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)

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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 It also gives information on projects, replaced and withdrawn publications.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.

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 47.020.70

ISBN 978-2-8322-8714-9

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

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

CONTENTS

FOREWORD 7
1 Scope 9
2 Normative references 9
3 Terms and definitions 10
4 General network and equipment requirements 14
4.1 Network topology example 14
4.2 Basic requirements 15
4.2.1 Requirements for equipment to be connected to the network 15
4.2.2 Additional requirements for network infrastructure equipment 16
4.3 Network function (NF) requirements 16
4.3.1 General requirements 16
4.3.2 Maximum data rate requirements 16
4.3.3 Error logging function 17
4.3.4 Provisions for network traffic filtering – IGMP 19
4.4 System function block (SF) requirements 19
4.4.1 General requirements 19
4.4.2 Implementing configurable transmission groups 19
4.4.3 Assignment of unique system function ID (SFI) 20
4.5 Serial to network gateway function (SNGF) requirements 20
4.5.1 General requirements 20
4.5.2 Serial line output buffer management 22
4.5.3 Datagram output requirements 23
4.5.4 Multi SF serial port 23
4.5.5 Handling malformed data received on serial line 24
4.6 PGN to network gateway function (PNGF) requirements 24
4.6.1 General requirements 24
4.6.2 Output buffer management from IEC 61162-450 network to IEC 61162-3 network 24
4.6.3 Datagram output requirements 25
4.6.4 PGN group number 25
4.7 Other network function (ONF) requirements 25
5 Low level network requirements 25
5.1 Electrical and mechanical requirements 25
5.2 Network protocol requirements 26
5.3 IP address assignment for equipment 27
5.4 Multicast address range 27
5.5 Device address for instrument networks 28
6 Transport layer specification 28
6.1 General 28
6.2 UDP messages 29
6.2.1 UDP multicast protocol 29
6.2.2 Use of multicast addresses and port numbers 29
6.2.3 UDP checksum 31
6.2.4 Datagram size 32
7 Application layer specification 32
7.1 Datagram header 32

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

7.1.1 Valid header 32
7.1.2 Error logging 32
7.2 General IEC 61162-1 sentence transmissions 32
7.2.1 Application of this protocol 32
7.2.2 Types of messages for which this protocol can be used 32
7.2.3 TAG block parameters for sentences transmitted in the datagram 33
7.2.4 Requirements for processing incoming datagrams 39
7.2.5 Error logging for processing incoming datagrams 39
7.3 Binary file transfer using UDP multicast – Single transmitter, multiple receivers 40
7.3.1 Application of this protocol 40
7.3.2 Binary file structure 40
7.3.3 61162-450 header 41
7.3.4 Binary file descriptor structure 43
7.3.5 Binary file data fragment 43
7.3.6 Sender process for binary file transfer 44
7.3.7 Receiver process for binary file transfer 47
7.3.8 Other requirements 49
7.3.9 Error logging 51
7.4 General IEC 61162-3 PGN message transmissions 51
7.4.1 Message structure 51
7.4.2 Message format 52
7.4.3 Address translation requirements 52
7.4.4 Message processing 53
7.4.5 Additional management requirements 53
7.5 System function ID resolution 53
7.5.1 General 54
7.5.2 Transmitter functions 54
7.6 Binary file transfer using TCP point-to-point 54
7.6.1 Definition 54
7.6.2 Data field structure for transfer of files 55
7.6.3 Structure of the transfer stream 57
7.6.4 TCP port and IP addresses 58
7.6.5 Implementation guidance 58
8 Methods of test and required results 59
8.1 Test set-up and equipment 59
8.2 Basic requirements 60
8.2.1 Equipment to be connected to the network 60
8.2.2 Network infrastructure equipment 60
8.2.3 Documentation 60
8.3 Network function (NF) 60
8.3.1 Maximum data rate 60
8.3.2 Error logging function 60
8.4 System function block (SF) 61
8.4.1 General 61
8.4.2 Assignment of unique system function ID (SFI) 61
8.4.3 Implementing configurable transmission groups 61
8.5 Serial to network gateway function (SNGF) 61
8.5.1 General 61

