmittable sender continues with normal transfer and ignores ACK messages,
- the binary transfer is finished and marked as not successful after all data is transmitted, if three QUERY messages are sent and no ACK message whose SequenceNum is equal to the MaxSequence is received, and
- log messages are correct.

8.11.2 Receiver process test

8.11.2.1 Non re-transmittable binary file transfer

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

- messages are received correctly on given IP and port address,
- message is only processed if the header token is equal to "RaUdP" or "RrUdP",
- message is only processed with valid header and valid binary file descriptor,
- each separate binary file 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, and
- log messages are correct.

8.11.2.2 Re-transmittable binary file transfer

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

- messages are received correctly on given IP and port address,
- message is only processed if the header token is equal to "RrUdP",
- message is only processed with valid header and valid binary file descriptor,
- message is only processed if DestID is equal to own SFI,
- each separate binary file transfer is identified by the combination of SrcID, BlockID, Device and Channel,
- the maximal re-transmission count is calculated correctly according 7.3.8.7,
- ACK messages are generated with the correct token = RrUdP, SrcID = own SFI, DestID = SrcID of received message, BlockID and without binary file descriptor and without data block,
- ACK messages are transmitted to the multicast group corresponding to the AckDestPort of the actual received binary file block,
- the receive process is marked as successful and an ACK message is transmitted when the received SequenceNum is equal to the MaxSequence with the same instance identifier and if all sequences of the actual binary file block are received,
- an ACK message for a successful received binary file block is not more than three times repeated if query messages are received,
- if no complete binary file block is received, the transfer is marked as not successful and no ACK message after the last received sequence with SequenceNum equal to MaxSequence is transmitted, either directly after received last sequence or after received query messages,

- an ACK message is transmitted with the last received SequenceNum before a gap when the re-transmittable receiver detects that there is a gap in the SequenceNum between two consecutive messages,
- an ACK message for the same requested SequenceNum is not more than three times repeated for the same binary file block,
- the number of all ACK messages for retransmission request is not more than the maximal re-transmission count for the same binary file block,
- 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 re-transmittable receiver does not send any ACK message when a re-transmittable sender sends a binary file block with different DestID, and
- log messages are correct.

8.11.3 Binary file descriptor test

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

- the AckDestPort field is correctly set,
- the Length field, the TypeLength field and the StatusLength field are correctly set,
- binary file length in the descriptor is the same as the size of the received data, and
- the received data format is the same as that of the data type in the descriptor.

8.11.4 Binary file transfer error logging

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

- number of binary file blocks where errors occur;
- missing datagrams;
- unrecognized headers (see 8.9.2).

8.11.5 Maximum outgoing rate

Confirm by inspection of documented evidence that the EUT has an effective method to limit the outgoing rate to be within the given limit of 2 Mbytes/s (see 7.3.8.4).

8.12 PGN to network gateway function (PNGF)

(see 7.4)

8.12.1 General

Check that it is possible to enter unique SFIs for all sources distinguished by different devices and that the mapping of SFI to sources distinguished by different device identifier is correctly implemented by analysing the UDP datagrams.

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

8.12.2 Output buffer management

Verify the output routing by feeding the network under test with datagrams containing PGNs for all IEC 61162-3 networks and check that PGNs are routed to the network having the set device identifier.

Check that documentation is available describing the maximum buffer capacity.

Check that the means are provided to configure the maximum buffer capacity.

Check that the overflow is logged as required.

8.12.3 Datagram output

Verify datagram conversion by feeding the input ports of the network under test with PGNs and check if these are transmitted in UDP datagrams as described in 7.4.1.

Verify a single IEC 61162-3 PGN message transmission per each feeding IEC 61162-450 message.

8.12.4 PGN group

Verify PGN group filtering by transmitting four PGN groups and check that the device only receives the PGN group messages to which it belongs.

8.12.5 Address conflicts

Confirm by observation that the EUT assigns new IEC 61162-3 addresses at the address translation table within 1 min when IEC 61162-3 addresses at the EUT conflict with the addresses in IEC 61162-3 Network.

8.13 System function ID resolution

(see 7.5)

Confirm by observation that the EUT sends SRP sentences to address 239.192.0.56 port 60056 when boot up, 1 min after boot up, 5 min after boot up and after reconfiguration, including both reconfiguration of setup parameters and reconfiguration based on a change caused by redundancy arrangements.

NOTE The boundaries of test for redundancy arrangements are the connections from each of its physical interfaces to their immediate switches only.

Confirm by observation that when the EUT receives an SRP sentence with all fields being null fields the EUT responds with an SRP sentence with the fields populated.

8.14 Binary file transfer using TCP point-to-point

(see 7.6)

8.14.1 Test of transmit client

8.14.1.1 Description

The test set-up is a controllable receiver server and the equipment under test. The following tests shall be performed and passed.

8.14.1.2 Connection establishment test

Remove receiver server from the network and power up the transmit client. Confirm by observation that the transmit client performs reconnection attempts as specified.

Connect receiver server and confirm by observation that connection is established.

8.14.1.3 Lost connection test

Power down or physically remove receiver server from the network and confirm by observation that the transmit client detects connection failure. This will normally require the transmission of some data from the transmit client.

Reconnect receiver server and confirm by observation that the transmit client reconnects the receiver server. Confirm by observation that the transmit client sends data as specified. Confirm by observation that the headers are according to the data format specification. Confirm by observation that time stamp is increased.

Break connection in the middle of a transfer. Confirm by observation that the transmit client continues to operate and tries to reconnect.

8.14.2 Test of receiver server

8.14.2.1 Test set-up

The test set-up is a controllable transmit client and the equipment under test. The transmit client shall be able to generate the following, and tests shall be made that check the correct functioning of the receiver server in these cases.

8.14.2.2 Connection establishment test

Remove transmit client(s) from the network and power up receiver server. Confirm by observation that receiver server starts up as specified.

Connect transmit client(s) and confirm by observation that receiver server enters normal operation.

8.14.2.3 Lost connection test

Break connection in the middle of a transfer. Confirm by observation that the receiver server continues to operate.

8.14.2.4 Message transfer test

Transfer at least one file with a content type which is supported by the receiver server, streamed as a sequence of at least 5 datablocks. Confirm by observation that the receiver server correctly processes the file.

8.14.2.5 Multiple transmit client test

If the receiver server supports simultaneous connections from multiple transmit clients, establish the maximum number of connections according to the manufacturer. Send files simultaneously over all connections. Confirm by observation that the receiver server correctly processes all received files.

8.14.2.6 Erroneous input test

Send a file with datalength in the header set to a value which is smaller than the actual size of transmitted data. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

Send a file with an invalid crcHeader value in the header. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

Send a file which is streamed as at least 5 packets. Discard the 3rd packet. Confirm by observation that the receiver server detects the error and indicates it according to the individual equipment standard.

8.14.2.7 Undefined header test

Send a file with the header version set to a value higher than defined in this document. Confirm by observation that the receiver server ignores the unknown part of the header based on the implemented header version and that the receiver server processes the file.

8.14.3 Maximum outgoing rate

Confirm by inspection of documented evidence that the EUT has an effective method to limit the outgoing rate to be within the given limit.

8.14.4 TCP port and IP addresses

Confirm by inspection of manufacturer's installation documentation that the default port is specified as 7097 and that there are instructions to set both sender and receiver in the same IP address range.

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 gives default classification of each of the IEC 61162-1 sentence formatters as belonging to one of the following three types of message:

- sensor broadcast message (SBM), see 3.22;
- multi-sentence message (MSM), see 3.14;
- command-response pair (CRP), see 3.4.

If provided by the equipment, the default transmission group and classification can be changed by the parameter setup system of the equipment to USR1 to USR8, RCOM, PROP in Table 4 or any in Table 5.

A.2 Talker identifier mnemonic to transmission group mapping

Table A.1 maps the two first characters of the SFI, which 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.

For alert communication purposes, an alert source shall use transmission group BAM1 or BAM2 as default or, if in addition optional configuration of transmission groups is provided, any transmission group in Table 4 and Table 5.

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
CAM of BAM	CA	CAM1 or CAM2
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

Type of equipment	Talker identifier	Transmission group
scanning receiver	CX	RCOM
Direction finder	DF	NAVD
Duplex repeater station	DU	MISC
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
Network device	ND	NETA
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
Voyage data recorder	VR	MISC
Watertight door controller/monitoring system	WD	VDRD
Water level detection system	WL	VDRD
Transducer	YX	MISC

Type of equipment	Talker identifier	Transmission group
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	SI	MISC

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 CRP 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	X	ABM Sometimes single
ACA	AIS channel assignment message		X		ACA, ACS Sometimes single
ACK	Acknowledge alarm			X	ALR
ACN	Alert command			X	AGL, ALC, ALF, ARC
ACS	AIS Channel management information source		X		ACA, ACS
AGL	Alert group list			X	ALC, ALF
AIR	AIS Interrogation request			X	ABK
AKD	Acknowledge detail alarm condition			X	ALA
ALA	Report detailed alarm condition			X	AKD
ALC	Cyclic alert list		X		ACN
ALF	Alert sentence		X		ACN
ALR	Set alarm state	X		X	ACK
APB	Heading/track controller (autopilot) sentence B	X			
ARC	Alert command refused			X	ACN
BBM	AIS Broadcast binary message		X	X	BBM Sometimes single
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			
CUR	Water current layer – multi-layer water current data	X			

	Description	SBM	MSM	CRP	Related sentence formatters
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			
EPM	Command or report long equipment property value	X			
EPV	Command or report equipment property value	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			
GDC	GNSS differential correction	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			
GSN	GNSS SBAS navigation message	X			
GST	GNSS pseudorange noise statistics	X			
GSV	GNSS satellites in view	X			
HBT	Heartbeat supervision sentence	X			
HCR	Heading correction report	X			
HDG	Heading, deviation and variation	X			
HDT	Heading true	X			
HMR	Heading monitor receive			X	HMS
HMS	Heading monitor set			X	HMR
HRM	Heel angle, roll period and roll amplitude measurement device	X			
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	X	LRF, LRI
LR2	AIS long-range reply sentence 2		X	X	LRF, LRI
LR3	AIS long-range reply sentence 3		X	X	LRF, LRI
LRF	AIS long-range function		X	X	LR1, LR2, LR3, LRF
LRI	AIS long-range interrogation		X	X	LR1, LR2, LR3, LRF

	Description	SBM	MSM	CRP	Related sentence formatters
MOB	Man over board notification	X			
MSK	MSK receiver interface	X			
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
NLS	Navigation light status	X			
NRM	NAVTEX receiver mask			X	NRX
NRX	NAVTEX received message		X		
NSR	Navigation status report	X			
OSD	Own ship data	X			
POS	Device position and ship dimensions report or configuration command			X	
PRC	Propulsion remote control status	X			
RLM	Return link message	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			
RRT	Report route transfer	X			
RSA	Rudder sensor angle	X			
RSD	Radar system data	X			
RTE	Routes	X			
SEL	Selection report	X			
SFI	Scanning frequency information	X			
SLM	Steering location/mode	X			
SM1	SafetyNET message, All ships/NavArea	X			
SM2	SafetyNET message, Coastal warning area	X			
SM3	SafetyNET message, Circular area address	X			
SM4	SafetyNET message, Rectangular area address	X			
SMB	IMO SafetyNET message body	X			
SMV	SafetyNET message, Vessel in distress information	X			
SPW	Security password sentence		X		
SRP	System function ID resolution protocol	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

	Description	SBM	MSM	CRP	Related sentence formatters
TRD	Thruster response data	X			TRC
TRL	AIS transmitter-non-functioning log	X			
TTD	Tracked Target Data		X		
TTM	Tracked target message	X			
TUT	Transmission of multi-language text		X		
TXT	Text transmission		X		Sometimes single
UID	User identification code transmission	X			
VBC	Water-referenced and ground-referenced docking speed data	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		Sometimes single
VDR	Set and drift	X			
VER	Version		X	X	Sometimes single
VHW	Water speed and heading	X			
VLW	Dual ground/water distance	X			
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
(normative)

TAG block definitions

B.1 Validity

The material in Annex B is a subset of a definition of a parameter structure from NMEA 0183 intended for adding information to IEC 61162-1 sentences. Conformance with this document on the sending side will guarantee conformance to NMEA 0183, but the description herein is not complete and a receiver that only implements Annex B will not be able to process all valid TAG block structures.

B.2 Valid TAG block characters

The "\" (back-slash) character is designated as the "TAG block delimiter". A TAG block shall begin and end with a TAG block delimiter.

The closing delimiter character is always preceded by the checksum (*hh) of the TAG block content. The TAG block closing "\" appears before a symbol beginning a sentence, either a "$" or "!"; another Tag Block, "\"; or the <CR><LF> symbols.

The beginning TAG block "\" symbol shall follow the "<CR><LF>" symbols at the end of the preceding sentence or before any other character is transmitted.

The maximum number of characters in a TAG block shall be 80 characters including the TAG block delimiters.

IEC 61162-1 requires that the maximum number of characters in a sentence shall be 79 characters between the starting delimiter "$" or "!" and terminating delimiter <CR><LF>. The "$" or "!" is always recognized as the beginning of an IEC 61162-1 sentence. The character content of a TAG block, plus the TAG block delimiters, is not included in the sentence character count.

The contents of the TAG block (valid characters between the two "\" characters) may contain any valid character (see "Valid characters" table in IEC 61162-1) and some of the reserved characters (see "Reserved characters" table in IEC 61162-1).

The TAG block shall not contain either the TAG block delimiter, or the start of sentence delimiters, "$" or "!", or characters reserved for future use; the "~" or <del> characters.

The remaining reserved characters (<CR>, <LF>, ",", "*", and "^", found in the "Reserved characters" table in IEC 61162-1) shall be used as defined in IEC 61162-1.

Additional rules are described in Clause B.3.

B.3 TAG block format

Each TAG block may contain one or more parameters consisting of a "parameter-code" and "parameter value." Each parameter value may be either a numeric value or a character string constructed of valid IEC 61162-1 characters as discussed in Clause B.2. The parameter-code consists of alphabetic characters only. Parameter-code and parameter value are separated by a colon (":").

The syntax for a TAG block is described below, in Extended Backus-Naur Form (EBNF) notation. The format is the same as that used in the XML specification and a brief explanation is given below.

parameterCode::= [a-zA-Z0-9]+

numericValue::= '-'? [0-9]+ ('.'[0-9]+)?

characterString::= [-. A-Za-z0-9]+

checksum::= [0-9A-F] [0-9A-F]

parameterPair::= parameterCode ':' (numericValue | characterString)

parameterList::= parameterList ',' parameterPair | parameterPair

TagBlock::= '\' parameterList '*' checkSum '\'

An additional constraint for the TAG block is that it shall be 80 or less characters long. When it appears, it shall be followed by another TAG block, a valid IEC 61162-1 sentence or a carriage return and line feed pair.

Two examples of syntactically valid TAG blocks are listed below:

\a:0.23,b:All the kings men – but jack.,c:-23*hh\

\d:A*hh\

A brief description of the EBNF notation follows below. The complete description can be found in W3C XML.

Any character in single quotes is itself, i.e., ':' is just a colon.

The square brackets denote exactly one character from the set of characters listed within. The dash ("-"), unless appearing as the first character, defines a range of characters, i.e. "[0-9A-F]", is one character in the range zero to nine or A to F. A dash as the first character represents itself in the selection.

The plus sign means that the immediately preceding character can be repeated one or more times. Thus, "[0-9]+" specifies a integer number, possibly with leading zeros.

The vertical bar ("|") specifies a selection. Either the left or right hand side expression is valid.

Ordinary parentheses group an expression and can be used in conjunction with the plus sign or the horizontal bar.

B.4 TAG block "hexadecimal checksum" (*hh)

In order to improve the integrity of the parameters in a TAG block, the "Exclusive OR" hexadecimal checksum (*hh), that is calculated for every IEC 61162-1 sentence shall also be used for the content of each TAG block. The checksum is the 8-bit Exclusive OR (no start or stop bits) of all characters in the TAG block, including the "," and "^" delimiters, between but not including the beginning "\" character and the "*" checksum delimiter.

B.5 TAG block "line"

A TAG block "line" can be formed in three ways.

1) The TAG block can appear alone to form a "line".
2) The TAG block may precede a sentence to form a "line" with an associated IEC 61162-1 sentence.

3) Multiple TAG blocks may appear one after another to form a "line" or they may precede a sentence to form a "line" with an associated IEC 61162-1 sentence.

A TAG block "line" is only valid when either a <CR><LF> immediately follows the last TAG block closing "\" symbol, or when a valid IEC 61162-1 sentence immediately follows the TAG block closing "\" symbol. TAG blocks are linked with a sentence when no <CR><LF> or any characters separate the TAG block and sentence.

B.6 TAG block parameter-code dictionary

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

Table B.1 – Defined parameter-codes

Parameter-code	Description	Form of parameter value
a	General authentication	Alphanumeric string (32 char. maximum)
c	POSIX time	Positive integer
d	Destination-identification	Alphanumeric string (15 char. maximum)
g	Sentence-grouping	Grouped numeric string (alphanumeric)
n	Line-count	Positive integer
r	Relative time	Positive integer
s	Source-identification	Alphanumeric string (15 char. maximum)
t	Text	Free text, including proprietary information
x	Destination cluster identification	Alphanumeric string (3 char.)
z	Source cluster identification	Alphanumeric string (3 char.)

Annex C
(normative)

Reliable transmission of command-response pair messages

C.1 Purpose

The rules that are listed in Annex C 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.

The requirements of Annex C are not applicable for SNGF and PNGF as they only act as converter between original sender and original receiver(s).

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, and
- 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.

