

DIN EN IEC 61162-460

ICS 47.020.70

Ersatz für
DIN EN 61162-460:2016-07
Siehe Anwendungsbeginn

**Navigations- und Funkkommunikationsgeräte und -systeme für die
Seeschifffahrt –
Digitale Schnittstellen –
Teil 460: Mehrere Datensender und mehrere Datenempfänger –
Ethernet-Verbund – Funktionale und Informationssicherheit
(IEC 61162-460:2018);
Englische Fassung EN IEC 61162-460:2018**

Maritime navigation and radiocommunication equipment and systems –
Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection –
Safety and security
(IEC 61162-460:2018);
English version EN IEC 61162-460:2018

Matériels et systèmes de navigation et de radiocommunication maritimes –
Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet –
Sûreté et sécurité
(IEC 61162-460:2018);
Version anglaise EN IEC 61162-460:2018

Gesamtumfang 80 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
DIN-Normenstelle Schiffs- und Meerestechnik (NSMT)

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2018-06-08 angenommene Europäische Norm als DIN-Norm ist 2019-02-01.

Für DIN EN 61162-460:2016-07 besteht eine Übergangsfrist bis 2021-06-08.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61162-460:2017-04.

Für dieses Dokument ist das nationale Arbeitsgremium K 738 „Elektronische Navigationsinstrumente“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 80 „Maritime navigation and radiocommunication equipment and systems“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN IEC 61162-460 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber DIN EN 61162-460:2016-07 wurden folgende Änderungen vorgenommen:

- a) vermittelnde 460er-Netzknoten und 460er-Netzkoppler sind erforderlich, um IGMP-Herumspionieren zu ermöglichen;
- b) Verkehrsverluste in 460er-Netzkopplern sind berichtet und erklärt;
- c) eine Verbindung zwischen sicheren und unsicheren Bereichen erfordert einen 460er-Netzkoppler als Isolationselement für Nutzlasten;
- d) Klarstellungen zur Funktionalität der Netzüberwachung;
- e) für das Berichten an die Netzüberwachung sind 460er-Protokollumsetzer und drahtlose 460er-Protokollumsetzer nicht länger erforderlich;
- f) alle Alerts von der Netzüberwachung haben normierte Alert-Kennzeichen;
- g) Anhang D beinhaltet weitere Beispiele für die Anwendung dieses Dokuments.

Frühere Ausgaben

DIN EN 61162-460: 2016-07

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

1 Anwendungsbereich

Dieser Teil der IEC 61162 ist eine Ergänzung zur IEC 61162-450, wenn höhere Schutz- und Sicherheitsanforderungen nötig sind, z. B. wegen des höheren Gefahrenpotenzials gegenüber externen Angriffen oder um die Netzwerkintegrität zu verbessern. Dieses Dokument legt die Anforderungen an Geräte und deren Prüfverfahren in einem IEC 61162-460-konformen Netz sowie Anforderungen an das Netz selbst und Anforderungen bei der Zusammenschaltung des Netzes mit anderen Netzwerken fest. Dieses Dokument enthält auch Anforderungen an ein redundantes IEC 61162-460-konformes Netz.

Dieses Dokument führt keine neuen Anwendungsprotokollanforderungen zu den in IEC 61162-450 festgelegten ein.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 61162-450 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

^{N1} Nationale Fußnote: Die Nummerierung aus IEC 61162-460:2018-05 wurde beibehalten.

3.1

450er-Netzknoten

(en: 450-Node)

Gerät, das mit DIN EN 61162-450 konform ist und das mit dem vorliegenden Dokument vorgegebene zusätzliche Anforderungen erfüllt

Anmerkung 1 zum Begriff: Dies umfasst auch Netzknoten, die nur den ONF-Funktionsblock implementiert haben.