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

8.5.2 Serial line output buffer management 62
8.5.3 Datagram output 62
8.5.4 ~~Datagram output~~ Multi SF serial port 62
8.5.5 Handling malformed data received on serial line 63
8.6 Other network function (ONF) 66
8.7 Low level network 66
8.7.1 Electrical and mechanical requirements 66
8.7.2 Network protocol 66
8.7.3 IP address assignment for equipment 66
8.7.4 Multicast address range 67
8.8 Transport layer 67
8.9 Application layer 67
8.9.1 Application 67
8.9.2 Datagram header 67
8.9.3 Types of messages 68
8.9.4 TAG block parameters 68
8.9.5 General authentication 69
8.10 Error logging 69
8.11 Binary file transfer using UDP multicast – Single transmitter, multiple receiver 70
8.11.1 Sender process test 70
8.11.2 Receiver process test 71
8.11.3 Binary file descriptor test 72
8.11.4 Binary file transfer error logging 72
8.11.5 Maximum outgoing rate 72
8.12 PGN to network gateway function (PNGF) 72
8.12.1 General 72
8.12.2 Output buffer management 72
8.12.3 Datagram output 73
8.12.4 PGN group 73
8.12.5 Address conflicts 73
8.13 System function ID resolution 73
8.14 Binary file transfer using TCP point-to-point 73
8.14.1 Test of transmit client 73
8.14.2 Test of receiver server 74
8.14.3 Maximum outgoing rate 75
8.14.4 TCP port and IP addresses 75
Annex A (normative) Classification of IEC 61162-1 talker identifier mnemonics and sentences 76
A.1 General 76
A.2 Talker identifier mnemonic to transmission group mapping 76
A.3 List of all sentence formatters and the sentence type 78
Annex B (normative) TAG block definitions 83
B.1 Validity 83
B.2 Valid TAG block characters 83
B.3 TAG block format 83
B.4 TAG block "hexadecimal checksum" (*hh) 84
B.5 TAG block "line" 84
B.6 TAG block parameter-code dictionary 85

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

Annex C (normative) Reliable transmission of command-response pair messages 86
C.1 Purpose 86
C.2 Information exchange examples 86
C.3 Characteristics 86
C.4 Requirements 86
C.5 Data flow description 87
C.5.1 Heartbeat message 87
C.5.2 Command response pair 87
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~~ 88
D.1 General 88
D.2 Alternative methods for compatibility 88
D.2.1 Use of IGMP proxy node 88
D.2.2 Use of virtual LAN (VLAN) 88
D.2.3 Use of static multicast switch configuration 89
Annex E (informative) Use of switch setup configuration to filter network traffic 90
Annex F (normative) Sentence to support SFI collision detection 91
F.1 General 91
F.2 SRP – System function ID resolution protocol 91
Annex G (informative) Examples for SRP sentences and SFI collision detection 92
G.1 SFI collision detection 92
G.2 Examples for SRP sentences 92
G.2.1 Redundancy on network level only 92
G.2.2 Examples for redundancy on network and serial (to network) level 96
G.3 Other uses of SRP sentence 98
Annex H (normative) Reserved cluster identifiers 99
Bibliography 100
List of comments 102

Figure 1 – Network topology example 15
Figure 2 – SNGF examples 21
Figure 3 – SNGF example, multi SF serial port 21
Figure 4 – Ethernet frame example for a SBM from a rate of turn sensor 28
Figure 5 – Non re-transmittable sender process 45
Figure 6 – Re-transmittable sender process 47
Figure 7 – Re-transmittable receive process 49
Figure C.1 – Command response communications 86
Figure G.1 – Two separate network interfaces connected to the same single network 92
Figure G.2 – An example of two equipment 93
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 94
Figure G.4 – An example of two equipment 94
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 95
Figure G.6 – An example of two equipment 96

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

Figure G.7 – One equipment with two separate serial interfaces connected through separate SNGFs to the network 97

Table 1 – Syslog message format 18
Table 2 – Syslog error message codes 19
Table 3 – Interfaces, connectors and cables 26
Table 4 – Destination multicast addresses and port numbers 30
Table 5 – Destination multicast addresses and port numbers for binary data transfer 31
Table 6 – Destination multicast addresses and port numbers for other services 31
Table 7 – Description of terms 40
Table 8 – Binary file structure 40
Table 9 – 61162-450 header format 41
Table 10 – Binary file descriptor format 43
Table 11 – Examples of MIME content type for DataType codes 43
Table 12 – Binary file data fragment format 44
Table 13 – Structure for PGN message 51
Table 14 – PGN message descriptor 52
Table 15 – Description of terms 55
Table 16 – Binary file structure 55
Table 17 – Header structure 56
Table 18 – Package data structure 57
Table A.1 – Classification of IEC 61162-1 talker identifier mnemonics 76
Table A.2 – Classification of IEC 61162-1 sentences 78
Table B.1 – Defined parameter-codes 85
Table H.1 – List of reserved cluster identifiers 99

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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.