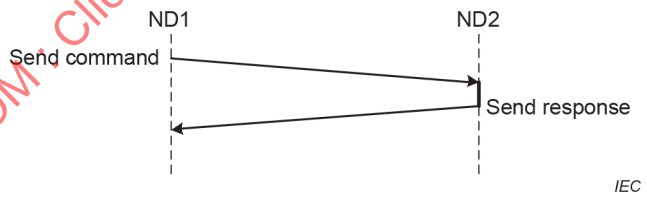


Figure C.1 – Command response communications

C.4 Requirements

The requirements for reliable communication are the following:

- 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;
- optionally, TAG block parameter "n" may be used to assign a sequence number to each sentence transmitted from a system function block;
- 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. It shall be sent by each node 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>
```

Annex D
(informative)

Compatibility between nodes based on IEC 61162-450:2011 connected to a network which uses methods based on later editions of IEC 61162-450

D.1 General

The hosts (i.e. nodes) in IEC 61162-450:2011 are not required to implement IGMP protocol. When the IGMP snooping introduced in IEC 61162-450:2018 is enabled, a switch snoops IGMP join message for multicast groups and maintains per port information of multicast groups into which the port belongs. When a multicast message is received, the IGMP enabled switch forwards the message only to ports which belong to this multicast group. Since the multicast traffic filtering at the switch is based on the snooping of IGMP join messages, the nodes of IEC 61162-450:2011, which do not implement IGMP protocol, will not receive the IEC 61162-450 traffic. The IGMP snooping prevents only reception of the messages. It does not cause any problem for the transmission of the messages by the node.

D.2 Alternative methods for compatibility

D.2.1 Use of IGMP proxy node

One method for a node based on IEC 61162-450:2011, which is non-IGMP capable, to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is IGMP proxy node.

When switches are enabled to do IGMP snooping, there is no way to receive multicasting messages without sending an IGMP join message from the node to the switch. A special node, an IGMP proxy node, which sends an IGMP join (and IGMP leave) message instead of the non-IGMP capable node is required to be between the node and the switch. This means that all non-IGMP capable nodes should be connected to an IGMP snooping enabled switch through a virtual IGMP agent. An IGMP proxy node collects the multicast membership information from the non-IGMP capable network (automatically or by configuration), and sends IGMP join (and maybe IGMP leave) messages periodically for the detected multicast groups. The IGMP proxy node also replies to IGMP membership report requests from the switch.

D.2.2 Use of virtual LAN (VLAN)

D.2.2.1 Method

Another method for a node based on IEC 61162-450:2011, which is non-IGMP capable, to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is VLAN.

IGMP snooping could be configured with per VLAN at a switch. This is only related with the setup of the switch and requires nothing to do with the node. When a port at a switch is connected directly or indirectly to nodes with non-IGMP capable nodes, then the ports are allocated the specific VLAN ID(s), which is configured to disable the IGMP snooping. The system designer or integrator may assign a special VLAN ID for the non-IGMP capable nodes in the networks.

VLAN can be used to avoid the burden of receiving all binary file transfers from ports in Table 5. A VLAN ID can be assigned to each binary file transfer port or some ports of the binary file transfer. This means that the system integrator could plan the system so that binary file transfers are not shared by all users who are not interested in the binary file transfers.

D.2.2.2 Requirements for switches

The following are required at a switch to support IGMP snooping compatibility based on VLAN:

a) means to configure VLAN for each Ethernet port;

b) means to enable or to disable IGMP snooping per each VLAN.

D.2.3 Use of static multicast switch configuration

A third method for a node based on IEC 61162-450:2011 which is non-IGMP capable to receive the multicasting messages when IGMP snooping is enabled in the IEC 61162-450:2018 network is to use static multicast switch configuration.

Managed switches typically provide the ability to define at switch port level which ports will receive data from multicast groups. This is often referred to as static multicast or static multicast routing and involves configuring the IP/MAC address of a multicast group to which a non-IGMP capable device wishes to receive data from and associating it with the network port of the device on the switch. As multicast data is received at the IP/MAC address on the switch, it is provided to the device without any explicit IGMP join requests.

Annex E
(informative)

Use of switch setup configuration to filter network traffic

Typically, a simple network consisting of only IEC 61162-1 sentences and screen capture images from radars and ECDIS to VDR, and ECDIS route exchange transmitted over LAN using IEC 61162-450 protocol would not need any filtering of the network traffic. Often, there is a need to share the same LAN infrastructure for things like raw radar video, CCTV pictures, transfer of SENC databases, etc. Such additional traffic is defined as ONF by this document. The issue is that such additional traffic may cause too high a CPU load for some of the simple nodes connected to the shared network infrastructure. There are many possibilities to address the issue of the filtering of the network traffic.

Annex E explains one family of methods. This family of methods uses network infrastructure elements, namely switches, to perform the filtering.

One method to filter or control network traffic is to use setup configuration of the managed switches. Such setup would typically allow traffic filtering based on any combination of

- the physical port,
- the logical port number,
- the protocol type,
- the source IP address,
- the source MAC address,
- the destination IP address,
- the destination MAC address, and
- the VLAN.

There are no international standards by IEEE, IETF, etc. to do this setup, but there is a de facto method called Access Control List (ACL). Typical of all methods used to control the setup is that the setup configuration can be stored as a simple text file which could be fed by a computer into the switch. Therefore, such methods offer a high level of manageability for an organization that makes system design or service and support (for example a company could create an environment in which experts prepare setup configurations as files, the setup files are centrally stored to be available in a cloud and the service and support persons can utilize these setup files while performing service and support).

Annex F
(normative)

Sentence to support SFI collision detection

F.1 General

Annex F describes details of a sentence used to support implementation of a network.

NOTE Refer to IEC 61162-1 for possible later versions of this sentence.

F.2 SRP – System function ID resolution protocol

This sentence is used to assist detection of possible system function ID (SFI) collision.

This sentence is transmitted as specified in this document (see 7.5). This sentence cannot be queried.

```
\s:ccxxxx*hh\$--SRP,x,hhhhhhhhhhhh,c--c*hh<CR><LF>
     |                 |       |          |
     |                 |       |          └─ IP address 4)
     |                 |       └─ MAC address 3)
     |                 └─ Instance number 2)
     └─ SFI of the transmitter 1)
```

Comments:

1) Reported SFI of the transmitter.
2) Instance number for available interfaces with the same SFI (i.e. number of physical port for identical SFI), null field if there is only one interface with identical SFI available. In case there is more than one interface using intentionally the identical SFI, the numbering starts with 1. The instance numbers shall be ordinal with no skipping (1, 2, 3, etc.).
3) Reported MAC address used by SFI, 48bit hexadecimal number, for example 32613C4EB605.
4) Reported IP address used by SFI as text string, for example 192.168.0.10.

Annex G
(informative)

Examples for SRP sentences and SFI collision detection

G.1 SFI collision detection

For the case where, in two SRP messages, the pair of SFI and instance number is equal and the pair of MAC address and the IP address is deviating, there is a (potential) conflict of SFI numbering in the system.

There could be at least three kinds of redundancy:

a) redundancy based on multiple SF available in a single network for the same purpose;

b) redundancy based on reuse of SFI but using separate MAC addresses;

c) redundancy based on multiple isolated networks.

The SFI collision detection is intended to detect conflicts within a single network. Multiple isolated networks may or may not reuse the same SFI value, see 4.4.2.

A potential SFI collision is detected within a single network when in two SRP messages the pair of SFI and instance number is equal and the MAC address or the IP address is not equal.

There could be also a need to use separate physical interfaces for different but related purposes for which there is a need to use a common SFI. For example, traffic related to the functionality of the equipment and traffic related to alert management could be available from separate physical interfaces. This could be the case for all physical interface types, but it is assumed that this is more common in the case of physical interfaces based on serial lines, for example IEC 61162-1 or IEC 61162-2.

G.2 Examples for SRP sentences

G.2.1 Redundancy on network level only

G.2.1.1 Two network interfaces provide the same information

In this use case there are two separate network interfaces connected to the same single network, see Figure G.1.

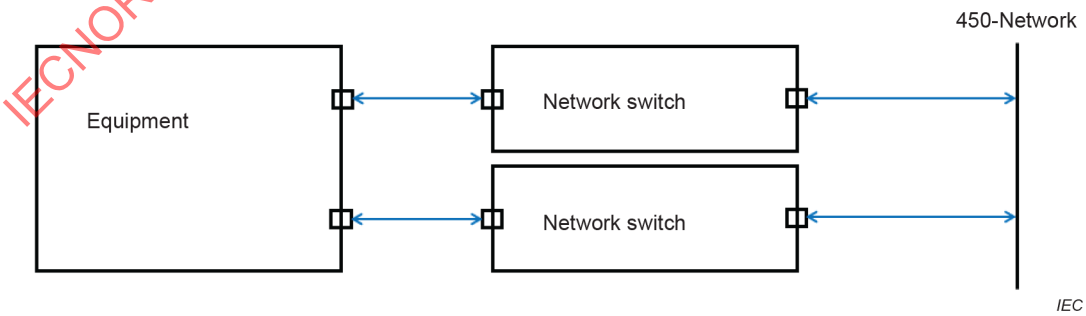


Figure G.1 – Two separate network interfaces connected to the same single network

Two active physical network interfaces with identical payload in data transfer. No link aggregation (also known as teaming/bonding, see G.2.1.3) is present. The EUT sends the same packet but either with the same source IP address or a different source IP address or a different source parameter code or some combination from each connected network interface to the same multicast group. The receiving device decides which of two identical packets to process and which should be discarded.

The data is transmitted on the same IEC 61162-450 network.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.1) both reporting using two physical interface, see Figure G.2. No SFI collision.

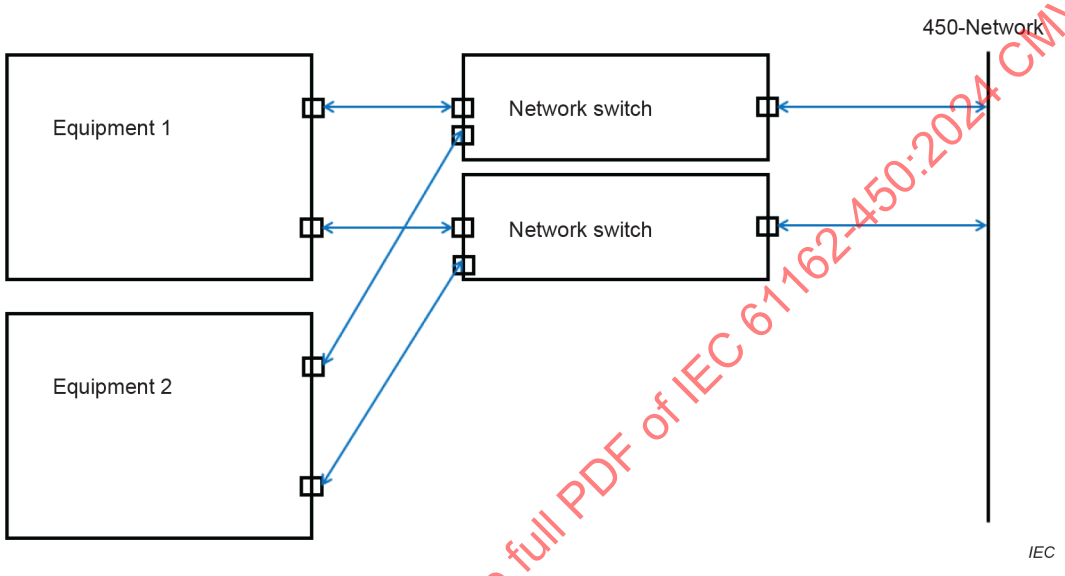


Figure G.2 – An example of two equipment

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0002*5C\$GPSRP,1,02004F68901C,192.168.0.21*46<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0002*5C\$GPSRP,2,02003D41FCB3,192.168.0.22*47<CR><LF>
```

- Example 2: two equipment both reporting using two physical interface, see Figure G.2. SFI collision as same SFI is shared by two separate equipment:

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0001*5F\$GPSRP,1,05A3CE170137,192.168.0.53*34<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0001*5F\$GPSRP,2,86FD61AC2802,192.168.0.30*41<CR><LF>
```

G.2.1.2 Two network interfaces provide the same information

This style may be called link, teaming, etc.

In this use case, there are two separate networks interfaces connected to the same single network but only one of the network interfaces is sending at any one time (this sending is controlled by the equipment), see Figure G.3.

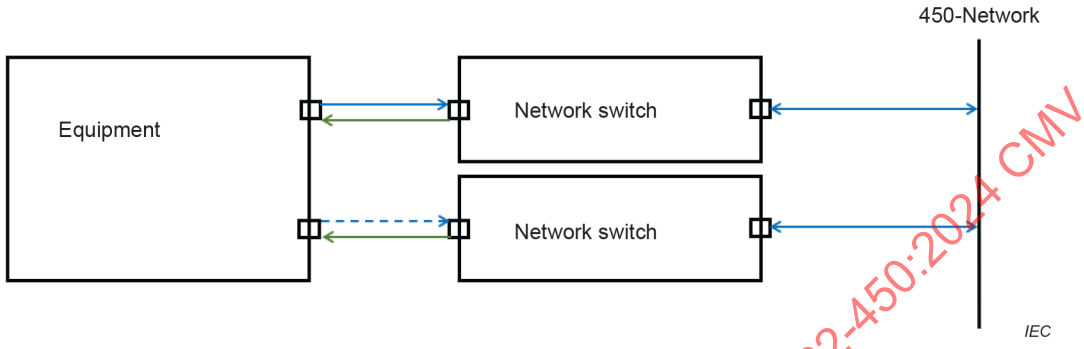


Figure G.3 – Two separate networks interfaces connected to the same single network, but only one of the network interfaces is sending at any one time

Both physical interfaces of the equipment provides/processes identical information. To the receiving equipment in the network, the equipment is identified as only "one connection". A switching over between the separate physical interfaces to be sender is managed by the equipment based on missing traffic from one of the physical interfaces.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.3) both reporting using two physical interface, see Figure G.4. No SFI collision.

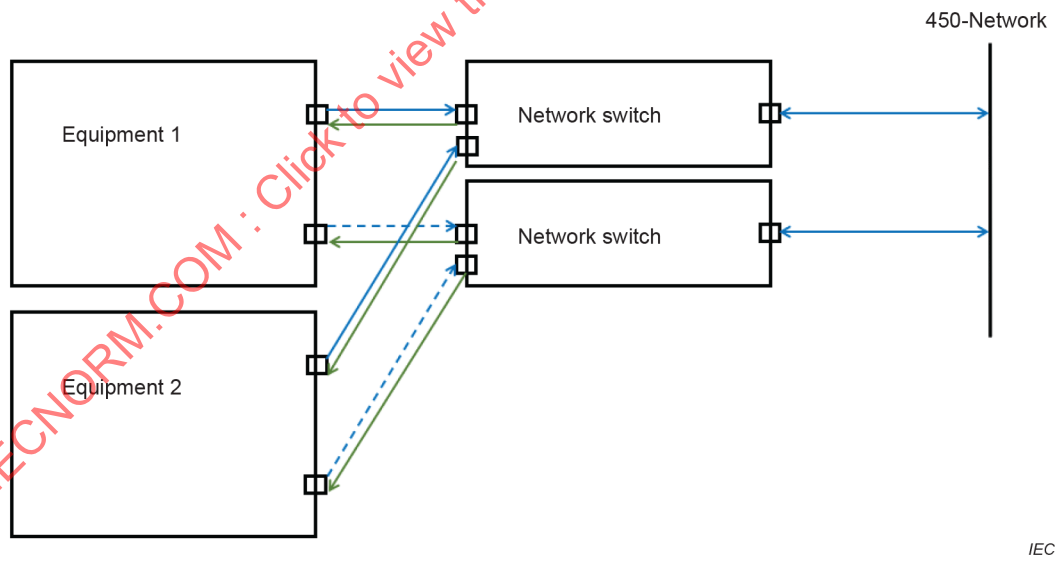


Figure G.4 – An example of two equipment

SRP equipment 1, interface 1. Note that, if this is sent, then interface 2 is not sending.

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2. Note that, if this is sent, then interface 1 is not sending

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1. Note that, if this is sent, then interface 2 is not sending

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

SRP equipment 2, interface 2. Note that, if this is sent, then interface 1 is not sending

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

- Example 2: two equipment (i.e. two sets of the cases in Figure G.3) both reporting using two physical interface, see Figure G.4. SFI collision occurs as the same SFI is shared by two separate equipment.

  Equal SFI on all interfaces, for equipment 2 deviating pair of MAC address and IP address

  SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

  SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

  SRP equipment 2, interface 1

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

  SRP equipment 2, interface 2

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

G.2.1.3 Link aggregation/teaming mode

In this use case, there are two separate network interfaces connected to the same single network, but a network switch controls the traffic so that the equipment is seen as one interface, see Figure G.5.

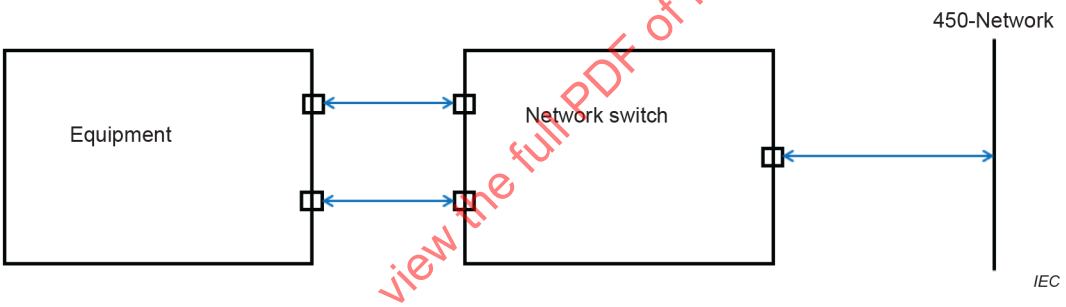


Figure G.5 – Two separate network interfaces connected to the same single network but a network switch makes the equipment to be seen as one

Both physical interfaces of the equipment provide/process identical information. To the equipment in the network, the equipment is identified as only "one connection". A network switch manages that the equipment is seen as one logical interface. Note that traffic from both physical interfaces of the equipment is available in the network.

- Example 1: two equipment (i.e. two sets of the cases in Figure G.5) both reporting using two physical interfaces, see Figure G.6. No SFI collision.

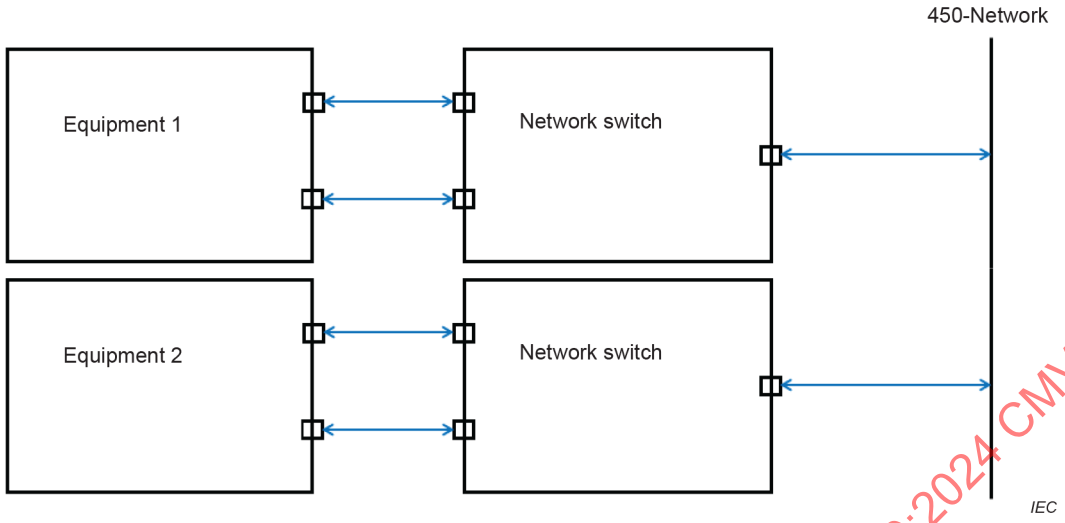


Figure G.6 – An example of two equipment

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0002*5C\$GPSRP,,02004F68901C,192.168.0.21*77<CR><LF>
```

- Example 2: two equipment (i.e. two sets of the cases in Figure G.5) both reporting using two physical interface, see Figure G.6. SFI collision occurs as the same SFI is shared by two separate equipment.

SRP equipment 1, interface 1

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 1, interface 2

```
\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>
```

SRP equipment 2, interface 1

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

SRP equipment 2, interface 2

```
\s:GP0001*5F\$GPSRP,,05A3CE170137,192.168.0.53*05<CR><LF>
```

G.2.2 Examples for redundancy on network and serial (to network) level

G.2.2.1 One equipment with redundant serial interfaces is connected to two different SNGFs

In this use case, there are two separate serial interfaces connected through two separate SNGF to the same single network, see Figure G.7.