3.2

460er-Netzkoppler

(en: 460-Forwarder)

Gerät der Netzinfrastruktur, das sicher Datenströme zwischen einem 460er-Netz und anderen kontrollierten Netzen einschließlich anderen 460er-Netzen vermitteln kann

3.3

460er-Protokollumsetzer

(en: 460-Gateway)

Gerät der Netzinfrastruktur, welches 460er-Netze und unkontrollierte Netze verbindet und die mit diesem Dokument vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.4

460er-Netz

(en: 460-Network)

Netz, das nur aus 460er-Netzknoten, 460er-vermittelnden Netzknoten, 460er-Netzkopplern, 460er-Protokollumsetzern und drahtlosen 460er-Protokollumsetzern sowie 450er-Netzknoten besteht

3.5

460er-Netzknoten

(en: 460-Node)

Gerät der Netzinfrastruktur, das mit den Anforderungen an einen 450er-Netzknoten konform ist und die mit diesem Dokument vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.6

vermittelnder 460er-Netzknoten

(en: 460-Switch)

Gerät der Netzinfrastruktur, welches zur Zusammenschaltung von Netzknoten in einem 460er-Netz genutzt wird und die mit diesem Dokument vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.7

drahtloser 460er-Protokollumsetzer

(en: 460-Wireless gateway)

Gerät der Netzinfrastruktur, welches ein 460er-Netz und drahtlose Netze verbindet und die mit diesem Dokument vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.8

Advanced Encryption Standard

AES

(en: advanced encryption standard)

symmetrischer Blockschlüsselalgorithmus, der auf einem Substitutions-Permutations-Netzwerk (SPN) basiert und nicht den Verschlüsselungsstandard (DES) nach Feistel anwendet

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.9

Alarmmeldung

(en: alarm)

Alert höchster Priorität, der eine Situation oder eine Bedingung ankündigt, die unmittelbare Aufmerksamkeit, Entscheidung und falls notwendig Maßnahmen der Brückenmannschaft erfordert, um die sichere Schiffsführung sicherzustellen

3.10**Protokollumsetzer in der Anwendungsebene**

(en: application level gateway)

Gerät der Netzinfrastruktur, welches ein 460er-Netz mit anderen Netzen verbindet und die mit diesem Dokument vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.11**Hintertür**

(en: backdoor)

installiertes Programm, das den Fernzugang zu einem Computer durch Bereitstellung eines Verfahrens zur Umgehung der normalen Authentifizierung erlaubt

3.12**kontrolliertes Netz**

(en: controlled network)

jedes Netz, das in einer Art entwickelt wurde und betrieben wird, dass Behörden durch schriftlichen Nachweis zufriedengestellt sind, dass das Netz keine Informationssicherheitsrisiken für angeschlossene Netzknoten darstellt

Anmerkung 1 zum Begriff: Zum Beispiel jedes DIN EN 61162-450-konforme Netz, das durch eine Klassifizierungsgesellschaft, einen Flaggenstaat oder eine anerkannte Organisation zugelassen ist.

3.13**Kategorie-B-Alert**

(en: category B alert)

Alarm, bei dem neben der Information, die am zentralen Alert-Management HMI angezeigt werden kann, keine Zusatzinformation als Entscheidungshilfe notwendig ist

3.14**Vorsichtsmeldung**

(en: caution)

niedrigste Priorität eines Alerts

Anmerkung 1 zum Begriff: Warnung, die die Aufmerksamkeit der Brückenmannschaft bezüglich einer Bedingung erregt, die keine Alarmmeldung oder Warnmeldung rechtfertigt, aber bei der normalen Bewertung der Situation oder durch die gegebene Information trotzdem Aufmerksamkeit erfordert.