AVA Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 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.

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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)*

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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

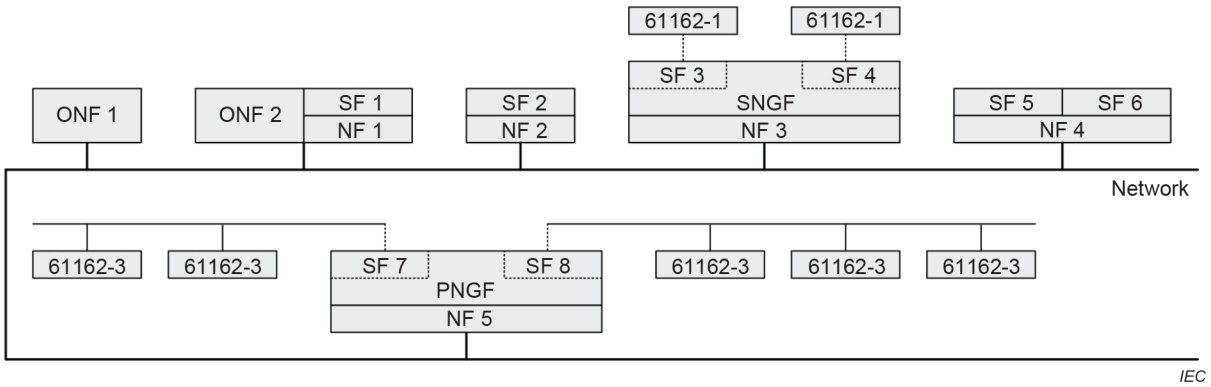
Note 1 to entry: ISOC RFC 768 makes no provision for transport-layer acknowledgement of packets received.

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV



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.

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

- 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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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 un-configured SF and shall not be used by any transmitting SF during normal operation. However, all receiving equipment shall accept the "9999" string.

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

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

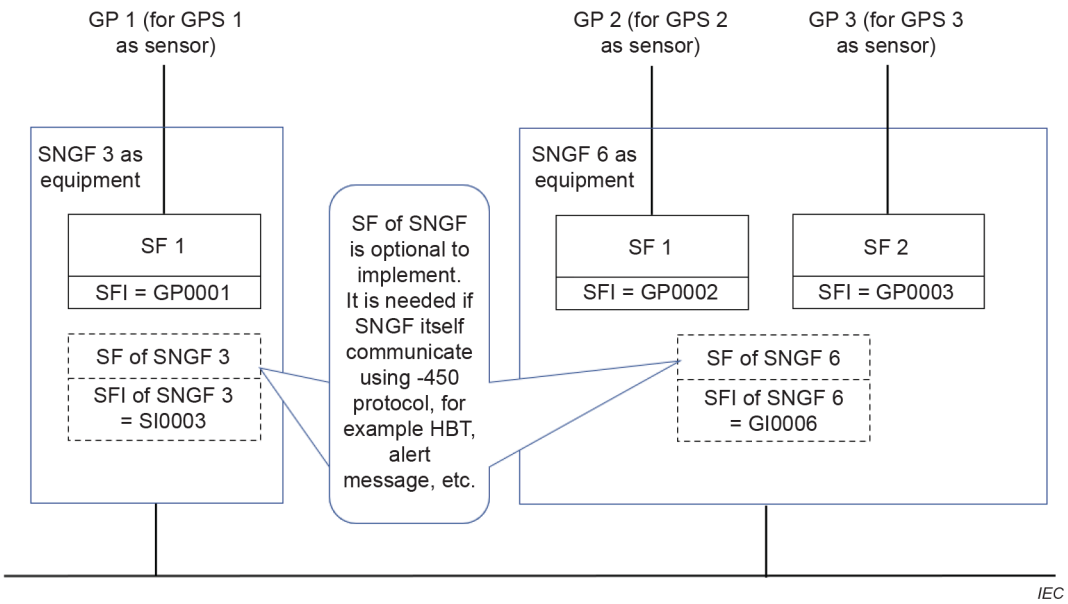


Figure 2 – SNGF examples

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.