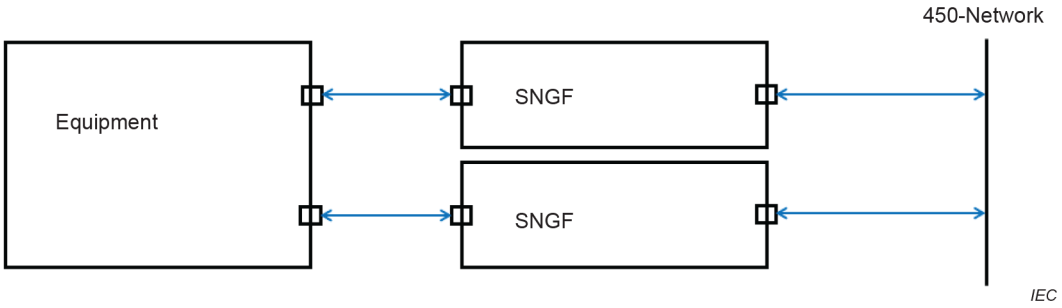


Figure G.7 – One equipment with two separate serial interfaces connected through separate SNGFs to the network

Two active physical serial interfaces with identical data transfer. The recipient can decide which channel he would like to process. For redundancy reasons, it is connected to two SNGFs. The two SNGFs distribute the identical information with the same SFI to the network. The combination of two source parameter codes "s" is unique within the 450-Network.

- EXAMPLE 1: one equipment reporting using two physical interfaces, see Figure G.7. No SFI collision:

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\\s:SI0001*hh\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\\s:SI0002*hh\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>`

  NOTE Although the second interface is providing the same serial line information, it is important that the instance number on SNGF 2 for the second serial interface is increased. Otherwise, the SFI failure detection will detect a SFI configuration error. The processing of redundant serial line information needs to be handled on system integration level by the recipient.

- Example 2: one equipment reporting using two physical interfaces, see Figure G.7. SFI collision as instance numbers of the SFI are not available (instance number-field is null):

  Correctly equal SFI on all interfaces and deviating pair of MAC address and IP address for the SNGFs, but null fields in the instance fields.

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\$GPSRP,,0091A5814187,192.168.0.12*0D<CR><LF>`

G.2.2.2 One data source has two different serial interfaces on which it provides different information to different SNGFs

In this use case, there are two separate serial interfaces connected through two separate SNGF to the same single network, see Figure G.7.

Two active physical serial interfaces with different information, e.g., one for data and another for BAM. Both are connected to different SNGFs.

NOTE 1 The case that one data source (device) provides different information on separate serial lines to one SNGF needs to be handled by this SNGF.

- Example 1: one equipment reporting using two physical interfaces, see Figure G.7. No SFI collision:

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\$GPSRP,1,0091A581E364,192.168.0.11*41<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\$GPSRP,2,0091A5814187,192.168.0.12*3F<CR><LF>`

NOTE 2 It is important that the instance number on SNGF 2 for the second serial interface is increased. Otherwise, the SFI failure detection will detect a SFI configuration error. The processing of redundant serial line information needs to be handled on system integration level.

- Example 2: one equipment reporting using two physical interfaces, see Figure G.7. SFI collision as instance numbers of the SFI are not available (instance number-field is null):

  SRP SNGF 1, (serial interface 1)

  `\s:GP0001*5F\$GPSRP,,0091A581E364,192.168.0.11*70<CR><LF>`

  SRP SNGF 2, (serial interface 2)

  `\s:GP0001*5F\$GPSRP,,0091A5814187,192.168.0.12*0D<CR><LF>`

G.3 Other uses of SRP sentence

When a source is redundantly available and redundant traffic is identified by the instance numbers. It is possible to monitor the correct configuration or healthy of the source.

If in this case, there is a SRP message with a SFI and instance ‘1’ and a corresponding SRP message with an instance ‘2’ is missing:

- the device with instance ‘2’ is switched off, is defective (i.e. unhealthy); or
- the device transmitting instance ‘1’ is wrongly configured and has to send a null field in the instance field.

If in this case, there is a SRP message with a SFI and instance ‘2’ and a corresponding SRP message with an instance ‘1’ is missing:

- the device with instance ‘1’ is switched off, is defective (i.e. unhealthy); or
- the device transmitting instance ‘2’ is wrongly configured and has to send a null field in the instance field.

Annex H
(normative)

Reserved cluster identifiers

The reserved cluster identifiers are specified in Table H.1.

Table H.1 – List of reserved cluster identifiers

Identifier	Cluster name	Description	Operator (example)
Nav	Navigation	Navigation bridge	Navigator
Com	Communication	Ship's communication	Radio operator
Aut	Automation	Engine room domain	Engineer
Cgo	Cargo	Regarding the payload of the ship	Chief officer/Supercargo
Htl	Hotel	Passenger related services	Hotel manager (passenger vessels)
ICT	ICT	Office network	ICT manager
SSe	Safety/Security	Access monitoring	Ship security officer
Pos	Position control	Dynamic position or mooring control	DP/mooring operator
ROV	Remote operated vehicle	ROV control centre	ROV operator

Bibliography

IEC 60603-7:2020, *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 61162-450:2011, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*[2]

IEC 61162-460, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security*

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 interconnecting devices and passive components – 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: 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, *Information technology – Generic cabling for customer premises*

ISO/IEC 8859-1, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*

ITU-R Recommendation M.1371, *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile band*

IEEE 802, *IEEE standard for local and metropolitan area networks: Overview and architecture*

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

ISOC RFC 793, *Transmission control protocol*

2 This publication has been withdrawn.

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

ISOC RFC 966, *Host Groups: A Multicast Extension to the Internet Protocol*

ISOC RFC 1321, *The MD5 Message-Digest Algorithm*

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 4: Registration Procedures*

ISOC RFC 4541, *Internet Group Management Protocol (IGMP) and Multicast listener discovery (MLD) snooping switches*

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

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

ANSI/TIA-568, *Generic telecommunications cabling for customer premises*

TIA-604-10, *FOCIS10 – Fibre Optic Connector Intermatebility Standard, Type LC*

W3C Recommendation, *Extensive markup language (XML)*, 1.0 (fifth edition). Available at: http://www.w3.org/TR/REC-xml/

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

Partie 450: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 61162-450 a été établie par le comité d'études 80 de l'IEC: Matériels et systèmes de navigation et de radiocommunication maritimes. Il s'agit d'une Norme internationale.

Cette troisième édition annule et remplace la deuxième édition parue en 2018. Cette édition constitue une révision technique.

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

a) clarification de la fonction de passerelle série-réseau (SNGF) au 4.5 avec l'ajout de deux nouvelles figures;

b) ajout d'adresses de multidiffusion de destination et de numéros d'accès supplémentaires au 6.2;

c) clarification des paramètres du bloc TAG au 7.2 ainsi qu'à l'Annexe B, dans une nouvelle Annexe H et dans les essais associés au 8.9.4;

d) clarification du processus d'envoi des fichiers binaires au 7.3.6 et du processus de réception des fichiers binaires au 7.3.7 avec mise à jour de la Figure 6 et de la Figure 7;

e) clarification de la détection de collision du SFI et de l'utilisation de la sentence SRP au 7.5 ainsi que dans une nouvelle Annexe G;

f) révision des essais de traitement des données mal formées reçues sur la ligne série au 8.5.5.

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

Projet	Rapport de vote
80/1094/FDIS	80/1098/RVD

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

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

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

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

- reconduit,
- supprimé, ou
- révisé.

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

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

Partie 450: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet

1 Domaine d'application

La présente partie de l'IEC 61162 spécifie les exigences d'interface et les méthodes d'essai de la communication à grande vitesse entre les matériels de navigation et de radiocommunication embarqués, et entre ce type de système et d'autres systèmes de navigation qui nécessitent de communiquer avec les matériels de navigation et de radiocommunication. Le présent document repose sur l'application d'une série appropriée de Normes internationales existantes visant à définir le cadre de mise en œuvre du transfert de données entre les dispositifs sur un réseau Ethernet embarqué.

Le présent document spécifie un réseau de type bus Ethernet dans lequel un récepteur peut recevoir des messages d'un émetteur avec les propriétés suivantes.

- Le présent document comporte les dispositions en matière de distribution de multidiffusion des informations mises en forme selon l'IEC 61162-1 (relevés de position et autres mesurages, par exemple) et en matière de transmission de blocs de données générales (fichier binaire) entre un radar et un VDR, par exemple. Enfin, il contient les dispositions relatives à la distribution de multidiffusion des informations mises en forme selon l'IEC 61162-3 (relevés de position et autres mesurages, par exemple).
- Le présent document se limite aux protocoles pour les matériels (nœuds de réseau) connectés à un seul réseau Ethernet composé uniquement d'un ou de deux dispositifs et câbles de niveau OSI (Infrastructure de réseau).
- Le présent document fournit les exigences relatives aux interfaces de matériel uniquement. En spécifiant les protocoles de transmission des sentences IEC 61162-1, des messages PGN IEC 61162-3 et des données générales de fichier binaire, ces exigences assurent l'interopérabilité entre le matériel mettant en œuvre le présent document, ainsi qu'un certain niveau de comportement sûr du matériel lui-même.
- Le présent document permet au matériel utilisant d'autres protocoles que ceux qu'il spécifie de partager une infrastructure de réseau comportant des interfaces conformes aux exigences décrites pour l'ONF.
- Le présent document comporte les dispositions en matière de filtrage du trafic réseau afin de limiter la quantité de trafic à un niveau gérable par chaque matériel.

Le présent document ne comporte aucune exigence système autre que celles qui peuvent être déduites à partir de la somme des exigences relatives au matériel seul. La norme connexe IEC 61162-460 traite davantage des exigences système.

2 Références normatives

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

IEC 60825-2, *Sécurité des appareils à laser – Partie 2: Sécurité des systèmes de télécommunication par fibres optiques (STFO)*

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

IEC 61162-1, *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques – Partie 1: Émetteur unique et récepteurs multiples*

IEC 61162-3, *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques – Partie 3: Réseau par liaison de données série d'instruments*

IEEE Std 802.3-2022, *IEEE Standard for Ethernet*

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

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

ISOC RFC 826, *An ethernet Address Resolution Protocol*

ISOC RFC 1112, *Host Extensions for IP Multicasting, Standard STD0005 (and updates)* (inclut IGMP version 1)

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

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

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

ISOC RFC 3376, *Internet Group Management Protocol, Version 3*

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

ISOC RFC 5227, *IPv4 Address Conflict Detection*

ISOC RFC 5424, *The Syslog Protocol*

NOTE Les normes de l'Internet Society (ISOC) sont disponibles sur les sites web de l'IETF à l'adresse http://www.ietf.org. Les dernières mises à jour peuvent être consultées à l'adresse http://www.rfc-editor.org/rfcsearch.html.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

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

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

3.1
ASCII
caractère imprimable de 7 bits codé sur un octet

3.2
fichier binaire
bloc de données sans mise en forme connue de ce protocole (c'est-à-dire données non mises en forme selon l'IEC 61162-1) qui peut être transmis au moyen du protocole défini au 7.3 ou au 7.5

Note 1 à l'article: Le terme "fichier binaire" est utilisé pour distinguer le protocole de transfert de données générales (qui peut ne pas être au format texte ordinaire) de la transmission des sentences toujours au format ASCII 7 bits.

3.3
octet
groupe de 8 bits traité comme une seule unité

3.4
paire commande-réponse
CRP
messages échangés entre des parties qui synchronisent les changements d'état des deux côtés par l'échange

Note 1 à l'article: Les CRP sont définis à l'Annexe A.

Note 2 à l'article: Dans certains cas, les messages de commande et de réponse peuvent également être utilisés comme un message de diffusion de capteur. Par conséquent, la mise en œuvre de la sémantique de l'échange de message est, à certains égards, différente selon les utilisateurs qui participent à l'échange.

Note 3 à l'article: L'abréviation "CRP" est dérivée du terme anglais développé correspondant "command-response pair".

3.5
datagramme
unité de transmission UDP atomique sur Ethernet, définie dans l'ISOC RFC 768 et contrainte dans le présent document

3.6
Ethernet
norme de protocole de réseau local à accès multiple à écoute de porteuse avec détection de collision (CSMA/CD) définie dans l'IEEE Std 802.3 et les révisions et ajouts ultérieurs à l'IEEE 802

Note 1 à l'article: Les types de supports Ethernet qui peuvent être utilisés pour la mise en œuvre du présent document sont définis à l'Article 5.

3.7
bloc fonctionnel
fonctionnalité spécifiée mise en œuvre par le matériel

Note 1 à l'article: En principe, le matériel met en œuvre plusieurs blocs fonctionnels. Les exigences relatives au matériel sont égales à la somme des exigences relatives aux blocs fonctionnels qu'il met en œuvre. Les blocs fonctionnels sont définis à l'Article 4.

3.8
protocole Internet de gestion de groupe
IGMP
protocole de communication utilisé par les hôtes et les routeurs adjacents sur les réseaux IPv4 pour établir des adhésions à un groupe de multidiffusion

Note 1 à l'article: L'IGMP fait partie intégrante de la multidiffusion IP.

Note 2 à l'article: L'abréviation "IGMP" est dérivée du terme anglais développé correspondant "Internet Group Management Protocol".

3.9
surveillance du trafic IGMP
processus d'écoute du trafic réseau IGMP (protocole Internet de gestion de groupe)

3.10
Internet Assigned Number Authority
IANA
coordination globale de la racine du serveur de noms de domaine (DNS), de l'adressage IP et d'autres ressources de protocole Internet, y compris les numéros d'accès UDP et TCP

Note 1 à l'article: Les numéros actuellement attribués sont indiqués à l'adresse http://www.iana.org/assignments/port-numbers.

3.11
protocole Internet
IP
protocole de signalisation utilisé et défini dans l'ISOC RFC 791 (avec les mises à jour)

Note 1 à l'article: L'abréviation "IP" est dérivée du terme anglais développé correspondant "Internet protocol".

3.12
message
ensemble d'une ou de plusieurs sentences regroupées par l'emploi du protocole de regroupement de blocs TAG ou de mécanismes internes à la sentence, par exemple par numéros de séquence comme dans la sentence TXT

Note 1 à l'article: Une sentence autonome est un message.

3.13
type de message
classification des données de formatage de sentences IEC 61162-1 en types SBM, MSM et CRP

Note 1 à l'article: Les types SBM, MSM et CRP sont définis à l'Annexe A.

Note 2 à l'article: Le présent document définit différentes exigences en matière de transmission de différents types de messages.

3.14
message multisentences
MSM
groupe logique de messages et/ou de sentences dont la signification complète du groupe dépend du récepteur qui lit l'ensemble du groupe

Note 1 à l'article: Les messages multisentences qui sont regroupés avec une construction TAG sont également un groupe de sentences.

Note 2 à l'article: Les MSM sont définis à l'Annexe A.

Note 3 à l'article: L'abréviation "MSM" est dérivée du terme anglais développé correspondant "multi-sentence message".

3.15
réseau
réseau Ethernet physique avec un espace adresse Internet, uniquement composé de nœuds de réseau, de commutateurs, de câbles et de matériels (des blocs d'alimentation, par exemple)

3.16
bloc fonctionnel de réseau
NF
bloc fonctionnel chargé de la connectivité physique au réseau et de la connectivité à la couche de transport, comme cela est décrit au 4.3

Note 1 à l'article: L'abréviation "NF" est dérivée du terme anglais développé correspondant "network function block".

3.17
infrastructure réseau
partie du réseau qui fournit une voie de transmission entre les nœuds de réseau

Note 1 à l'article: Les nœuds de réseau ne font pas partie de l'infrastructure réseau.

3.18
nœud de réseau
dispositif physique connecté au réseau et qui dispose d'une adresse Internet

Note 1 à l'article: Un nœud de réseau est également appelé "hôte Internet".

Note 2 à l'article: Un nœud de réseau correspondant en principe au matériel. Ce dernier terme est utilisé dans le présent document.

3.19
autre bloc fonctionnel de réseau
ONF
bloc fonctionnel qui assure l'interface avec le réseau, mais qui n'utilise pas la définition de protocole de l'Article 5, de l'Article 6 et de l'Article 7

EXEMPLE Diffusion en continu et en temps réel de transfert d'image radar et CCTV ou de transfert de son VDR.

Note 1 à l'article: Les exigences définies au 4.7 permettent de s'assurer qu'un ONF peut cohabiter avec des nœuds de réseau SF et des blocs fonctionnels qui utilisent le protocole du présent document.

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

3.20
bloc fonctionnel de passerelle PGN/réseau
PNGF
bloc fonctionnel qui permet de transférer des sentences entre le réseau et les dispositifs conformes à l'interface de réseau d'instruments de données série IEC 61162-3

Note 1 à l'article: L'abréviation "PNGF" est dérivée du terme anglais développé correspondant "PGN to network gateway function block".

3.21
message PGN
message de numéro de groupe de paramètres
message composé d'un numéro à 8 bits ou 16 bits qui identifie chaque groupe de paramètres

Note 1 à l'article: Le numéro de groupe de paramètres (PGN) est analogue aux données de formatage de sentence à trois caractères de l'IEC 61162-1. Par définition, les groupes de paramètres identifiés par des numéros de groupes de paramètres à 16 bits sont diffusés vers toutes les adresses du réseau. Les groupes de paramètres identifiés par des numéros de groupes de paramètres à 8 bits peuvent être utilisés pour diriger les données vers une adresse spécifique.

Note 2 à l'article: L'abréviation "PGN" est dérivée du terme anglais développé correspondant "parameter group number".

[SOURCE: IEC 61162-3:2008, 3.1.21, modifié – Le mot "message" a été ajouté au terme, et la définition a été reformulée.]

3.22
message de diffusion de capteur
SBM
message composé d'une seule sentence

Note 1 à l'article: Les SBM sont envoyés avec un taux de mise à jour suffisamment important pour s'assurer que le récepteur peut maintenir un état correct, même au sein d'environnements dans lesquels certains messages peuvent être perdus.

Note 2 à l'article: Les SBM sont définis à l'Annexe A.

Note 3 à l'article: L'abréviation "SBM" est dérivée du terme anglais développé correspondant "sensor broadcast message".

3.23
sentence
unité de transport d'informations normalisée, décrite dans l'IEC 61162-1

3.24
groupe de sentences
groupe logique de sentences qu'il est nécessaire de traiter ensemble pour donner la signification complète des informations contenues dans la ou les sentences

Note 1 à l'article: Un groupe de sentences peut être composé d'une seule sentence.

Note 2 à l'article: Le regroupement de sentences en groupe de sentences est assuré par les mécanismes de bloc TAG.

Note 3 à l'article: Le présent document permet le regroupement explicite de sentences à l'aide d'un codage dans un datagramme. Le présent document n'établit aucune relation entre le datagramme et le groupe de sentences. Par conséquent, un datagramme peut contenir plusieurs groupes de sentences, ou un groupe de sentences peut être divisé en deux datagrammes ou plus.

3.25
bloc fonctionnel de passerelle série/réseau
SNGF
bloc fonctionnel qui permet de transférer des sentences entre le réseau et les dispositifs conformes aux interfaces de ligne en série IEC 61162-1 et IEC 61162-2

Note 1 à l'article: Un SNGF peut contenir plusieurs blocs fonctionnels de système qui ont chacun leur propre SFI. En outre, le SNGF lui-même possède un SFI pour des besoins administratifs.

Note 2 à l'article: L'abréviation "SNGF" est dérivée du terme anglais développé correspondant "serial to network gateway function block".

3.26
bloc fonctionnel de système
SF
bloc fonctionnel identifié par un ID de fonction système (SFI) unique, et qui est le seul bloc fonctionnel pouvant envoyer des informations dans le format de datagramme défini à l'Article 7

Note 1 à l'article: L'abréviation "SF" est dérivée du terme anglais développé correspondant "system function block".