3.15**entmilitarisierte Zone****DMZ**

(en: demilitarized zone)

physikalisches oder logisches Teilnetz, das von extern erreichbare Dienste enthält und einem größeren und ungesicherten Netz, gewöhnlich dem Internet, offenlegt

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.16**Dienstverweigerung****DoS**

(en: denial of Service)

Versuch, rechtmäßige Nutzer daran zu hindern, auf eine Maschine oder eine Netzressource zuzugreifen

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.17**Informationsfluss**

(en: flow)

Kombination der folgenden Informationen: Ursprungs- und Ziel-MAC-Adresse, Ursprungs- und Ziel-IP-Adresse, Protokoll, Ursprungs- und Ziel-Anschluss-Nummer

3.18

Fehlermöglichkeits- und -einflussanalyse FMEA

(en: failure mode and effects analysis)

Verfahren nach DIN EN 60812 zur Analyse eines Systems zur Identifizierung potenzieller Fehlermöglichkeiten, ihrer Ursachen und Auswirkungen auf die Systemleistung

3.19

Fehlermöglichkeits-, Einfluss- und Kritikalitätsanalyse FMECA

(en: failure mode, effects and criticality analysis)

analytisches Verfahren nach DIN EN 60812, das Mittel beinhaltet, um den Schweregrad der Fehlermöglichkeiten einzustufen

Anmerkung 1 zum Begriff: FMECA erweitert FMEA durch Ergänzung der Kritikalitätsanalyse, die dazu verwendet wird, die Wahrscheinlichkeit von Fehlerarten gegenüber dem jeweiligen Schweregrad und dessen Folgen zu bewerten.

3.20

Internet Control Message Protocol ICMP

(en: internet control message protocol)

Protokoll entsprechend ISOC RFC 792

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.21

Internet Group Management Protocol IGMP

(en: internet group management protocol)

Protokoll entsprechend ISOC RFC 1112 (Version 1), ISOC RFC 2236 (Version 2) und ISOC RFC 4604 (Version 3)

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.22

Verlustrate

(en: loss rate)

Menge der durch den Empfänger aus einem Informationsfluss verlorenen Daten als Anzahl der verlorenen Pakete gegenüber der am Eingang eines Geräts gemessenen Gesamtmenge von Paketen

Anmerkung 1 zum Begriff: Die Verlustrate wird in Prozent ausgedrückt.

3.23

Schadsoftware böartiger Code

(en: malware; malicious code)

Software, die angewandt oder entwickelt wurde, um den Computerbetrieb zu unterbrechen

3.24

maximale Netzlast

(en: maximum network load)

kumulierte, maximale Gesamtverkehrsmenge aller Netzknoten und Netzinfrastrukturkomponenten eines einzelnen 460er-Netzes

Anmerkung 1 zum Begriff: Die maximale Netzlast wird in Bytes je Sekunde (B/s) gemessen.

3.25

maximale Übertragungsrate

(en: maximum transmission rate)

maximale Anzahl von Bytes je Sekunde, die durch einen Netzknoten oder eine Netzinfrastruktureinrichtung übertragen werden kann

3.26**Multiple spanning tree protocol
MSTP**

(en: multiple spanning tree protocol)

Protokoll nach IEEE 802.1Q, welches eine Erweiterung von RSTP für VLANs ist

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.27**Nachbar-MAC-Adresse**

(en: neighbour MAC address)

MAC-Adresse von verbundenem 450er- oder 460er-Netznoten, wie vom vermittelnden 460er-Netznoten aus gesehen und durch SNMP signalisiert

3.28**Netzinfrasturkturkomponente**

(en: network infrastructure components)

Gerät, das zumindest zwei Netznoten in einem 460er-Netz und zwei unterschiedliche Netze verbindet, wie z. B. vermittelnder 460er-Netznoten, 460er-Netzkoppler, 460er-Protokollumsetzer und drahtlose 460er-Protokollumsetzer

3.29**nominelle Netzkapazität**

(en: nominal network capacity)

Netzkapazität als eine Byte-Rate, die auf der Konfiguration basiert

Anmerkung 1 zum Begriff: Die Kapazität ist die niedrigste Kapazität eines vermittelnden Netznotens im Netz, um den Gesamtverkehr zu steuern.

Anmerkung 2 zum Begriff: Dies wird zur Festlegung der Leistungsfähigkeit von Geräten benutzt.