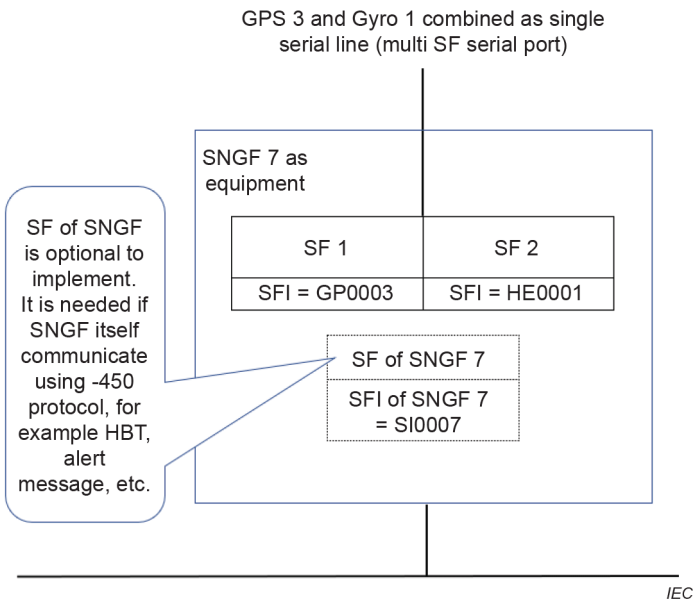


Figure 3 – SNGF example, multi SF serial port

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

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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)

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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;

AVA Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

- 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).

AVA Documents Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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).