3.27
ID de fonction système
SFI
chaîne de paramètres définie au 4.4.2

Note 1 à l'article: L'abréviation "SFI" est dérivée du terme anglais développé correspondant "system function ID".

3.28
groupe de transmission
paire adresse de multidiffusion/numéro d'accès utilisée par un SF pour émettre des sentences

Note 1 à l'article: Les groupes de transmission sont définis dans le Tableau 4, et l'Annexe A définit les groupes de transmission par défaut pour le SF.

3.29
annotation et groupe de transport
TAG
bloc de données mis en forme, défini dans la NMEA 0183, qui ajoute des paramètres aux sentences IEC 61162-1

Note 1 à l'article: L'Annexe B donne une vue d'ensemble des blocs TAG utilisés dans le présent document.

Note 2 à l'article: L'abréviation "TAG" est dérivée du terme anglais développé correspondant "transport annotate and group".

3.30
protocole de datagramme utilisateur
UDP
protocole de datagramme sans connexion défini par l'ISOC RFC 768

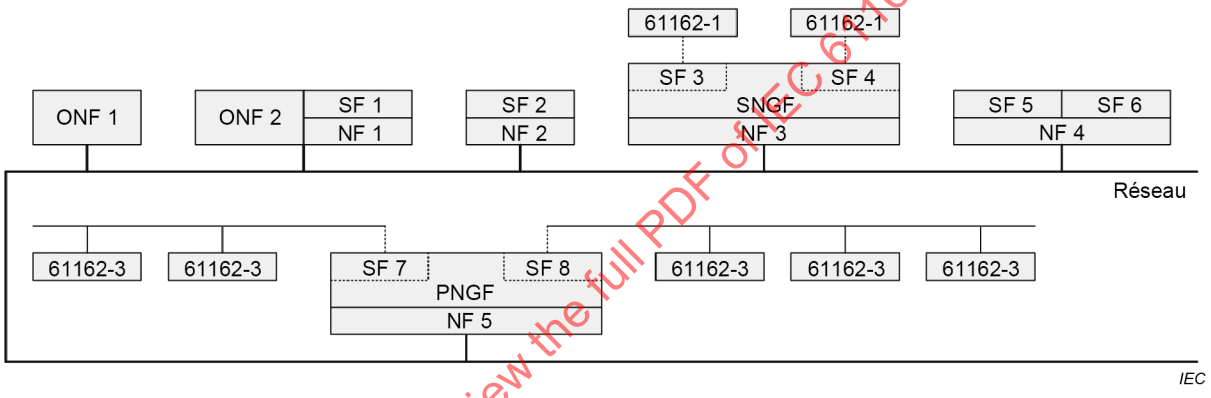
Note 1 à l'article: L'ISOC RFC 768 ne formule aucune disposition en matière d'acquittement de couche de transport des paquets reçus.

Note 2 à l'article: L'abréviation "UDP" est dérivée du terme anglais développé correspondant "user datagram protocol".

4 Exigences générales relatives au réseau et au matériel

4.1 Exemple de topologie de réseau

La Figure 1 représente une topologie de réseau IEC 61162-450 possible composée d'un réseau local (LAN) IP et d'un certain nombre de nœuds de réseau différents contenant chacun différents blocs fonctionnels. Ce schéma est informel et n'implique aucune autre exigence que celles définies à l'Article 4.



Légende

SF bloc fonctionnel de système
NF bloc fonctionnel de réseau
SNGF bloc fonctionnel de passerelle série/réseau
ONF autre bloc fonctionnel de réseau
PNGF bloc fonctionnel de passerelle PGN/réseau

Figure 1 – Exemple de topologie de réseau

Exemples de nœuds de réseau (voir la Figure 1):

- un capteur, par exemple un récepteur GNSS qui est également un nœud de réseau (SF2 et NF2);
- un dispositif qui envoie ou reçoit des données conformes à l'IEC 61162-450 (sentences et/ou fichier binaire) et d'autres types d'informations sur le réseau, par exemple un ECDIS qui peut également charger des données de carte provenant d'un autre dispositif (SF1, ONF2 et NF1);
- deux fonctions indépendantes, comme un compas gyroscopique également approuvé comme un capteur de vitesse angulaire mis en œuvre dans un nœud de réseau (SF5, SF6 et NF4);
- un bloc fonctionnel de dispositif du système représenté par un matériel conforme à l'IEC 61162-1 connecté à un bloc fonctionnel de passerelle série/réseau (SNGF). Dans ce cas, le SNGF met en forme les sentences sortantes selon les exigences du présent document (SF3, SF4, SNGF et NF3);

- un bloc fonctionnel de dispositif du système représenté par un matériel conforme à l'IEC 61162-3 connecté à une fonction de passerelle réseau (PNGF). Dans ce cas, le PNGF met en forme les sentences sortantes selon les exigences du présent document (SF7, SF8, PNGF et NF5);
- un dispositif qui n'envoie ni ne reçoit des données conformes à l'IEC 61162-450 (sentences et/ou fichier binaire), mais qui satisfait aux exigences minimales pour une utilisation compatible du même réseau (ONF1).

4.2 Exigences fondamentales

4.2.1 Exigences relatives aux matériels à connecter au réseau

(voir le 8.2.1)

Les exigences relatives aux matériels connectés au réseau sont les suivantes.

- Tous les matériels connectés au réseau, y compris les matériels d'infrastructure réseau, doivent satisfaire aux exigences physiques et électriques correspondantes définies au 5.1.
- Tous les matériels qui mettent en œuvre au moins un SF et/ou SNGF doivent mettre en œuvre le NF. Ces matériels doivent satisfaire aux exigences relatives aux blocs fonctionnels qu'ils mettent en œuvre définies au 4.3 (NF), au 4.4 (SF), au 4.5 (SNGF) et au 4.6 (PNGF).
- Tous les autres matériels qui ne sont pas des matériels d'infrastructure réseau et qui partagent cette infrastructure doivent satisfaire aux exigences relatives à un ONF définies au 4.7.
- Les matériels d'infrastructure réseau, c'est-à-dire les commutateurs, doivent satisfaire aux exigences définies au 4.2.2.
- Tous les matériels connectés à un réseau doivent satisfaire aux exigences de l'IEC 60945.

  NOTE Cette exigence s'applique uniquement aux dispositifs sur le réseau lorsque ce dernier fonctionne normalement. Lors de la mise en service ou de la maintenance, si le système n'est pas utilisé pour la navigation liée à la sécurité, d'autres matériels peuvent être provisoirement connectés au réseau sans être conformes à l'IEC 60945.

Tout autre matériel ne peut pas se connecter au réseau.

4.2.2 Exigences supplémentaires relatives aux matériels d'infrastructure réseau

(voir le 8.2.2)

Pour éviter d'éventuels problèmes avec certains matériels d'infrastructure réseau, des concentrateurs-répéteurs ne doivent pas être utilisés pour interconnecter des composants d'un réseau IEC 61162-450.

NOTE 1 Les concentrateurs-répéteurs sont des dispositifs d'infrastructure réseau sans stockage interne qui répètent les datagrammes entrants sur toutes les connexions sortantes.

NOTE 2 Les commutateurs sont des dispositifs d'infrastructure réseau reposant sur des tables de transfert, qui peuvent traiter et transférer des datagrammes entre des nœuds du même réseau au moyen d'un stockage intermédiaire dans le commutateur avant la retransmission.

Les commutateurs utilisés dans un réseau IEC 61162-450 doivent disposer des moyens de filtrage du trafic réseau à l'aide de la surveillance du trafic IGMP. Si la surveillance du trafic IGMP est activée et si un datagramme de multidiffusion est reçu, le commutateur doit le transférer uniquement sur les accès qui ont rejoint le même groupe de multidiffusion. Les moyens qui doivent être fournis pour assurer le filtrage des données de multidiffusion à l'aide de la surveillance du trafic IGMP sont les suivants:

- la surveillance du trafic IGMP doit être effectuée selon IGMPv1, IGMPv2 ou IGMPv3; la version IGMP doit être choisie en fonction de la version la plus élevée prise en charge par tous les nœuds connectés;

- le filtrage du trafic multidiffusion doit être effectué en fonction de l'adresse de multidiffusion IP;
- le filtrage de données de multidiffusion ne doit pas être activé pour la plage d'adresses comprise entre 224.0.0.1 et 224.0.0.255, comme cela est recommandé dans le document RFC 4541.

En plus ou à la place des techniques de filtrage de multidiffusion (surveillance du trafic IGMP, par exemple), il est également admis de configurer manuellement les différents accès des commutateurs pour bloquer le flux de trafic inutile (pour isoler les capteurs simples d'ECDIS et du radar, par exemple).

Voir l'Annexe D pour les questions de compatibilité de la surveillance du trafic IGMP des nœuds fondés sur l'IEC 61162-450:2011[1].

Une autre méthode possible de filtrage et de contrôle du trafic réseau est décrite à l'Annexe E.

4.3 Exigences de fonction de réseau (NF)

4.3.1 Exigences générales

Tous les matériels qui mettent en œuvre une fonction de réseau (NF) doivent satisfaire aux exigences définies à l'Article 5 et à l'Article 6.

4.3.2 Exigences de débit maximal des données

(voir le 8.3.1)

Le fabricant doit spécifier le débit d'entrée maximal auquel le matériel peut toujours exécuter l'ensemble des fonctions exigées par ses normes de performances, excepté dans le cas des normes de matériel pertinentes ou des fonctions spécifiées autrement par le fabricant.

Le débit d'entrée maximal doit être spécifié comme suit:

a) nombre maximal de datagrammes reçus par seconde, destinés au matériel et traités par celui-ci;

b) nombre maximal de datagrammes reçus par seconde, mais non destinés au matériel; et

c) nombre maximal de datagrammes reçus par seconde, mais non destinés au matériel, à 50 % de la charge maximale du point a).

NOTE 1 L'expression "reçus par" concerne les datagrammes reçus sur tous les groupes de transmission écoutés par le matériel.

NOTE 2 L'expression "destinés au" concerne les datagrammes traités par le matériel dans le cadre de sa fonction spécifiée.

Le débit maximal de données doit être le débit moyen sur une période de mesure de 10 s.

[1] Cette publication a été annulée.

4.3.3 Fonction de consignation des erreurs

(voir le 8.3.2)

4.3.3.1 Consignation interne

Des moyens doivent être prévus dans chaque NF afin de consigner les erreurs qui se produisent dans le NF lui-même et dans le SF et le SNGF qui l'utilisent. Les 4.5.2, 7.1.2, 7.2.5 et 7.3.9 spécifient les exigences minimales concernant les éléments qui doivent être consignés.

Le fabricant doit au moins fournir les mécanismes par lesquels un opérateur humain, par exemple un ingénieur de service formé, peut consulter les journaux d'erreurs. Il est admis de procéder à la consultation par un simple mécanisme de réseau, tel qu'un émulateur de terminal, comme cela est indiqué dans le présent document ou par toute autre méthode raisonnable.

Les exigences minimales relatives au journal concernent le comptage de chaque occurrence. Le compteur peut se remettre à zéro selon une méthode spécifiée par le fabricant.

4.3.3.2 Consignation externe

Un NF peut être configuré pour prendre en charge la consignation externe, lorsque des informations non essentielles sont envoyées à un serveur de consignation. Dans ce cas, un message "syslog" doit être utilisé, comme cela est indiqué dans l'ISOC RFC 5424.

Les messages syslog doivent être mis en forme comme des messages de texte ASCII et envoyés sous forme de paquets UDP sur l'accès 514 et à l'adresse de multidiffusion définie dans le Tableau 6. Les messages d'erreur définis dans le présent document doivent être consignés par l'intermédiaire d'un message simplifié, comme cela est décrit dans le Tableau 1, les mots en italique étant des espaces réservés pour les données expliquées dans la colonne de droite. Les autres caractères doivent être transmis de la manière indiquée, y compris les espaces.

Tableau 1 – Format de message syslog

Élément	Description
<pri>	Code de priorité et d'installation combiné (numéro entre 0 et 199 inclus) placé entre chevrons. Pour les erreurs définies dans le présent document, la valeur 131 doit être utilisée (installation "utilisation locale 0" et priorité "condition d'erreur").
Version	Code de version. Le code 1 (un) doit être utilisé pour les messages issus du présent document.
Space	Un caractère d'espace.
Timestamp	Horodatage contenant la date, l'heure et le décalage UTC facultatif, dans un format valide, par exemple 1985-04-12T23:20:50-03:00. L'exemple indique la date, suivie du "T" majuscule, puis de l'heure locale et enfin du décalage par rapport à UTC (3 h ouest – négatif, les décalages Est doivent être précédés du préfixe "+"; le décalage UTC peut être abrégé par un "Z" majuscule, sans "-" ou "+" de début). En variante, le champ d'horodatage peut être nul ("-", un tiret).
Space	Un caractère d'espace.
Hostname	Le nom d'hôte du nœud de réseau, représenté par l'adresse IP en notation décimale. En variante, ce champ peut être nul ("-", un tiret).
Space	Un caractère d'espace.
Appname	Nom de l'application. Il doit s'agir de la chaîne "450-" suivie du code SFI configuré si l'erreur provient de SF ou de SNGF, "NF" si l'erreur provient du bloc fonctionnel de réseau ou "ONF" si elle provient du bloc fonctionnel ONF.
Space	Un caractère d'espace.
Procid	En principe, il convient que ce champ soit nul ("-", un tiret). D'autres valeurs définies dans la norme syslog peuvent être utilisées.
Space	Un caractère d'espace.
Msgid	Pour les erreurs définies dans le présent document, ce champ doit contenir le code d'erreur défini dans le Tableau 2.
Space	Un caractère d'espace.
Structured	Ce champ peut être nul ("-", un tiret) ou contenir les informations définies dans l'ISOC RFC 5424.
Space	Un caractère d'espace.
Msg	Un message au format libre au format ASCII.
Les mots en italique sont des espaces réservés pour les données expliquées dans la colonne de droite.	

Un paquet "syslog" ne doit pas dépasser 480 octets et doit être envoyé sous la forme d'un simple datagramme UDP. Le paquet "syslog" correspondant à plusieurs occurrences de la même identité de message ne doit pas être consigné plus d'une fois par minute. Le paquet "syslog" correspondant à une occurrence de l'identité de message ne doit pas être retardé plus de 10 min.

Le présent document ne spécifie pas les exigences relatives aux matériels recevant les messages syslog. Ce type de matériel relève de la catégorie des ONF. Le Tableau 1 étant un sous-ensemble de la spécification ISOC RFC 5424 intégrale, les implémenteurs de tels matériels doivent se référer à l'ISOC RFC 5424 et s'assurer que les messages syslog provenant d'autres ONF puissent être reçus et traités sans problèmes.

Pour faciliter l'utilisation du protocole syslog, une identité de message a été attribuée aux erreurs définies dans le présent document, comme cela est indiqué dans le Tableau 2.

Tableau 2 – Codes de message d'erreur syslog

Identité de message	Description	Paragraphe
101	Dépassement de mémoire tampon SNGF	4.5.2
102	Erreur d'en-tête de datagramme	7.1.2
103	Erreur de format de bloc TAG ou de sentence	7.2.5
104	Erreur de fichier binaire	7.3.9
201	Dépassement de mémoire tampon PNGF	4.6.2
202	Erreurs de message PGN	7.4.2 et 7.4.4
203	Aucune adresse disponible pour les dispositifs	7.4.3.2

Des informations supplémentaires peuvent être données dans le champ "Msg", le cas échéant.

4.3.4 Dispositions en matière de filtrage du trafic réseau – IGMP

NOTE Pour le présent document, l'IGMP a pour objet d'offrir la possibilité de procéder à un filtrage du trafic réseau reposant sur la surveillance du trafic IGMP.

Le fabricant doit spécifier la version d'IGMP définie dans l'ISOC RFC 1112, l'ISOC RFC 2236 et l'ISOC RFC 3376 que le NF prend en charge. Au moins la version 1 définie dans l'ISOC RFC 1112 doit être mise en œuvre.

Voir l'Annexe D pour les questions de compatibilité des nœuds fondés sur l'IEC 61162-450:2011.

4.4 Exigences relatives au bloc fonctionnel de système (SF)

4.4.1 Exigences générales

(voir le 8.4.1 et le 8.2.3)

Le matériel qui met en œuvre un SF doit satisfaire aux exigences suivantes:

- les exigences définies au 6.2 doivent être respectées pour tous les matériels qui mettent en œuvre un SF;
- mise en œuvre d'au moins l'un des types de datagrammes définis à l'Article 7, sans avoir à mettre en œuvre la totalité d'entre eux;
- les types de datagrammes mis en œuvre doivent être spécifiés dans la documentation du fabricant (voir le 7.1.1);
- les exigences définies au 7.2 doivent être respectées pour tous les matériels qui mettent en œuvre la transmission de sentences IEC 61162-1 ou qui reçoivent des blocs fonctionnels;
- les exigences définies au 7.3 doivent être respectées pour les matériels qui mettent en œuvre un SF qui peut transmettre ou recevoir des données de fichier binaire;
- les exigences définies au 7.4 doivent être respectées pour tous les matériels qui mettent en œuvre la transmission de messages PGN IEC 61162-3 ou qui reçoivent des blocs fonctionnels.

4.4.2 Mise en œuvre de groupes de transmission configurables

(voir le 8.4.3)

Par défaut, un seul groupe de transmission/une seule adresse de multidiffusion doit être attribuée à chaque SF pour tous les messages sortants. La valeur par défaut de ce groupe de transmission est déterminée par le SFI, comme cela est décrit à l'Annexe A.

Pour chaque SF mis en œuvre par le matériel, le fabricant doit documenter les groupes de transmission par défaut que le SF écoute et indiquer les sentences qu'il prévoit de recevoir sur chaque groupe. Le fabricant peut choisir les groupes de transmission par défaut dans la liste des groupes du 6.2.2.

Des moyens doivent être prévus pour configurer tous les groupes de transmission et les SF qui leur sont attribués dans les limites de la plage valide des adresses de multidiffusion définie au 5.4. Un intégrateur de système peut, par exemple, diviser un SF en différents groupes de transmission pour assurer un équilibrage optimal des charges pour un système donné. Si des configurations de SF et des groupes de transmission personnalisés sont utilisés, il convient que l'intégrateur de système en précise les détails.

4.4.3 Attribution d'un ID de fonction système (SFI) unique

(voir le 8.4.2)

Le format de la chaîne de paramètres SFI doit être "ccxxxx", où "cc" correspond à deux caractères valides définis dans l'IEC 61162-1 et "xxxx" correspond à quatre caractères numériques.

Un SF qui met en œuvre la fonctionnalité d'un matériel auquel a été attribué un code mnémonique d'émetteur IEC 61162-1 doit utiliser ce code comme caractère "cc" dans le SFI. Si le code mnémonique d'émetteur est propriétaire (c'est-à-dire s'il est composé du caractère "P" suivi du code mnémonique du fabricant à trois caractères), les deux premiers caractères sont utilisés comme caractère "cc" dans le SFI.

Le format de chaîne SFI d'autres SF peut être défini dans d'autres normes ou le fabricant peut devoir choisir un code. Dans ce dernier cas, les codes mnémoniques d'émetteur déjà définis doivent être évités.

La chaîne de caractères numériques "xxxx" est un numéro d'instance compris entre "0001" et "9999". La chaîne de caractères numériques "9999" est réservée à un SF non configuré et ne doit pas être utilisée par un SF émetteur en fonctionnement normal. Toutefois, tous les matériels récepteurs doivent accepter la chaîne "9999".