3.30**sonstige Netzfunktion****ONF**

(en: other network function)

Funktionsblock mit Schnittstelle(n) zum Netz, wie in DIN EN 61162-450 festgelegt

Anmerkung 1 zum Begriff: ONF stellt eine Funktion dar, die es erlaubt, die Infrastruktur eines Netzes nach DIN EN 61162-450 mitzubedenutzen, aber nicht die in DIN EN 61162-450 festgelegten Protokolle nutzt.

Anmerkung 2 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.31**Rapid Spanning Tree Protocol****RSTP**

(en: rapid spanning tree protocol)

Protokoll nach IEEE 802.1D zum Berechnen und Konfigurieren der aktiven Topologie eines Netzwerks

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.32**austauschbare externe Datenquelle****REDS**

(en: removable external data source)

durch den Anwender austauschbare, nicht-netzseitige Datenquelle, einschließlich Compact Disks, Speicher-Sticks oder Bluetooth¹-Geräten, aber nicht darauf beschränkt

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

¹

Bluetooth ist die Handelsmarke eines durch die Bluetooth Special Interest Group gelieferten Produkts. Diese Information ist für die Bequemlichkeit der Nutzer dieses Dokuments gegeben und stellt keine Billigung des Produkts durch IEC dar. Gleichwertige Produkte dürfen verwendet werden, wenn nachgewiesen werden kann, dass sie zu denselben Ergebnissen führen.

3.33

Netzfernüberwachung RMON

(en: remote network monitoring)

standardisierte Überwachungsspezifikation, wie in ISOC RFC 3577 beschrieben

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.34

ringförmige Netzstruktur

(en: ring topology)

Netzstruktur, bei der jeder Netzknoten mit zwei anderen Netzknoten in Reihe geschaltet verbunden ist

3.35

RSA-Kryptosystem

(en: RSA)

Kryptosystem mit öffentlichem Schlüssel, wie in IEEE 1363 beschrieben

3.36

Systemsicherheit

(en: safety)

Schutz von Netzen gegen ungewollte Bedrohungen wie z. B. Systemfehlfunktion, Falschkonfiguration und Fehlbedienung

3.37

Sicherheitsbereich

(en: secure area)

Bereich mit definierter physikalischer Begrenzung und mit Barrieren, mit physikalischen Eingangskontrollen oder mit Zugriffsschutz und Zugangsbeobachtung

Anmerkung 1 zum Begriff: Eine Steuerungsbrücke eines Schiffs mit geschlossenen Konsolen und Zugriffsbeobachtung durch den Kapitän oder den Wachoffizier ist ein Beispiel für einen Sicherheitsbereich.

3.38

Informationssicherheit

(en: security)

Schutz für Netze gegen beabsichtigte Bedrohungen wie z. B. Viren, Würmer, Dienstblockade-Angriffen, unerlaubter Zugriff, usw.

3.39

Simple Network Management Protocol SNMP

(en: simple network management protocol)

Protokoll nach ISOC RFC 3411 zur Übertragung von Verwaltungsinformation(en)

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.40

SNMP-Fänger

(en: SNMP-Trap)

Verfahren zur Sammlung von Ereignissen und statistischer/n Information(en) von vermittelnden Netzknoten gemäß ISOC RFC 1157, ISOC RFC 2021 und ISOC RFC 2819

3.41

Bordnetz

(en: shipborne network)

Datennetzinfrastruktur an Bord eines Schiffes, um Daten zwischen Geräten an Bord auszutauschen

Anmerkung 1 zum Begriff: Es kann über Satelliten oder andere Mittel mit dem Land verbunden sein oder auch nicht.