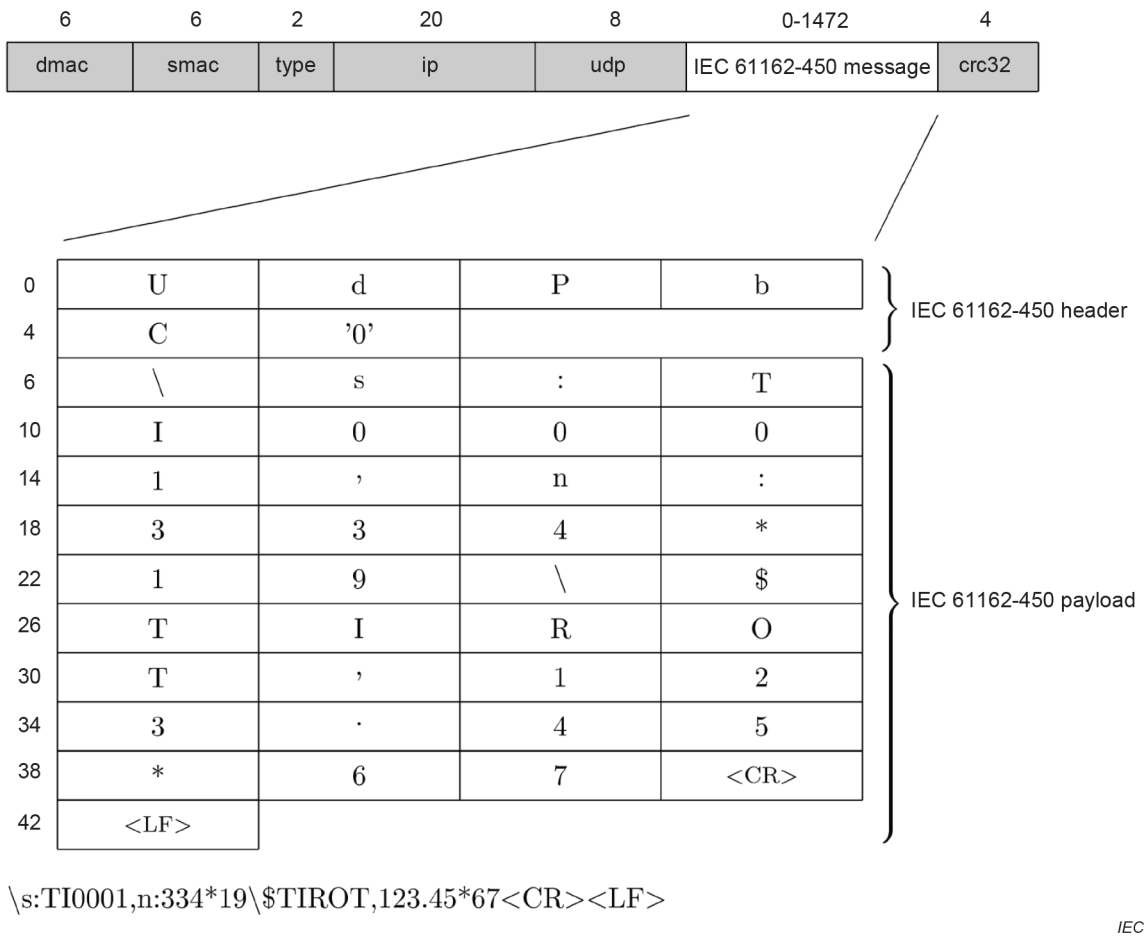


Figure 4 – Ethernet frame example for a SBM from a rate of turn sensor

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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

Documents
Document Sharing Hub

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).

AVA Documents Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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)

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

```
\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

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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
```

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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

AVA Documents
Document Sharing Hub

\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;

AVA Documents
Document Sharing Hub

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)

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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.

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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).

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

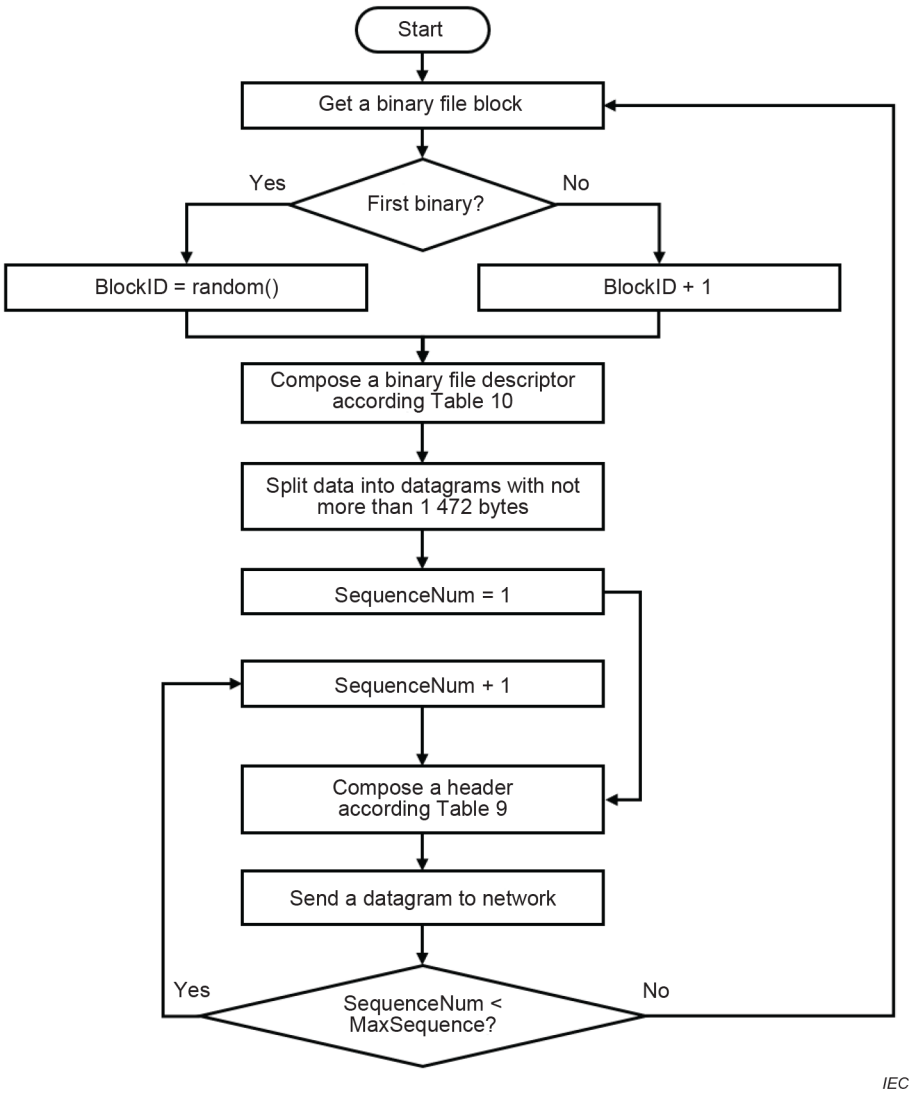


Figure 5 – Non re-transmittable sender process

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**

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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).