En fonctionnement normal, la chaîne de paramètres SFI doit être unique pour tous les SF d'un réseau IEC 61162-450. Pour la mise en œuvre de la redondance d'interface (un dispositif unique est disponible à travers plusieurs voies dans le réseau), le SF et le SFI associé doivent être identiques. La combinaison de codes de paramètre source "s" doit être unique pour chaque voie (voir le 7.2.3.4).

Il est recommandé d'attribuer un SFI unique de navire à l'ensemble des SF d'un navire, qu'ils résident ou non sur un réseau commun.

Une seule adresse IP ou adresse MAC peut être attribuée à plusieurs SF, chacun communiquant avec son propre SFI.

Des moyens doivent être prévus par le fabricant pour configurer le SFI pour chaque SF (voir le 7.2.3.4).

4.5 Exigences de bloc fonctionnel de passerelle série/réseau (SNGF)

4.5.1 Exigences générales

(voir le 8.5.1)

Le SNGF doit mettre en œuvre l'ensemble des fonctionnalités pertinentes définies au 4.4 pour chaque SF qu'il prend en charge.

Le SNGF peut prendre en charge un ou plusieurs accès série (voir la Figure 2).

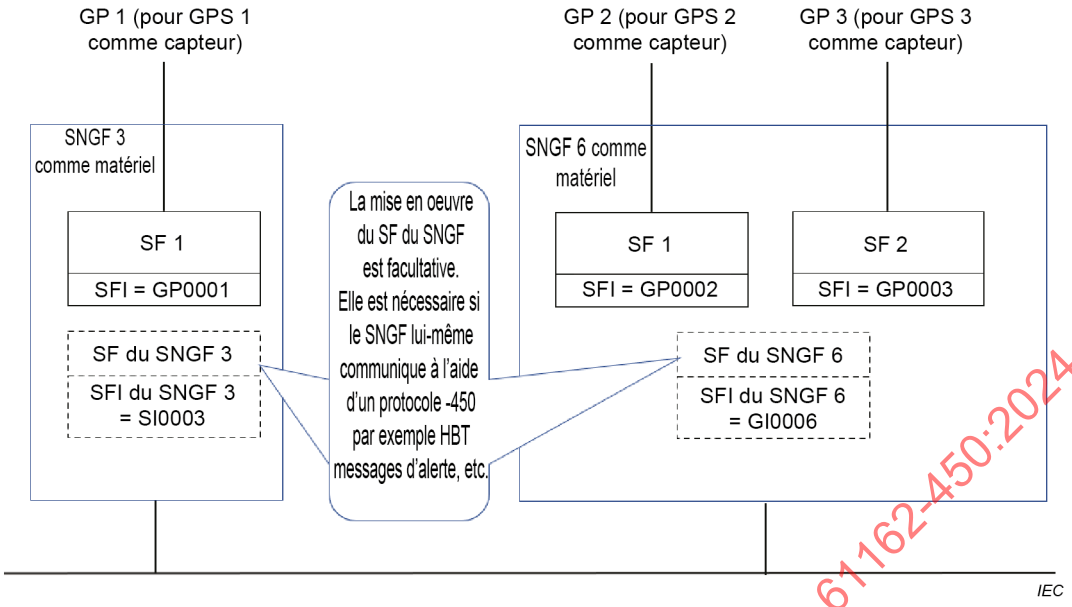


Figure 2 – Exemples de SNGF

Chaque accès série doit être mis en œuvre sous la forme d'un SF séparé et un SFI distinct doit lui être attribué, sauf si le SNGF met en œuvre un accès série multi-SF (voir le 4.5.4 et la Figure 3) ou si le SNGF met en œuvre la redondance d'interface. Dans la mesure du possible, la partie "cc" du SFI doit reposer sur l'identificateur d'émetteur utilisé par l'accès série. Sinon, un identificateur d'émetteur approprié doit être utilisé.

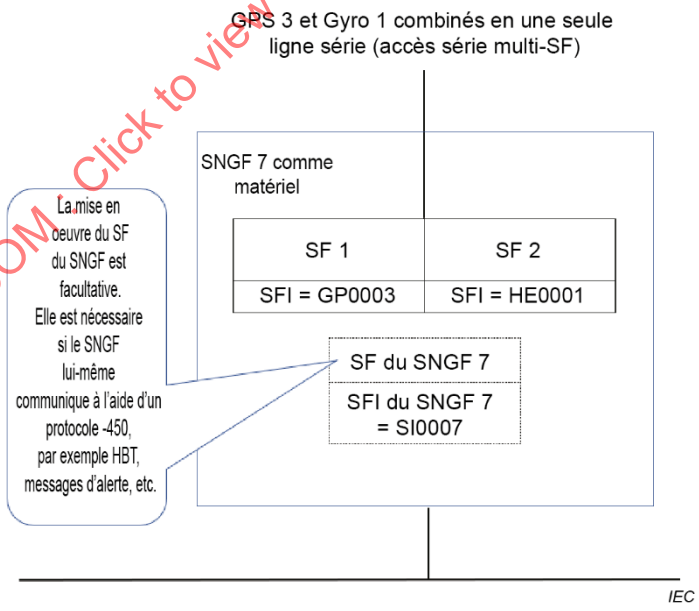


Figure 3 – Exemple de SNGF, accès série multi-SF

Le SNGF peut mettre en œuvre différents types de filtrages en fonction des sentences de ligne série retransmises sous forme de datagrammes et en fonction des datagrammes obtenus dans une sentence de ligne série envoyée. Toutes les méthodes de filtrage doivent être décrites dans le manuel d'installation.

NOTE Une méthode de filtrage classique consiste à utiliser le TAG de destination "d" pour déterminer les sentences des datagrammes entrants qui doivent être envoyées sur la ligne série.

Toutes les sentences, y compris celles au contenu non identifié ou illégal, ainsi que les sentences propriétaires, doivent être transmises, sauf en cas de filtrage, à partir du SF associé à l'accès série. Les sentences au contenu non identifié ou illégal doivent être envoyées avec un bloc annotation et groupe de transport (TAG) légal défini au 7.2.3, mais avec les données série reçues de la ligne suivant le bloc TAG.

En tant que destination, chaque accès série doit être associé au SFI correspondant. Les sentences sortantes doivent être transmises exactement telles qu'elles ont été reçues dans le datagramme.

Le SNGF peut prendre en charge une ou plusieurs sources se distinguant par différents codes mnémoniques d'émetteur au niveau de chaque accès série. Chaque source d'un accès série partagé doit être mise en œuvre sous la forme d'un SF séparé, et un SFI distinct doit lui être attribué. Dans la mesure du possible, la partie "cc" du SFI doit reposer sur le code mnémonique d'émetteur utilisé par chaque source d'un accès série partagé. En tant que destination, chaque source d'un accès série partagé doit reposer sur le SFI. Les sentences propriétaires ne contiennent aucun identificateur d'émetteur et, selon les paramètres de configuration, elles doivent utiliser le même SFI que les sentences normalisées provenant de la même source. La sentence STN est un qualificatif supplémentaire de la sentence suivante. La sentence STN et la sentence suivante appartiennent au même SF et doivent utiliser le même SFI.

Les sentences propriétaires reçues en provenance de l'accès série doivent être associées au SF de l'accès série selon:

- le code mnémonique d'émetteur utilisé par les sentences non propriétaires (voir l'alinéa précédent); ou
- le SF déterminé par la sentence STN précédente; ou
- en option, le SF défini par la configuration de l'accès série.

Les sentences mal formées (voir le 4.5.5) reçues en provenance d'un accès série doivent être associées au SF:

- s'il est disponible, du code mnémonique d'émetteur de la sentence mal formée; ou
- du code mnémonique d'émetteur utilisé par les sentences qui ne sont pas mal formées pour l'accès série; ou
- défini par la configuration pour les sentences mal formées.

Le fabricant doit déclarer dans le manuel d'installation les différentes méthodes qui ont été utilisées pour l'association au SF des sentences mal formées.

Le bloc TAG pour l'identification de la source "s" doit reposer sur le SFI. S'il est disponible, le routage entre un réseau et les accès série doit reposer sur le bloc TAG pour l'identification de la destination "d".

Le SFI d'un SNGF utilisé pour les besoins administratifs, par exemple syslog, heartbeat (HBT) du SNGF lui-même, etc., doit utiliser le code mnémonique d'émetteur "SI".

4.5.2 Gestion de la mémoire tampon de sortie de la ligne série

(voir le 8.5.2)

Un bloc fonctionnel SNGF doit fournir une mémoire tampon indépendante pour chaque SF séparé mis en œuvre pour chaque accès série par lequel il peut envoyer des sentences. Le fabricant doit spécifier la capacité maximale de mémoire tampon pour chaque accès. La capacité maximale peut être configurable au moment de l'installation.

La mémoire tampon doit être mise en place comme une mémoire tampon FIFO (*First In, First Out*, premier entré, premier sorti). Si la mémoire tampon est saturée, les dernières sentences arrivées doivent être ignorées, sauf si elles sont spécifiées comme étant prioritaires (voir ci-dessous). Les dernières sentences arrivées sont insérées dans la mémoire tampon si l'espace disponible le permet. La méthode de traitement des sentences regroupées par le TAG "g" (voir le 7.2.3.3) peut être configurable ou spécifiée dans la documentation du fabricant.

Le SNGF peut mettre en œuvre une fonctionnalité fondée sur la priorité pour certaines sentences avec les données de formatage de sentences spécifiées. Les données de formatage hiérarchisées peuvent être configurables ou spécifiées dans la documentation du fabricant.

Les sentences hiérarchisées doivent être traitées comme suit.

- La mémoire tampon ne doit contenir qu'une seule sentence avec un ID d'émetteur et une donnée de formatage de sentence uniques. Les messages multisentences ou les groupes de sentences du bloc TAG sont des exceptions: ils doivent uniquement être remplacés en totalité.

  NOTE Lors de la hiérarchisation des sentences SIA VDM et VDO, la chaîne commençant par le caractère "!" et se terminant par le 7^{e} caractère du champ d'encapsulation est utilisée en comparaison pour identifier les sentences identiques. Une correspondance de cette chaîne provenant d'une sentence récemment arrivée avec celle figurant dans la mémoire tampon indique que la sentence contient le même message UIT-R M.1371 provenant de la même MMSI que la sentence figurant déjà dans la mémoire tampon. Elle peut alors remplacer l'ancienne sentence à sa position dans la file d'attente.

- Si une seule sentence, un seul message multisentences ou des sentences regroupées dans un bloc TAG, dont l'ID d'émetteur et les données de formatage de sentences sont identiques, sont présents dans la mémoire tampon, la ou les nouvelles sentences remplacent la ou les sentences existantes à la position correspondante dans la file d'attente. Ce remplacement ne doit pas déclencher la consignation d'une erreur ni l'envoi d'éléments à syslog.

  Lors de la hiérarchisation des sentences regroupées dans un bloc TAG, il est nécessaire de comparer plusieurs champs du bloc TAG et de comparer les sentences. Il convient que tous les composants comparés correspondent à ceux du groupe de blocs TAG en cours afin de remplacer ce dernier dans la file d'attente. Les composants à comparer sont les suivants: la valeur de code du paramètre source du bloc TAG, la partie "nombre de lignes" du code du paramètre de groupe du bloc TAG et les sentences à l'intérieur du groupe de blocs TAG.

- Sinon, la nouvelle sentence doit respecter les principes FIFO décrits ci-dessus.

Si une sentence est écartée de la file d'attente, cet événement doit être consigné comme une erreur interne au matériel, comme cela est indiqué au 4.3.3. Le matériel doit disposer de moyens de comptage des erreurs distincts pour chaque accès série.

4.5.3 Exigences relatives à la sortie de datagramme

(voir le 8.5.3)

Le SNGF doit mettre en forme les datagrammes sortants, comme cela est indiqué au 7.2.

Le SNGF doit émettre une sentence IEC 61162-1 ou, s'il s'agit d'une partie d'une séquence multisentences, peut émettre plusieurs sentences IEC 61162-1 par datagramme IEC 61162-450 sortant. La séquence multisentences inclut le cas décrit dans l'IEC 61162-1 (Messages multisentences), et les cas pour lesquels l'IEC 61162-1 exige l'envoi d'une sentence avant l'envoi d'une autre sentence. Le datagramme doit inclure le SFI approprié, l'identification de la source (s:) et, si cela est exigé, l'identification de la destination (d:).

4.5.4 Accès série multi-SF

(voir le 8.5.4)

Le SNGF peut mettre en œuvre plusieurs SF pour une seule ligne série. Les sentences reçues sur cette ligne série avec un code mnémonique d'émetteur valide sont émises à partir de l'un des SF associés en fonction des codes mnémoniques d'émetteur. Un SFI distinct doit être attribué à chaque SF et, en tant que destination, chaque SF doit également émettre des sentences sortantes sur la ligne série conformément aux règles indiquées au 4.5.1.

Les sentences propriétaires reçues sur la ligne série ne contiennent aucun identificateur d'émetteur. Les paramètres de configuration doivent permettre de déterminer à partir de quel SF elles doivent être émises.

Les données non identifiées provenant de la ligne série doivent être envoyées à partir de tous les SF associés à l'accès série. Cet envoi de données non identifiées ne doit pas déclencher la consignation d'une erreur ni l'envoi d'éléments à syslog.

4.5.5 Traitement des données mal formées reçues sur la ligne série

(voir le 8.5.5)

Le SNGF est destiné à occuper la fonction de convertisseur de données série distant avec un traitement minimal des données. Pour chacun des cas ci-dessous, le SNGF doit envoyer un datagramme avec les données mal formées comme cela est exigé au 4.5.1 et au 4.5.4. Si le message mis en forme dépasse la longueur maximale du datagramme (voir le 6.2.4), les données doivent être tronquées à partir de la fin. Les cas suivants doivent générer un message contenant les données mal formées à envoyer:

1) si des données ont été reçues avant un caractère de début;
2) si des données ont été reçues après un caractère de début valide et si la longueur maximale de sentence et de bloc TAG a été dépassée;
3) si des données ont été reçues après un caractère de début valide et si la fin de ligne (CR,LF) n'a pas été reçue après 1 s;
4) si un caractère réservé a été reçu et n'a pas fait l'objet d'un échappement correct;
5) si des données binaires aléatoires ont été reçues sur la ligne série.

Le "caractère de début" est un début de sentence ("$", "!") ou un caractère de début de bloc TAG valide.

4.6 Exigences de bloc fonctionnel de passerelle PGN/réseau (PNGF)

(voir le 8.12)

4.6.1 Exigences générales

(voir le 8.12)

Le PNGF doit mettre en œuvre l'ensemble des fonctionnalités pertinentes définies au 4.4 pour chaque SF qu'il prend en charge.

Le SFI d'un PNGF utilisé pour les besoins administratifs, par exemple syslog, heartbeat (HBT) du PNGF lui-même, etc., doit utiliser le code mnémonique d'émetteur "SI".

Le PNGF peut mettre en œuvre différents types de filtrages, en fonction des messages PGN en provenance et à destination du réseau IEC 61162-3. Toutes les méthodes de filtrage doivent être décrites dans la documentation du fabricant.

NOTE La synchronisation exacte entre les messages PGN disponibles dans le réseau IEC 61162-3 n'est pas prise en charge si la conversion a lieu dans le réseau IEC 61162-450.

4.6.2 Gestion de la mémoire tampon de sortie entre un réseau IEC 61162-450 et un réseau IEC 61162-3

(voir le 8.12)

Un bloc fonctionnel PNGF doit fournir une mémoire tampon indépendante pour chaque réseau IEC 61162-3 dans lequel il peut procéder à des envois. Le fabricant doit spécifier la capacité maximale de mémoire tampon pour chaque accès. La capacité maximale peut être configurable au moment de l'installation.

La gestion de mémoire tampon PNGF doit reposer sur la priorité IEC 61162-3 incluse dans chaque message. Le fabricant doit décrire la méthode dans sa documentation.

Si la mémoire tampon est saturée et si un message PGN est ignoré, il doit être consigné comme cela est spécifié au 4.3.3.

4.6.3 Exigences relatives à la sortie de datagramme

(voir le 8.12)

Le PNGF doit mettre en forme les messages sortants, comme cela est indiqué au 7.4.1.

Le PNGF doit émettre un message PGN IEC 61162-3 par datagramme IEC 61162-450 sortant pour réduire le plus possible les délais.

4.6.4 Numéro de groupe PGN

(voir le 8.12)

Un groupe PGN est défini comme un groupe logique de dispositifs qui peuvent partager les informations et les messages. Un message provenant d'un dispositif est diffusé à tous les dispositifs appartenant au même groupe PGN. Un dispositif peut appartenir à plusieurs groupes PGN. Le nombre maximal de groupes PGN n'est pas supérieur à quatre. Le groupe PGN peut être utilisé pour filtrer les messages (voir le 4.6.1).

4.7 Exigences relatives à l'autre fonction de réseau (ONF)

(voir le 8.6)

L'ONF représente une fonction qui peut partager la même infrastructure réseau que les blocs fonctionnels de réseau (NF) sur un réseau IEC 61162-450.

L'ONF doit satisfaire aux exigences définies au 4.2.1.

Le matériel ONF ne doit pas utiliser d'adresse de multidiffusion IP réservée par le présent document, comme cela est indiqué au 5.4.

La documentation doit décrire les protocoles de réseau utilisés par l'ONF pour envoyer des datagrammes ou des flux d'octets, par exemple UDP, TCP/IP ou autres.

La documentation doit décrire l'incidence de l'ONF sur le réseau.

5 Exigences relatives au réseau de bas niveau

5.1 Exigences électriques et mécaniques

(voir le 8.7.1)

Le câble et les connecteurs utilisés doivent au moins satisfaire aux spécifications indiquées dans le Tableau 3 s'ils sont utilisés dans un environnement protégé, comme cela est défini dans l'IEC 60945.

Les interfaces à fibres optiques doivent satisfaire aux exigences de sécurité relatives aux lasers pour les dispositifs de Classe 1 spécifiés dans l'IEC 60825-2.

L'exigence relative à la couche physique pour les accès IEC 61162-3 du PNGF doit être conforme à l'Article 4 de l'IEC 61162-3:2008.

Tableau 3 – Interfaces, connecteurs et câbles

Interface IEEE 802.3	Distance de liaison maximale de la section de réseau	Type de connecteur d'interface de dispositif mécanique (environnement protégé)	Attribution de broche	Catégorie de câble, minimale
100BASE-TX IEEE Std 802.3-2022, Articles 24 et 25	100 m	IEC 60603-7-3, connecteur modulaire blindé à 8 voies Voir l'IEC 60603-7:2020, Figures 1 à 5, et l'IEEE Std 802.3:2022, Article 25	[b]	CAT5 STP Deux paires torsadées blindées ANSI/TIA-568-A, ANSI/TIA-568-B ou ISO/IEC 11801 (classe D).
(non spécifiée)	[a]	Répartiteur	[b]	CAT5 STP Deux paires torsadées blindées
100BASE-SX IEEE Std 802.3-2022, Articles 24 et 26	550 m	IEC 61754-20 Connecteur optique duplex type LC[d]		Deux fibres optiques multimodales Longueur d'onde courte 850 nm
1000BASE-T IEEE Std 802.3:2022, Article 40	100 m	IEC 60603-7-7, connecteur modulaire blindé à 8 voies Voir l'IEC 60603-7:2020, Figures 1 à 5.	[c]	CAT5 STP Quatre paires torsadées blindées ANSI/TIA-568-A, ANSI/TIA-568-B ou ISO/IEC 11801 (classe D).
1000BASE-SX IEEE Std 802.3-2022, Article 38	220 m (62/125 µm, faible bande passante modale) 550 m (50/125 µm, bande passante modale élevée)	IEC 61754-20 Connecteur optique duplex type LC[d]		Deux fibres optiques multimodales Longueur d'onde courte 850 nm
Pour une utilisation dans des environnements exposés, des dispositions supplémentaires sont nécessaires. Il convient de prendre en considération le type M12 spécifié dans l'IEC 61076-2-101, pour le câble réseau en cuivre. Il convient également d'envisager un connecteur robuste similaire pour les connexions externes à fibres optiques.				

[a] Dans ce cas, il convient que le fabricant spécifie la distance maximale de fonctionnement.

[b] Le connecteur modulaire à 8 voies spécifié dans l'IEC 60603-7 est le type "8P8C" qui a été couramment utilisé dans les connexions LAN d'ordinateur de bureau, et qui est très souvent appelé, à tort, "RJ45". Les fils sont placés dans l'ordre 1, 2, 3, 6, 4, 5, 7, 8 sur la prise modulaire. Il est identique aux deux extrémités du câble. L'ordre des fils 1 à 8 par couleur doit être le suivant: vert/blanc, vert, orange/blanc, bleu, bleu/blanc, orange, marron/blanc, marron. Il est identique aux deux extrémités du câble. Voir l'IEEE Std 802.3-2022, 25.4.3, et l'IEC 60603-7-3.

[c] Le connecteur modulaire à 8 voies spécifié dans l'IEC 60603-7 est le type "8P8C" qui a été couramment utilisé dans les connexions LAN d'ordinateur de bureau, et qui est très souvent appelé, à tort, "RJ45". Les fils sont placés dans l'ordre 1, 2, 3, 6, 4, 5, 7, 8 sur la prise modulaire. Il est identique aux deux extrémités du câble. L'ordre des fils 1 à 8 par couleur doit être le suivant: vert/blanc, vert, orange/blanc, bleu, bleu/blanc, orange, marron/blanc, marron. Il est identique aux deux extrémités du câble. Voir l'IEEE Std 802.3-2022, 40.8.1, et l'IEC 60603-7-7.

[d] Voir le document TIA-604-10.

5.2 Exigences de protocole de réseau

(voir le 8.7.2)

Le matériel doit mettre en œuvre IPv4 comme cela est généralement décrit dans l'ISOC RFC 5000, avec une exigence minimale de prise en charge des protocoles de réseau spécifiques suivants:

- ARP – Address Resolution Protocol (protocole de résolution d'adresse) décrit dans l'ISOC RFC 826 et mis à jour dans l'ISOC RFC 5227;
- IP – Internet Protocol (protocole Internet) décrit dans l'ISOC RFC 791 et mis à jour dans l'ISOC RFC 2474.

Les protocoles suivants peuvent être pris en charge en fonction des exigences du matériel:

- UDP – User Datagram Protocol (protocole de datagramme utilisateur) décrit dans l'ISOC RFC 768;

  NOTE 1 Pour un matériel purement ONF (ni SF ni SNGF), cela n'est pas nécessairement exigé. Un tel dispositif ONF peut communiquer uniquement sur TCP ou uniquement sur UDP, voire avec des paquets IP ou ICMP bruts.

- multidiffusion UDP – Groupes d'hôtes décrits dans l'ISOC RFC 966 et extensions d'hôte décrites dans l'ISOC RFC 1112;

  NOTE 2 Pour un matériel purement ONF (ni SF ni SNGF), cela n'est pas nécessairement exigé. Un tel dispositif ONF peut communiquer uniquement sur TCP ou uniquement sur UDP, voire avec des paquets IP ou ICMP bruts.

- TCP – Transmission Control Protocol (protocole de contrôle de transmission) décrit dans l'ISOC RFC 793;

  NOTE 3 En règle générale, TCP n'est pas exigé pour les fonctions SF et SNGF. Même si la prise en charge de TCP peut être pertinente pour certains matériels, le présent document n'exige pas l'utilisation de TCP.

- ICMP – Internet Control Message Protocol (protocole de message de contrôle Internet) décrit dans l'ISOC RFC 792;

  NOTE 4 Le présent document ne contient aucune exigence concernant ICMP.

- IGMP – Internet Group Management Protocol (protocole Internet de gestion de groupe) décrit dans l'ISOC RFC 1112, l'ISOC RFC 2236 ou l'ISOC RFC 3376;

  NOTE 5 La prise en charge de la surveillance du trafic IGMP est pertinente en particulier pour les dispositifs SF et SNGF, mais elle n'est pas strictement exigée dans le présent document. Voir le D.2.1.

5.3 Attribution d'adresse IP pour le matériel

(voir le 8.7.3)

Des moyens doivent être prévus pour configurer le matériel sur l'une des adresses réservées à une utilisation dans des réseaux privés, comme cela est décrit dans l'ISOC RFC 1918, avec un masque d'adresse réseau valide. Le masque de sous-réseau par défaut doit être défini de manière appropriée pour 192.168.0.0/24 (classe C existante). L'adresse IP attribuée doit rester fixe pendant le fonctionnement normal du matériel, y compris lors de la mise sous tension et hors tension du matériel.

Un nœud 450 peut réserver des sous-réseaux pour une utilisation non 450, par exemple pour une utilisation interne (au matériel) ou pour d'autres interfaces. Tous les sous-réseaux réservés doivent être documentés. Les sous-réseaux suivants doivent toujours être disponibles pour le réseau IEC 61162-450: 192.168.0.0/24 – 192.168.10.0/24 et 172.16.0.0/16 (classe B).

5.4 Plage d'adresses de multidiffusion

(voir le 8.7.4)

La plage de 239.192.0.1 à 239.192.0.64 est réservée à l'usage actuel et à un usage ultérieur dans les protocoles de couche d'application (voir le 6.2.2).

La plage d'adresses de multidiffusion 239.192.0.57 à 239.192.0.64 est utilisée pour l'interconnexion avec les réseaux IEC 61162-3.

Le matériel ONF ne doit pas utiliser les adresses de multidiffusion figurant dans la plage 239.192.0.1 à 239.192.0.64.

NOTE 1 L'ISOC RFC 2365 définit la plage d'adresses de multidiffusion de 239.192.0.0 à 239.192.63.255 comme la portée IPv4 Organization Local Scope, qui est l'espace à partir duquel une organisation attribue des sous-plages lors de la définition des portées destinées à une utilisation privée.

NOTE 2 La durée de vie (ou TTL [Time-To-Live], c'est-à-dire le nombre de sauts) pour la multidiffusion est adaptable afin de permettre la transmission sur plusieurs routeurs réseau. La valeur TTL par défaut est de 64. Le masque de sous-réseau est correctement défini pour une classe C (réseau local).

5.5 Adresse de dispositif pour les réseaux d'instruments

Des moyens doivent être prévus pour attribuer une plage d'adresses de dispositif entre 0 et 251 lorsque le PNGF émet dans un réseau IEC 61162-3. L'adresse de dispositif peut être définie automatiquement.

6 Spécification de la couche de transport

(voir le 8.8)

6.1 Généralités

L'Article 6 spécifie la manière dont sont utilisés les messages de multidiffusion UDP pour la communication entre les matériels sur un réseau Ethernet.

Le matériel peut mettre en œuvre les fonctionnalités d'envoi et/ou de réception. Les dispositions de l'6 s'appliquent aux deux fonctionnalités, mais elles doivent être soumises à l'essai indépendamment, comme cela est décrit au 7.6.

La Figure 4 représente un exemple de structure de trame Ethernet avec une sentence IEC 61162-450. Le bloc supérieur représente l'ensemble de la trame Ethernet, le bloc de données à la disposition de l'utilisateur UDP étant indiqué en blanc. Les en-têtes IP et UDP sont inclus dans les blocs gris. Le bloc inférieur représente le bloc de données à la disposition de l'utilisateur UDP dans lequel une sentence IEC 61162-450 mise en forme est incluse.

Les nombres au-dessus de la trame Ethernet indiquent la taille de chaque bloc. Les nombres en regard du bloc de données d'utilisateur UDP indiquent le décalage par rapport au début du bloc (0 – zéro).

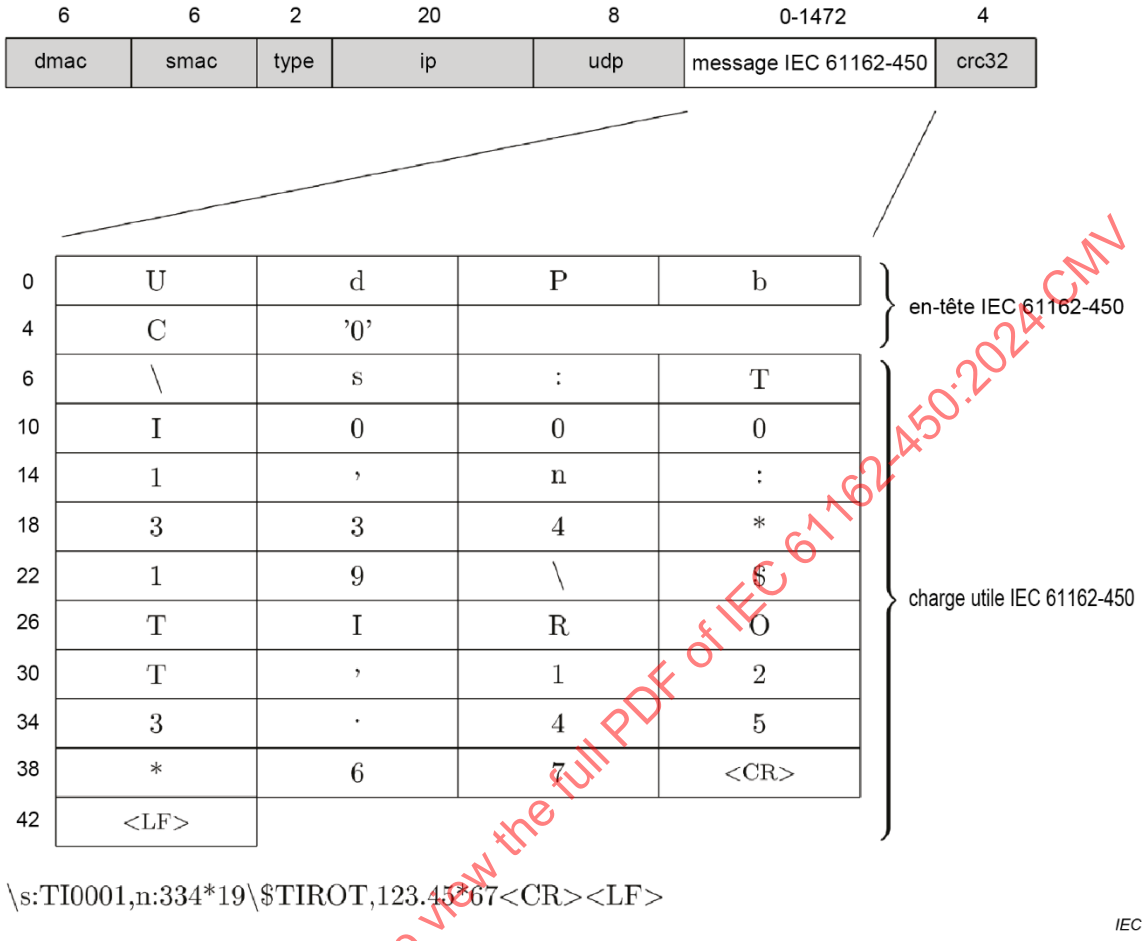


Figure 4 – Exemple de trame Ethernet pour un SBM provenant d'un capteur de vitesse angulaire

6.2 Messages UDP

6.2.1 Protocole multidiffusion UDP

Multidiffusion UDP – la multidiffusion IP est une technique de communication plusieurs à plusieurs sur l'infrastructure IP d'un réseau. Les nœuds de destination envoient des messages de jonction et peuvent envoyer des messages de retrait. La multidiffusion IP touche une plus large population de récepteurs, car elle n'exige pas une connaissance préalable des récepteurs ni de leur nombre. La multidiffusion capitalise l'infrastructure de réseau en exigeant que la source n'envoie un paquet qu'une seule fois, même s'il est nécessaire de le livrer à un grand nombre de destinataires. Les nœuds du réseau veillent à répliquer le paquet pour atteindre plusieurs destinataires uniquement lorsque cela est nécessaire. Le protocole de couche de transport le plus fréquent pour utiliser l'adressage de multidiffusion est le protocole de datagramme utilisateur (UDP).

Les émetteurs et récepteurs doivent au moins être en mesure d'utiliser l'UDP défini par l'ISOC RFC 768 et spécifié plus en détail dans le présent document.

6.2.2 Utilisation des adresses de multidiffusion et des numéros d'accès

Les numéros d'accès doivent être attribués à partir de la plage d'accès dynamiques que l'Internet Assigned Number Authority (IANA) a réservée pour les numéros d'accès dynamiques et/ou privés (plage 49152 à 65535 inclus)

Le Tableau 4 définit les adresses de multidiffusion et les numéros d'accès de destination qui doivent être utilisés lors de la transmission de sentences à partir d'un bloc fonctionnel de système. Le mapping du SFI sur le groupe de transmission par défaut est décrit à l'Annexe A. Si le groupe de transmission par défaut est fourni par le matériel, le système de configuration des paramètres du matériel peut remplacer cet élément par tout groupe de transmission indiqué dans le Tableau 4 ou par l'un des éléments du Tableau 5 (par exemple, pour prendre en charge l'utilisation du même groupe de transmission pour le "fichier binaire" et les sentences connexes: échange d'itinéraire ECDIS et sentence RRT, par exemple).

NOTE La différentiation d'accès a pour objet de fournir un mécanisme assurant un certain niveau de réduction de charge pour le matériel récepteur.

Tableau 4 – Adresses de multidiffusion de destination et numéros d'accès

Groupe de transmission	Catégorie	Adresse de multidiffusion	Accès de destination
MISC	SF qui n'est pas explicitement répertorié ci-dessous	239.192.0.1	60001
TGTD	Données relatives à la cible (SIA), messages relatifs à la cible suivie (radar)	239.192.0.2	60002
SATD	Taux de mise à jour élevé, par exemple cap du navire, données d'assiette	239.192.0.3	60003
NAVD	Sortie de navigation autre que celle des groupes TGTD et SATD	239.192.0.4	60004
VDRD	Données exigées pour le VDR conformément à l'IEC 61996-1	239.192.0.5	60005
RCOM	Matériel de communication radio	239.192.0.6	60006
TIME	Matériel de transmission de l'heure	239.192.0.7	60007
PROP	SF propriétaires et spécifiés par l'utilisateur	239.192.0.8	60008
USR1	Groupe de transmission défini par l'utilisateur 1	239.192.0.9	60009
USR2	Groupe de transmission défini par l'utilisateur 2	239.192.0.10	60010
USR3	Groupe de transmission défini par l'utilisateur 3	239.192.0.11	60011
USR4	Groupe de transmission défini par l'utilisateur 4	239.192.0.12	60012
USR5	Groupe de transmission défini par l'utilisateur 5	239.192.0.13	60013
USR6	Groupe de transmission défini par l'utilisateur 6	239.192.0.14	60014
USR7	Groupe de transmission défini par l'utilisateur 7	239.192.0.15	60015
USR8	Groupe de transmission défini par l'utilisateur 8	239.192.0.16	60016
BAM1	Source d'alerte conforme BAM signalant au CAM, groupe 1	239.192.0.17	60017
BAM2	Source d'alerte conforme BAM signalant au CAM, groupe 2	239.192.0.18	60018
CAM1	CAM de la BAM, groupe 1	239.192.0.19	60019
CAM2	CAM de la BAM, groupe 2	239.192.0.20	60020
NETA	Administration de réseau, par exemple détection de collision du SFI	239.192.0.56	60056
PGP1	PGN, groupe 1	239.192.0.57	60057
PGP2	PGN, groupe 2	239.192.0.58	60058
PGP3	PGN, groupe 3	239.192.0.59	60059
PGP4	PGN, groupe 4	239.192.0.60	60060

Groupe de transmission	Catégorie	Adresse de multidiffusion	Accès de destination
PGB1	PGN de secours, groupe 1	239.192.0.61	60061
PGB2	PGN de secours, groupe 2	239.192.0.62	60062
PGB3	PGN de secours, groupe 3	239.192.0.63	60063
PGB4	PGN de secours, groupe 4	239.192.0.64	60064
NOTE 1 Les groupes de transmission USR1 à USR8 peuvent être utilisés, par exemple, pour les données propriétaires au format binaire. NOTE 2 Pour équilibrer le trafic ou assurer la rétrocompatibilité, en plus de la mise en œuvre de l'utilisation obligatoire des groupes de transmission BAM1/BAM2 et CAM1/CAM2, la communication liée à la BAM peut être configurée pour utiliser les groupes de transmission SATD ou NAVD par exemple.			

Le Tableau 5 définit les adresses de multidiffusion et les numéros d'accès de destination qui doivent être utilisés lors de la transmission de données de fichier binaire. Si l'adresse de multidiffusion ou le numéro d'accès de destination par défaut est fourni par le matériel, le système de configuration des paramètres du matériel peut remplacer cet élément par les adresses de multidiffusion ou les numéros d'accès de destination des groupes de transmission USR1 à USR8, RCOM, PROP du Tableau 4 ou par l'un des éléments du Tableau 5 (par exemple, pour prendre en charge l'utilisation du même groupe de transmission pour le "fichier binaire" et les sentences connexes).

Tableau 5 – Adresses de multidiffusion de destination et numéros d'accès pour le transfert de données binaires

Catégorie	Adresse de multidiffusion	Accès de destination
Transfert de fichier binaire non retransmissible, groupe 1 [a]	239.192.0.21	60021
Transfert de fichier binaire non retransmissible, groupe 2 [a]	239.192.0.22	60022
Transfert de fichier binaire non retransmissible, groupe 3 [a]	239.192.0.23	60023
Transfert de fichier binaire non retransmissible, groupe 4 [a]	239.192.0.24	60024
Transfert de fichier binaire non retransmissible, groupe 5 [a]	239.192.0.25	60025
Transfert de fichier binaire retransmissible, groupe 1 [b]	239.192.0.26	60026
Transfert de fichier binaire retransmissible, groupe 2 [b]	239.192.0.27	60027
Transfert de fichier binaire retransmissible, groupe 3 [b]	239.192.0.28	60028
Transfert de fichier binaire retransmissible, groupe 4 [b]	239.192.0.29	60029
Transfert de fichier binaire retransmissible, groupe 5 [b]	239.192.0.30	60030
[a] L'adresse 239.192.0.25 et l'accès 60025 sont définis par défaut pour le transfert d'itinéraire ECDIS (voir l'IEC 61174). [b] L'adresse 239.192.0.26 et l'accès 60026 sont définis par défaut pour le transfert d'image VDR (voir l'IEC 61996-1). L'adresse 239.192.0.30 et l'accès 60030 sont définis par défaut pour les blocs de données retransmissibles ECDIS pour le transfert d'itinéraire (voir l'IEC 61174).		

Le Tableau 6 répertorie d'autres adresses de multidiffusion et accès réservés par le présent document.

Tableau 6 – Adresses de multidiffusion de destination et numéros d'accès pour d'autres services

Catégorie	Adresse de multidiffusion	Accès de destination
Syslog	239.192.0.254	514
L'envoi à syslog peut avoir lieu par multidiffusion ou par monodiffusion UDP. Certains commutateurs peuvent ne prendre en charge que la monodiffusion UDP.		