Documents
Document Sharing Hub

Full document details: IEC 61162-450 2024 CMV

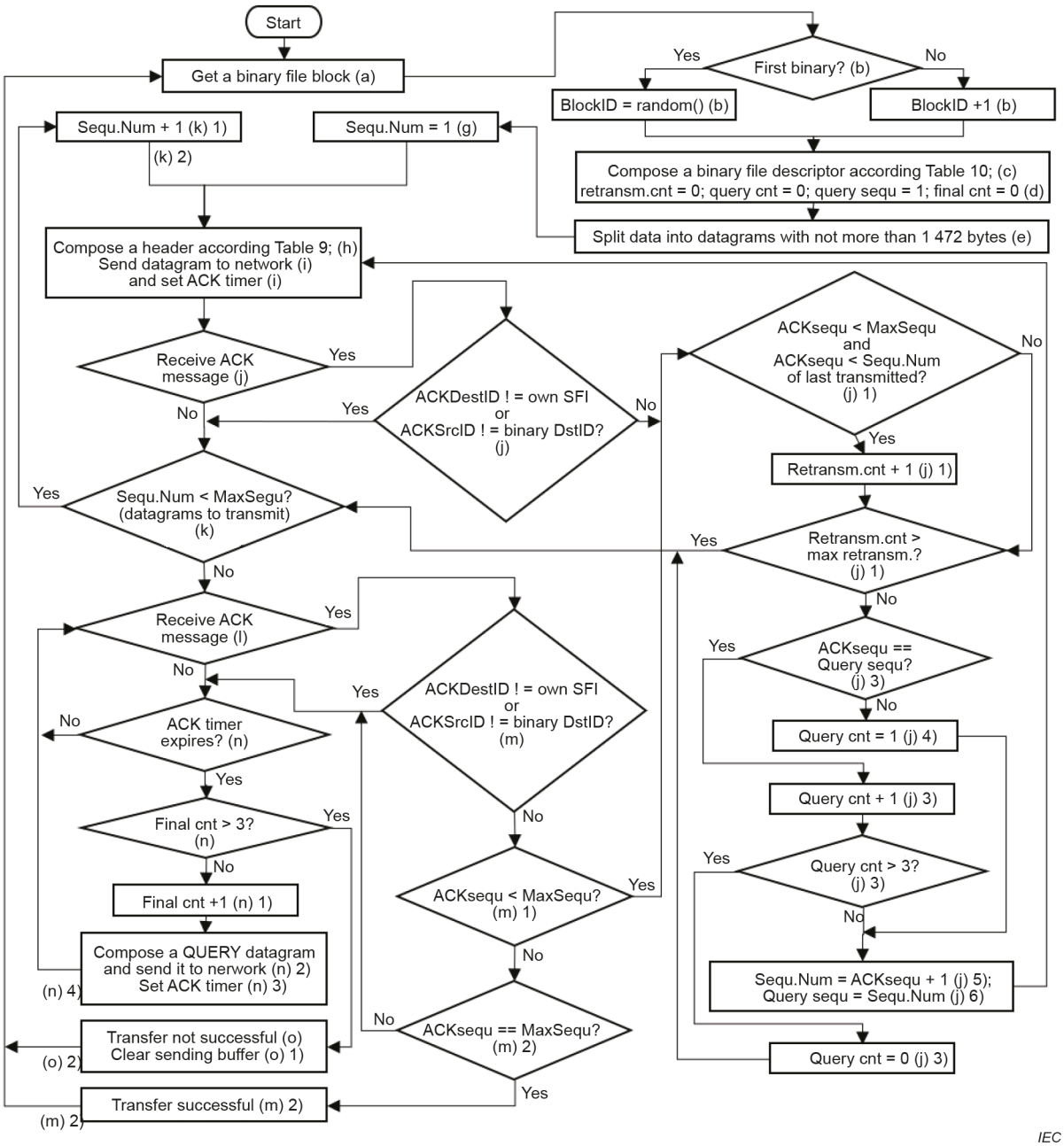


Figure 6 – Re-transmittable sender process

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;

Documents
Document Sharing Hub
Full document details: IEC 61162-450 2024 CMV

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,

AVA Documents
Document Sharing Hub