Les adresses 239.192.0.31 à 239.192.0.55 sont réservées pour une extension ultérieure.

L'IANA a défini que la plage d'accès 49152 à 65535 est réservée à une utilisation dynamique et privée. Les accès spécifiques du présent document sont dans les limites de cette plage IANA. Les systèmes d'exploitation utilisent également cette plage IANA pour leur usage interne en tant qu'accès éphémères. Ce double usage peut engendrer des conflits de numéros d'accès, donnant ainsi lieu à des pertes de communication des messages IEC 61162-450. Il est recommandé d'envisager une limitation de la plage d'accès éphémères du système d'exploitation du matériel connecté à un réseau IEC 61162-450 pour éviter les conflits de numéros d'accès.

6.2.3 Somme de contrôle UDP

Tous les dispositifs doivent calculer et vérifier la somme de contrôle UDP définie par l'ISOC RFC 768. Il n'est pas admis d'attribuer une valeur nulle au champ de somme de contrôle (aucune somme de contrôle).

Un datagramme dont la somme de contrôle est incorrecte ou absente doit être ignoré par le destinataire.

6.2.4 Taille des datagrammes

Le bloc fonctionnel de réseau ne doit pas émettre plus de 1 472 octets de données dans chaque datagramme, y compris l'en-tête, comme cela est indiqué à l'Article 7.

Le matériel récepteur peut ignorer les datagrammes dont la taille est supérieure à la taille maximale spécifiée.

NOTE La taille maximale des datagrammes UDP peut être de 64 ko au maximum lorsqu'ils sont envoyés comme plusieurs fragments IP.

7 Spécification de la couche d'application

7.1 En-tête de datagramme

(voir le 8.9.2)

7.1.1 En-tête valide

Les six premiers octets de tout datagramme de multidiffusion UDP doivent contenir l'une des chaînes suivantes, suivie d'un caractère nul (tous les bits définis sur zéro):

- "`UdPbC`" pour la transmission de sentences mises en forme selon l'IEC 61162-1, comme cela est décrit au 7.2;
- "`RaUdP`" pour la transmission de fichiers binaires, comme cela est décrit au 7.3;
- "`RrUdP`" pour la transmission de fichiers binaires retransmissibles, comme cela est décrit au 7.3;

- "NkPgN" pour la transmission de messages PGN IEC 61162-3, comme cela est décrit au 7.4.

Les six premiers octets de tout datagramme TCP/IP doivent contenir la chaîne suivante, suivie d'un caractère nul (tous les bits définis sur zéro):

- "RrTcP" pour la transmission de fichiers binaires, comme cela est décrit au 7.6.

NOTE 1 Le terme "datagramme" signifie "paquet" dans ce contexte.

Les datagrammes entrants dont l'en-tête est inconnu doivent être ignorés sans traiter le contenu après l'en-tête.

NOTE 2 Les éditions ultérieures de l'IEC 61162-450 peuvent définir d'autres codes d'en-tête. Ce type de code d'en-tête est différent de ceux déjà utilisés et contient au moins six octets, incluant éventuellement un caractère nul de fin.

7.1.2 Consignation des erreurs

Le matériel doit procéder au comptage des datagrammes reçus dont l'en-tête n'est pas valide et tenir ces informations à disposition, comme cela est indiqué au 4.3.3.

7.2 Transmissions de sentences IEC 61162-1 générales

7.2.1 Application de ce protocole

(voir le 8.9.1)

Ce protocole fournit un mécanisme par lequel les sentences IEC 61162-1 peuvent être envoyées à un ou plusieurs destinataires présents sur le réseau. Le protocole permet de fusionner plusieurs sentences en un datagramme.

7.2.2 Types de messages pour lesquels ce protocole peut être utilisé

(voir le 8.9.3)

Ce protocole doit être utilisé pour les messages de types SBM et MSM (voir l'Annexe A). Il doit également être utilisé pour les échanges de messages CRP selon les dispositions spécifiées à l'Annexe C.

7.2.3 Paramètres de bloc TAG pour les sentences émises dans le datagramme

(voir le 8.9.4)

7.2.3.1 Bloc TAG valide

Chaque sentence doit être précédée d'au moins un bloc TAG, comme cela est indiqué à l'Annexe B, contenant un ou plusieurs des codes de paramètre décrits du 7.2.3.3 au 7.2.3.8. L'ajout de blocs TAG avec des codes de paramètre a lieu après le dernier bloc TAG existant.

Un exemple d'application d'un ou de plusieurs codes de paramètre "s" est fourni ci-après.

Source d'origine = GP0001

```
\s:GP0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A*27<CR><LF>
\s:GP0001*hh\\s:AB0001*hh\\s:TT0001*hh\$GPGLL,5057.970,N,00146.110,E,142451,A
*27<CR><LF>
```

Si une valeur est attribuée plusieurs fois à un code de paramètre dans l'ensemble des blocs TAG alors qu'une seule valeur est attendue, la valeur de code de paramètre la plus proche du début de la sentence IEC 61162-1 et conforme à l'IEC 61162-450 (voir le 7.2.3.4) doit être utilisée.

NOTE Le code de paramètre "s" conforme à l'IEC 61162-450 peut être ajouté par le SNGF ou l'ONF.

S'il existe plusieurs codes de paramètre source "s", la source d'origine est le paramètre "s" le plus à droite dans le bloc TAG le plus à gauche à partir du début de la sentence IEC 61162-1 et conforme à l'IEC 61162-450 (voir le 7.2.3.4).

Si un dispositif modifie le contenu d'une sentence IEC 61162-1 reçue, alors les blocs TAG qui contiennent les codes de paramètre source "s" doivent être supprimés et remplacés par un bloc TAG qui contient un code de paramètre source "s" fondé sur le SFI du dispositif qui a effectué la modification.

Un bloc TAG, ou un groupe avec deux blocs TAG ou plus, peut contenir plusieurs destinations. Chaque récepteur est responsable de la reconnaissance de son propre identificateur, et chaque récepteur traite la ligne de bloc TAG (voir l'Article B.5) ou le groupe de lignes de bloc TAG comme étant adressée à cette unité.

- Premier exemple

  Deux datagrammes valides sont représentés ci-dessous. Le second datagramme montre deux occurrences du code de paramètre "s", où la première occurrence (AC1000) est la source d'origine et la seconde occurrence qui est la plus proche de la sentence (BC1000) identifie le dispositif que cette sentence a traversé.

  ```
  \d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,
  0*7C

  \s:AC1000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,,A,
  3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
  ```

- Second exemple

  Le datagramme ci-dessous représente le cas où un code de paramètre "s" (002300000) provient d'une source non conforme à l'IEC 61162-450. Un récepteur peut utiliser ou ignorer cette source non conforme à l'IEC 61162-450. Noter que le code de paramètre "s" (BC1000) le plus proche de la sentence est conforme à l'IEC 61162-450.

  ```
  \s:002300000,c:1558090544462*hh\\d:AB0001,d:AB0002,s:BC1000*hh\!BSVDM,1,1,
  ,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
  ```

Pour la conformité au présent document, tous les codes de paramètre de bloc TAG sont définis au moment de l'installation et ne doivent pas être configurables de manière dynamique en fonctionnement normal.

NOTE Les sentences de contrôle permettant de modifier les codes de paramètre dans la NMEA 0183 ne doivent pas être utilisées en fonctionnement normal.

7.2.3.2 Contrôle de bloc TAG

Seules les sentences précédées de blocs TAG valides définis comme cela est indiqué au 7.2.3.1 doivent être traitées par le destinataire.

Un bloc TAG peut contenir des codes de paramètre et leurs valeurs connues et/ou non connues par le récepteur. En outre, il peut exister plusieurs occurrences d'un code de paramètre. Les exemples ci-dessous constituent une aide pour une interprétation correcte.

Si la valeur du code de paramètre "s" n'est pas comprise par le récepteur, par exemple si elle n'est pas codée comme dans le présent document (voir le 7.2.3.4), le message doit être ignoré, par exemple:

```
\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
```

Si le code de paramètre "s" est présent deux fois, la première instance codée comme dans le présent document (voir le 7.2.3.4) et la seconde instance non comprise par le récepteur, alors le message doit être accepté en fonction du code de paramètre compris par le récepteur et l'existence du code de paramètre non compris est ignorée, par exemple:

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:002300000*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R
=23BTB3F00Uh,0*7C
```

NOTE L'exemple ci-dessus peut être le résultat d'un nœud qui ajoute son bloc TAG devant les blocs TAG existants plutôt que devant le début de la sentence (voir le 7.3.2.1).

Lorsque le code de paramètre "s" est présent deux fois, seul le code de paramètre "s" plus proche du début de la sentence IEC 61162-1 est utilisé (s:AI0001 dans l'exemple ci-dessous) et l'autre est ignoré, par exemple:

```
\d:AB0001,d:AB0002,s:BC1000*hh\\s:AI0001*hh\!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23
BTB3F00Uh,0*7C
```

Si le message contient des codes de paramètre connus (par exemple, "s") et inconnus (par exemple, "c" défini dans le présent document, mais non mis en œuvre par le récepteur), alors le message doit être accepté et le code de paramètre inconnu doit être ignoré, par exemple:

```
\s:BC1000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
```

Si tous les codes de paramètre sont inconnus du récepteur (par exemple, "h" n'est pas défini dans la présente norme et "c" n'est pas mis en œuvre par le récepteur), alors le message doit être ignoré, par exemple:

```
\h:002300000,c:1558090544462*hh\!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*
37
```

7.2.3.3 Commande de regroupement – g

Le code de paramètre "g" doit être utilisé par les émetteurs pour regrouper les blocs TAG et/ou les sentences. Il doit au moins être utilisé pour regrouper les sentences classées comme appartenant au type de message "MSM" du Tableau A.2, si le groupe multisentences est composé de plusieurs messages. Il n'est pas exigé d'inclure le code de paramètre "g" pour les sentences à une seule ligne.

NOTE Un exemple d'utilisation facultative consiste à associer ou à lier des sentences connexes, par exemple les sentences GGA et VTG provenant d'un récepteur GNSS peuvent être regroupées.

Les destinataires doivent accepter le code de paramètre "g" pour tous les types de messages.

Une sentence de type MSM valide dont les champs de données internes spécifient qu'elle appartient à un groupe de plusieurs messages doit être ignorée si le groupe "g" est absent ou s'il contient des informations incohérentes.

La valeur du code de paramètre "g" est divisée en trois champs. Les champs dans les paramètres "g" sont séparés par le caractère "-" comme délimiteur. Les utilisations de chaque champ (de gauche à droite) sont les suivantes:

1) le numéro de ligne pour ce bloc TAG particulier et la sentence associée;
2) le nombre total de lignes;
3) le code de groupe. Il est utilisé pour différencier les différents groupes de blocs TAG et les sentences.

Le code de groupe est déterminé par le dispositif émetteur. La valeur initiale du code de groupe doit être un ("1") et sa valeur d'incrément doit être égale à un ("1"). Le code de groupe doit être réinitialisé sur un ("1") après 99; la plage valide est donc comprise entre 1 et 99 inclus. Le récepteur ne doit pas faire d'hypothèse concernant la valeur initiale du code de groupe.

Lorsqu'il est utilisé, le code de paramètre "g" doit être le premier code de paramètre du bloc TAG.

Toutes les sentences regroupées de type MSM d'un message doivent être incluses dans le même groupe de lignes liées, mais le groupe de lignes liées peut également inclure d'autres sentences que celles de type MSM.

Il est recommandé d'envoyer les sentences regroupées en un nombre de datagrammes aussi restreint que possible afin de réduire le plus possible la probabilité de réception de paquets dans le désordre.

Un exemple d'utilisation conforme est donné ci-dessous. Dans cet exemple, quatre sentences VDM sont regroupées (les 2 premières sont distinctes et les 2 dernières font partie du MSM).

```
\g:1-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F00Uh,0*7C
\g:2-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD8@Ip,0*37
\g:3-4-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\g:4-4-45*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

Un exemple d'utilisation non conforme du regroupement est donné ci-dessous. Dans cet exemple, le regroupement des trois premières lignes n'inclut pas la seconde partie du message MSM.

```
\g:1-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,A,3Cu>2;002nQHiO`R=23BTB3F 00Uh,0*7C
\g:2-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,1,1,,B,1D80CB003HQi5WPR7l;PnhgD 8@Ip,0*37
\g:3-3-45,d:AB0001,d:AB0002,s:BC1000*hh\
!BSVDM,2,1,3,A,5CLBG7T28eodt`4V2205E86222222222222220t3HK8440Ht;BCRCp88888,0
*1E
\d:AB0001, d:AB0002,s:BC1000*hh\!BSVDM,2,2,3,A,88888888880,2*3E
```

L'exemple suivant décrit le code de paramètre "g" utilisé pour regrouper des sentences en deux groupes différents, chacun composé de deux sentences:

```
\g:1-2-34,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-46,s:IN0001*3F\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D
\g:2-2-46,s:IN0001*3C\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20
```

Les exigences supplémentaires relatives à l'utilisation du code de paramètre "g" sont les suivantes:

1) toutes les lignes de bloc TAG regroupées doivent être envoyées par ordre croissant, comme cela est indiqué par la première valeur numérique du code de paramètre "g";
2) les lignes de bloc TAG regroupées ne doivent pas être envoyées avec un retard de plus d'une seconde entre chaque ligne de bloc TAG.

Les récepteurs peuvent ignorer le groupe complet si les deux exigences ci-dessus ne sont pas respectées.

Un exemple d'utilisation non conforme de la première exigence est une variante de l'exemple précédent avec une séquence incorrecte (deux lignes sont envoyées dans le mauvais ordre):

```
\g:2-2-34,s:IN0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
\g:1-2-34,s:IN0001*3A\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*04
```

7.2.3.4 Identification de la source – s

Le code de paramètre "s" doit être défini pour les émetteurs et doit contenir l'ID de fonction système (SFI, voir le 4.4.2) correspondant au bloc fonctionnel d'où provient la sentence.

Les messages reçus sans aucun code de paramètre "s" connu doivent être ignorés.

Plusieurs codes de paramètre "s" peuvent être utilisés pour indiquer la voie empruntée par un message. Le premier code de paramètre "s" ou le code de paramètre "s" le plus à droite est le SFI du dispositif qui crée le message. Des SFI de matériels supplémentaires pour les codes de paramètre source peuvent être ajoutés à gauche afin d'indiquer l'itinéraire suivi par le message.

Par exemple, un SNGF peut ajouter son SFI comme paramètre source à un message afin d'indiquer que le message provient d'un SNGF particulier. Pour un exemple de configuration des SFI capteur et des SFI SNGF, voir la Figure 2 et la Figure 3.

7.2.3.5 Identification de la destination – d

Le code de paramètre "d" doit être défini pour les sentences de type CRP et est facultatif pour les autres types. S'il est utilisé, il doit contenir l'ID de fonction système (SFI, voir le 4.4.2) correspondant au destinataire prévu de la sentence.

Si aucun code de paramètre de destination n'est présent, tous les dispositifs qui reçoivent cette sentence doivent la traiter.

Plusieurs codes de paramètre "d" peuvent être spécifiés si plusieurs destinataires prévus sont présents. Tous les codes de paramètre "d" dans un groupe de blocs TAG s'appliquent collectivement à toutes les sentences associées au groupe de blocs TAG. Les destinataires énumérés doivent traiter le contenu des sentences associées et réagir à celui-ci.

NOTE Cela peut être le cas pour les fonctions de commande redondantes. Les autres destinataires lisent également le message, par exemple pour les besoins de l'enregistrement des données du voyage, mais il n'est pas prévu qu'ils interviennent sur le contenu.

S'il est nécessaire de spécifier plus de codes de paramètre "d" qu'un seul bloc TAG peut contenir, la liste des codes de paramètre "d" doit être divisée sur plusieurs blocs TAG. Si ces blocs TAG se trouvent sur la même ligne de bloc TAG, il n'est pas nécessaire de les lier en utilisant le code de paramètre "g". Par exemple, deux blocs TAG, l'un avec 7 et l'autre avec 2 codes de paramètre "d":

```
\s:IN0001,d:AB0001,d:AB0002,d:AB0003,d:AB0004,d:AB0005,d:AB0006,d:AB0007*hh\\
d:AB0008,d:AB0009*hh\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
```

7.2.3.6 Paramètre de comptage de ligne – n

(voir le 8.9.4.1)

Le code de paramètre "n" peut être utilisé pour attribuer un numéro de séquence à des sentences spécifiques émises à partir d'un bloc fonctionnel de système. Le format de la valeur de paramètre est un entier positif. La valeur doit commencer à un ("1") et doit être incrémentée de un ("1") pour les sentences spécifiques émises à partir de ce bloc fonctionnel de système. La valeur de paramètre doit être réinitialisée sur un ("1") après 999, la plage valide est donc comprise entre 1 et 999 inclus.

EXEMPLE 1 Un récepteur GPS envoie ses sentences à tout le monde. Des sentences spécifiques, toutes les sentences ou un sous-ensemble de sentences envoyées peuvent être pris en charge par un seul compteur de ligne.

EXEMPLE 2 Un matériel met en œuvre l'ECDIS et le contrôle de route. Des sentences spécifiques envoyées par la fonction de contrôle de route au pilote automatique peuvent être prises en charge par un compteur de ligne. Toutes les autres sentences envoyées par le matériel sont sans code de paramètre de comptage de ligne.

EXEMPLE 3 Une commande de variation d'intensité d'affichage centrale envoie des sentences DDC séparément pour plusieurs moniteurs. Chaque moniteur est identifié à l'aide du code de paramètre d. Chaque flux de sentences DDC peut être pris en charge par des compteurs de ligne distincts.

7.2.3.7 Paramètre de chaîne de texte – t (données propriétaires)

Le code de paramètre "t" est un champ de texte libre. Le présent document réserve le codage pour les codes TAG propriétaires avec les champs définis ci-dessous, le "p" de début et le code mnémonique à trois lettres du fabricant étant exigés pour ce type de chaîne de texte.

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

Un exemple utilisé pour l'authentification propriétaire des lignes à l'aide du regroupement et de la source pour le fabricant "mmm" peut être

```
\g:1-2-34,s:TI0001,n:333*6B\$TIROT,123.45*67
\g:2-2-34,s:TI0001,n:334,t:pmmma;MD5;0x12345678*0D\
```

7.2.3.8 Authentification générale – a

(voir le 8.9.5)

Le code de paramètre d'authentification est utilisé pour signer un message avec un mot de passe. Le simple envoi d'un mot de passe avec le message révèle le mot de passe à quiconque écoute le trafic. L'envoi d'un condensé de signature permet de garder le mot de passe secret.

Tous les types de messages peuvent être signés à l'aide du code de paramètre d'authentification. Le code de paramètre d'authentification ne modifie en aucun cas le message d'origine. Il est toujours possible d'ignorer ce bloc TAG et d'utiliser le reste du message.

EXEMPLE Signature des commandes de configuration pour les dispositifs ou les commandes au pilote automatique.

Le code de paramètre d'authentification fournit un mécanisme normalisé de transmission du condensé avec le message. La gestion du mot de passe est hors du domaine d'application du présent document. Un moyen consiste à utiliser des clés prépartagées (PSK, *Pre-Shared Keys*) sur les dispositifs participants.

NOTE 1 La clé prépartagée peut être composée de 32 caractères alphanumériques, par exemple "Alea iacta est 1234567890".

Ce code de paramètre est facultatif, et il convient de ne l'utiliser qu'en cas de problèmes de sécurité particuliers. Si ce TAG est fourni, la documentation du fabricant doit décrire quelles méthodes de calcul de signature le matériel prend en charge parmi les différents types de méthodes disponibles et doit expliquer comment partager les clés.

Le format du bloc TAG est le suivant:

\a:c-h--h*hh\

dans lequel

c est le type de méthode de calcul facultative de la signature:

1) MD5;

2) SHA-256; et

P) propriétaire;

h-h est la représentation hexadécimale de la signature, par exemple 32 codes hexadécimaux pour MD5.

Un exemple de bloc TAG est le suivant:

\a:1-123456789abcdef67890123456789012*hh\

Les types de méthodes de calcul de signature sont les suivants.

1) MD5

   La signature est un condensé MD5 du mot de passe plus le message. MD5 est un algorithme de condensé de message à sens unique (RFC 1321). La longueur totale de la signature est de 128 bits ou 32 codes hexadécimaux. MD5 est couramment utilisé pour stocker les mots de passe sous Unix. La révélation du condensé n'expose pas le mot de passe.

   NOTE 2 Voir http://tools.ietf.org/html/rfc1321 et http://en.wikipedia.org/wiki/MD5.

   La sécurité fournie en 2023 par MD5 est faible. Pour une nouvelle conception, SHA-256 est recommandé.

2) SHA-256

   La signature est un condensé SHA-256 du mot de passe plus le message. La longueur totale de la signature est de 256 bits ou 64 codes hexadécimaux. La révélation du condensé n'expose pas le mot de passe.

P) Propriétaire

   La signature est un condensé propriétaire du mot de passe plus le message. Cette variante exige que les deux parties utilisent la même méthode propriétaire spécifiée par le fabricant.

La valeur du code de paramètre d'authentification est calculée par concaténation d'une clé prépartagée et de tous les blocs TAG et toutes les sentences du message en une seule chaîne à utiliser par la méthode de calcul de signature, de manière à produire le condensé de signature. Les "retours chariot" et "sauts de ligne" à partir des sentences ne sont pas inclus dans la chaîne d'entrée.

Si le code de paramètre d'authentification "a" est utilisé, il doit se trouver dans le bloc TAG d'authentification qui lui est propre, sans autre code de paramètre. Pour un message regroupé composé de plusieurs lignes de blocs TAG et de sentences, le bloc TAG d'authentification doit être placé sur la première ligne du groupe. Dans la première ligne, le bloc TAG d'authentification doit être le dernier bloc TAG, et placé avant une sentence de cette ligne. Cela s'applique également à un bloc TAG et une sentence à une seule ligne sans regroupement.

Exemple d'utilisation de bloc TAG d'authentification:

Message composé de deux sentences regroupées à protéger par authentification:

\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Clé prépartagée à utiliser pour le calcul de signature:

Alea iacta est 1234567890

Chaîne d'entrée obtenue pour le calcul de signature:

Alea iacta est 1234567890\g:1-2-23,s:IN0001*3C\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Message à envoyer incluant la signature, méthode MD5:

\g:1-2-23,s:IN0001*3C\\a:2-851E40CC1CB7E3B39D961D7CF10BD8D3*44\!ABVDM,1,1,1,B,15N1u<PP1cJnFj:GV4>:MOw:0<02,0*2D

\g:2-2-23,s:IN0001*3F\$ABVSI,r3669962,1,013538.05654921,1427,-101,,*20

Les messages sans code de paramètre d'authentification sont acceptés, à moins que les paramètres de configuration du destinataire soient explicitement définis pour exiger l'authentification des paquets entrants.

S'il est prévu que le dispositif exige l'authentification des paquets entrants, les paquets sans authentification valide doivent être supprimés.

NOTE 3 Il est conseillé que le SNGF évite de transmettre des mots de passe en clair à partir des sentences SPW reçues sur une connexion série.

7.2.3.9 Identification du paquet de destination – x

(voir le 8.9.4.1 et le 8.9.4.2)

Le code de paramètre "x" est facultatif, sauf s'il est exigé par une norme de matériel (par exemple, communication liée à la BAM). Voir l'Annexe H pour les identificateurs de paquet.

7.2.3.10 Identification du paquet source – z

(voir le 8.9.4.1)

Le code de paramètre "z" est facultatif, sauf s'il est exigé par une norme de matériel. Voir l'Annexe H pour les identificateurs de paquet.

7.2.4 Exigences de traitement des datagrammes entrants

Pour les datagrammes destinés à être traités par le SF, une erreur de syntaxe dans un bloc TAG ou dans une sentence doit conduire le matériel récepteur à ignorer l'ensemble du datagramme sans autre traitement que celui spécifié au 7.2.5. L'exception est un SNGF qui peut retransmettre les sentences anormales à l'accès série approprié, s'il peut être déterminé à partir d'un champ de destination valide, ou à l'ensemble des accès série connectés, si aucun champ de destination n'est spécifié.

7.2.5 Consignation des erreurs pour le traitement des datagrammes entrants

(voir le 8.10)

Le matériel doit procéder au comptage des erreurs détectées dans le traitement des datagrammes contenant des sentences IEC 61162-1. Les erreurs suivantes doivent au moins être comptées et mises à disposition, comme cela est indiqué au 4.3.3:

- toutes les erreurs de mise en forme du bloc TAG, comme cela est indiqué au 7.2.3.1;
- erreur de somme de contrôle TAG;
- erreur de syntaxe TAG (longueur de ligne, utilisation de délimiteurs, caractères non valides);
- erreur de cadrage TAG (début ou fin incorrecte du bloc TAG);
- toutes les erreurs de syntaxe de sentence, y compris de mise en forme, de longueur ou de somme de contrôle, comme cela est indiqué au 7.2.3.9.

7.3 Transfert de fichier binaire par multidiffusion UDP – Un seul émetteur, plusieurs récepteurs

(voir le 8.11)

7.3.1 Application de ce protocole

Ce protocole fournit un mécanisme par lequel les données non mises en forme selon l'IEC 61162-1, par exemple images radar placées dans un fichier, peuvent être transmises à un ou plusieurs récepteurs. Ce protocole prend en charge la transmission de fichiers de zéro octet jusqu'à 4 milliards de blocs de fichiers.

Le matériel utilisant ce mécanisme doit être en mesure d'utiliser l'une des formes suivantes de transfert de fichier binaire:

- transferts non retransmissibles, dans lesquels l'émetteur envoie l'ensemble du fichier binaire sans retour du récepteur;
- transferts retransmissibles dans lesquels un retour limité d'un récepteur identifié par DestID peut être utilisé pour retransmettre certaines parties du fichier binaire, alors que d'autres

récepteurs parallèles fonctionnent comme des récepteurs uniquement passifs du fichier binaire.

NOTE L'avantage que présentent les méthodes de transfert de fichiers binaires non retransmissibles et retransmissibles par rapport au TCP/IP réside dans la possibilité de disposer de plusieurs récepteurs parallèles pour une même transmission.

Le Tableau 7 donne une description des termes utilisés dans cette application.

Tableau 7 – Description des termes

Terme	Description
DWORD	Mot double. Un entier de 32 bits non signé (dans la plage de 0 à 4294967295). DWORD est construit à partir de quatre OCTETS transmis à la suite, dont l'ordre de transmission sur le réseau est le suivant: OCTET de poids fort en premier, suivi de l'OCTET de poids fort suivant jusqu'à l'OCTET de poids faible.
Caractère nul	Un OCTET avec la valeur zéro
Octets réservés	Nombre d'octets dans le datagramme qui peuvent être ignorés par le récepteur. Les octets réservés peuvent être des informations d'en-tête supplémentaires qui n'ont un sens que pour les nouvelles versions du protocole.
WORD	Un entier de 16 bits non signé (dans la plage de 0 à 65535). WORD est construit à partir de deux OCTETS transmis à la suite, dont l'ordre de transmission sur le réseau est le suivant: OCTET de poids fort suivi de l'OCTET de poids faible.
STRING[n]	Une suite de n OCTETS exactement, interprétée comme une chaîne de caractères. L'ordre de transmission sur le réseau est le suivant: caractère le plus à gauche en premier. Si la chaîne comporte moins de n OCTETS, un caractère nul doit être attribué aux octets de fin supplémentaires. Toutes les chaînes de l'en-tête sont codées ISO/IEC 8859-1 (ISO Latin 1).

7.3.2 Structure de fichier binaire

7.3.2.1 Généralités

Les fichiers binaires sont transmis sur le réseau dans un ou plusieurs datagrammes. La structure du fichier binaire est un flux d'octets séquentiel et non complété divisé en trois groupes principaux: l'en-tête, le descripteur de fichier binaire et les données du fichier binaire (voir le Tableau 8 et le Tableau 9). L'en-tête est nécessaire à la synchronisation et à la validation de l'intégrité des données. Le descripteur de fichier binaire sert à décrire les données du fichier binaire et n'est utilisé que dans le premier datagramme pour chaque transfert de fichier binaire.

7.3.2.2 Transferts non retransmissibles et retransmissibles

Tableau 8 – Structure de fichier binaire

En-tête 61162-450 (voir le 7.3.3)
Descripteur de fichier binaire (dans le premier datagramme uniquement) (voir le 7.3.4)
Fragment de données du fichier binaire (voir le 7.3.5)
En-tête 61162-450 (zéro ou plus)
Fragment de données du fichier binaire (zéro ou plus)

Une transmission minimale de fichier binaire à l'aide d'un transfert non retransmissible ou retransmissible est composée des trois premiers blocs dans lesquels la longueur du fragment du fichier binaire peut être nulle.

L'en-tête doit être répété comme le premier élément d'un datagramme contenant des fragments de données du fichier binaire.

7.3.3 En-tête 61162-450

7.3.3.1 Format de l'en-tête

L'en-tête a pour objet de fournir le statut de transfert de données aux récepteurs. Cela permet à un récepteur d'identifier une éventuelle perte de données lors du transfert de fichier, ainsi que la mesure de cette perte. De plus, l'en-tête est utilisé pour fournir un mécanisme de retransmission pour le transfert de fichier binaire retransmissible.

Le format de l'en-tête 61162-450 est défini dans le Tableau 9.

Tableau 9 – Format de l'en-tête 61162-450

Élément de données	TYPE	Description
Token	STRING[6]	Identificateur sous la forme d'une chaîne ASCII de 5 octets suivie d'un caractère nul (voir le 7.1.1.
Version	WORD	Définit la version de l'en-tête. La version de l'en-tête de valeur 2 est définie dans le présent document. Des extensions et/ou des versions modifiées peuvent mettre à jour cette valeur.
HeaderLength	WORD	Définit la longueur de l'en-tête en octets. Il s'agit au moins de la longueur de l'en-tête. Les éditions ultérieures de l'IEC 61162-450 peuvent ajouter d'autres champs à cet en-tête, pour autant qu'ils soient conformes à la définition de l'en-tête indiquée dans le présent document. Les récepteurs qui ne connaissent pas ces champs supplémentaires doivent les ignorer.
SrcID	STRING[6]	Définit l'identificateur du système source au format "ccxxxx" (voir le 4.4.2).
DestID	STRING[6]	Pour le transfert retransmissible, définit l'identificateur du système de destination au format "ccxxxx", par exemple "VR0001" pour VDR (voir le 4.4.2). Si DestID = "XXXXXX", aucune destination n'est attribuée.
Type	WORD	Identifie les informations de l'en-tête.
BlockID	DWORD	Identificateur de bloc de fichier binaire. La valeur initiale est générée de manière aléatoire dans les limites de la plage comprise entre 0 et (2^{32} – 1 = 4294967295). Elle est incrémentée de 1 après la transmission d'un bloc complet.
SequenceNum	DWORD	Définit le numéro de séquence du bloc de fichier binaire. Dans les messages ACK, il est utilisé pour informer l'émetteur que le bloc a été reçu.
MaxSequence	DWORD	Le nombre de datagrammes nécessaires à la transmission de ce bloc de données de fichier binaire. Si SequenceNum est égal à MaxSequence, cela signifie que ce datagramme est le dernier du bloc de données. MaxSequence est uniquement utilisé pour le message de type DATA. Pour les autres messages (QUERY,ACK), la valeur de ce champ doit être 0.
Device	BYTE	Source de données (dispositif) en tant que valeur binaire, 1 pour le matériel 1, 2 pour le matériel 2, etc. La valeur peut être comprise entre 1 et 255.
Channel	BYTE	Subdivision en fonction de la source de données (dispositif), valeurs comprises entre 1 et 255, valeur par défaut = 1.

Les champs Device et Channel sont définis par l'application et peuvent être utilisés par les récepteurs pour déterminer la manière de traiter les données du fichier binaire.

7.3.3.2 Utilisation du jeton d'en-tête

Le jeton d'en-tête permet d'identifier le type de bloc de données et le mode de transfert. Il n'est pas utilisé pour accepter ou rejeter des transmissions. Deux jetons d'en-tête sont définis au 7.1.1:

- "RaUdP" – Simple service de transfert de fichier binaire avec multidiffusion UDP;
- "RrUdP" – Service de transfert de fichier binaire retransmissible avec multidiffusion UDP.

7.3.3.3 Version

Définit la version de l'en-tête. Elle doit être définie sur 2 pour le présent document.

7.3.3.4 Identificateur de destination

Pour les transmissions vers un récepteur spécifique, le champ doit contenir le SFI de destination. La valeur du champ doit être "XXXXXX" pour une destination non spécifique.

7.3.3.5 Type de message

Le type de message donne les informations relatives aux informations que contient le datagramme:

- DATA (0x01) – Ce type est utilisé pour la transmission de données de fichier binaire, y compris le descripteur de fichier;
- QUERY (0x02) – Ce type est utilisé par l'émetteur pour demander le statut de réception du récepteur. La longueur de la charge utile de ce message est toujours nulle (0). Il est recommandé à l'émetteur du fichier binaire d'envoyer un message QUERY si aucun message ACK n'a été reçu 1 s après l'envoi du dernier datagramme du bloc de fichier binaire ou après l'envoi d'un message QUERY;
- ACK (0x03) – Ce message est utilisé comme acquittement provenant du récepteur. Ce message est transmis par le récepteur si un fichier binaire complet a été reçu sans erreur ou si des erreurs se sont produites lors de la réception du fichier binaire, par exemple un numéro de séquence a été ignoré. De même, si un récepteur reçoit un message QUERY de la part de l'émetteur, il répond également par un message ACK.

Le transfert non retransmissible utilise uniquement le message DATA, tandis que le transfert retransmissible utilise tous les messages.

7.3.3.6 Identificateur de bloc de fichier binaire

L'identificateur de bloc permet d'identifier chaque bloc de fichier binaire. Un bloc de fichier binaire étant fragmenté en plusieurs datagrammes, l'identificateur de bloc permet d'assembler un ou plusieurs d'entre eux dans un bloc de fichier binaire d'un récepteur.

7.3.3.7 Numéro de séquence et numéro de séquence maximal

Le numéro de séquence (SequenceNum) et le numéro de séquence maximal (MaxSequence) sont utilisés pour les besoins de la segmentation et du réassemblage. Lorsqu'un récepteur extrait un datagramme, il vérifie le numéro de séquence et le numéro de séquence maximal afin de déterminer si des erreurs se sont produites ou s'il a reçu l'intégralité du message.

Le numéro de séquence est également utilisé dans les messages ACK. Dans les messages ACK, le numéro de séquence identifie le dernier message que le récepteur reçoit sans erreur. Le numéro de séquence maximal n'est pas utilisé pour les messages de contrôle (Query).

7.3.3.8 Identification du transfert de fichier binaire distinct

Chaque transfert de fichier binaire doit être identifié par une combinaison unique de SrcID, Device, Channel et BlockID (voir le Tableau 9).

NOTE Si un seul SrcID souhaite à plusieurs reprises envoyer des fichiers binaires (ECDIS envoyant une image d'écran, des informations sur la source des cartes et un échange d'itinéraire, par exemple), alors chaque transfert de fichier binaire est identifié, par exemple: ECDIS numéro 1 envoie l'image écran avec Device = 1 et Channel = 1, et les informations sur la source des cartes avec Device = 1 et Channe = 2.

7.3.4 Structure du descripteur de fichier binaire

Le format du descripteur de fichier binaire est défini dans le Tableau 10.

Tableau 10 – Format du descripteur de fichier binaire

Élément de données	TYPE	Description
Length	DWORD	Définit la longueur du descripteur de fichier binaire, en octets. Il s'agit au moins de la longueur de l'en-tête, y compris les octets réservés. Les éditions ultérieures de l'IEC 61162-450 peuvent ajouter d'autres champs à ce descripteur de fichier, pour autant qu'ils soient conformes à la définition du descripteur de fichier indiquée dans le présent document. Les récepteurs qui ne connaissent pas ces champs supplémentaires doivent les ignorer.
fileLength	DWORD	Définit la longueur du contenu du fichier binaire complet en octets, à l'exclusion des en-têtes et du descripteur.
Status of acquisition	WORD	Statut du renvoi de données. Un zéro est renvoyé pour le fonctionnement normal. Une valeur non nulle est utilisée pour indiquer une condition d'erreur. Un texte descriptif peut être placé dans le champ de texte de statut et d'informations.
AckDestPort	WORD	Numéro d'accès à utiliser pour l'acquittement. Les numéros d'accès admis sont compris entre 60006, 60008 et 60016, 60021 et 60030 (voir le 7.3.8.9).
TypeLength	BYTE	Longueur du champ DataType.
DataType	STRING[n]	Cette chaîne définit le codage du bloc de données en attribuant un type de contenu MIME au bloc de données pour le serveur, suivi d'un caractère nul. Par exemple, "image/jpeg" est utilisé pour le type d'image JPEG.
StatusLength	WORD	Longueur du champ "Status and information text", en octets.
Status and information text	STRING[n]	Informations de statut (codes de fonctionnement réussi ou d'erreur, par exemple). Il peut s'agir d'une ou de plusieurs chaînes, chacune terminée par une valeur nulle binaire.
NOTE 1 Le contenu de l'en-tête de fichier binaire ne fait l'objet d'aucun contrôle d'erreur, ce contrôle étant géré par la couche UDP. Dans le présent document, la somme de contrôle d'en-tête UDP est obligatoire. NOTE 2 MIME est l'abréviation de Multipart Internet Mail Extensions. Le type de contenu MIME était à l'origine utilisé pour les services de messagerie électronique. Il a été par la suite largement utilisé pour de nombreuses autres applications, y compris les applications web. De même, il présente une souplesse suffisante pour prendre en charge les nouveaux types de supports. La spécification et l'enregistrement du type de contenu MIME sont définis dans l'ISOC RFC 4288 et l'ISOC RFC 4289.		

DataType doit être codé par le type de contenu MIME "type/sub-type" et est défini par l'IANA. Le Tableau 11 donne des exemples de type de contenu MIME pour les fichiers binaires et les données compressées. Pour plus d'informations à jour, consulter sur le site web de l'IANA à l'adresse http://www.iana.org/assignments/media-types/.

Tableau 11 – Exemples de types de contenus MIME pour les codes DataType

Type de contenu	Extension de fichier	Type/sous-type MIME
GIF	gif	image/gif
Bitmap Microsoft Windows	bmp	image/x-ms-bmp
Format tar Gnu	gtar	application/x-gtar
Format tar 4.3BSD	tar	application/x-tar
DOS/PC – Archive PKZIP	zip	application/zip
XML	xml	application/xml