3.42**Schnüffeln**

(en: sniffing)

Beobachtung und Analyse des Netzverkehrs

3.43**Datenstrom**

(en: stream)

Kombination aller Informationsflüsse eines Gerätes, die dasselbe Protokoll benutzen

3.44**Syslog-Protokoll**

(en: syslog)

Protokoll entsprechend ISO/IEC RFC 5424, welches für eine externe Erfassung nach DIN EN 61162-450 benutzt wird

3.45**Systemintegrator**

(en: system integrator)

für die Funktionalität eines integrierten 460er-Netzes verantwortliche Person oder Organisation

3.46**Bedrohung**

(en: threat)

mögliche Ursache eines Störfalles in der Informationssicherheit eines Computers, die zu einem Schaden am System führen kann

3.47**Datenverkehr**

(en: traffic)

Kombination aller Datenströme von einem Gerät

3.48**unkontrolliertes Netz**

(en: uncontrolled network)

Datennetzwerk, das kein EN 61162-450-konformes, kein EN 61162-460-konformes oder ein kontrolliertes Netz ist

BEISPIEL Drahtlose Netze.

3.49**virtuelles lokales Netz****VLAN**

[en: virtual local area network]

Netzwerk nach IEEE 802.1Q, bestehend aus miteinander über Brücken verbundenen Netzwerken

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.50**virtuelles Privatnetz****VPN**

(en: virtual private network)

Erweiterung eines Privatnetzes durch verschachtelten, verschlüsselten und authentifizierten Verbindungen über mitbenutzte oder öffentliche Netze

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

3.51**Warnmeldung**

(en: warning)

kündigt eine Situation oder Bedingung an, die Aufmerksamkeit, aber keine unmittelbare Aufmerksamkeit oder Aktivität der Brückenbesatzung erfordert

Anmerkung 1 zum Begriff: Warnmeldungen werden vorsorglich angezeigt, um die Brückenbesatzung auf veränderte Situationen hinzuweisen, die noch nicht unmittelbar gefährlich sind, dies aber werden können, wenn keine vorausschauende Entscheidung getroffen oder nichts unternommen wird.

3.52

drahtloser Zugangspunkt

(en: wireless access point; wireless AP)

Gerät, das drahtlose Geräte mit drahtgebundenen Geräten mittels unterschiedlichen Drahtlostechniken, wie z. B. Wi-Fi, Bluetooth, verbindet

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprache.

English Version

Maritime navigation and radiocommunication equipment and
systems - Digital interfaces - Part 460: Multiple talkers and
multiple listeners - Ethernet interconnection - Safety and security
(IEC 61162-460:2018)

Matériels et systèmes de navigation et de
radiocommunication maritimes - Interfaces numériques -
Partie 460: Émetteurs multiples et récepteurs multiples -
Interconnexion Ethernet - Sécurité et sécurité
(IEC 61162-460:2018)

Navigations- und Funkkommunikationsgeräte und -systeme
für die Seeschifffahrt - Digitale Schnittstellen -
Teil 460: Mehrere Datensender und mehrere
Datenempfänger - Ethernet-Verbund - Funktionale und
Informationssicherheit
(IEC 61162-460:2018)

This European Standard was approved by CENELEC on 2018-06-08. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 80/879/FDIS, future edition 2 of IEC 61162-460, prepared by IEC/TC 80 "Maritime navigation and radiocommunication equipment and systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 61162-460:2018.

The following dates are fixed:

- latest date by which the document has to be (dop) 2019-03-08
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2021-06-08
standards conflicting with the
document have to be withdrawn

This document supersedes EN 61162-460:2015.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61162-460:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60812	NOTE	Harmonized as EN 60812.
IEC 61162 Series	NOTE	Harmonized as EN 61162 Series.
IEC 61162-1	NOTE	Harmonized as EN 61162-1.
IEC 61162-2	NOTE	Harmonized as EN 61162-2.
IEC 62388	NOTE	Harmonized as EN 62388.
IEC 62439 Series	NOTE	Harmonized as EN 62439 Series.
IEC 62439-1	NOTE	Harmonized as EN 62439-1.
IEC 62439-2	NOTE	Harmonized as EN 62439-2.
IEC 62439-3	NOTE	Harmonized as EN 62439-3.
IEC 62439-4	NOTE	Harmonized as EN 62439-4.
IEC 62439-5	NOTE	Harmonized as EN 62439-5.
IEC 62439-6	NOTE	Harmonized as EN 62439-6.
IEC 62940	NOTE	Harmonized as EN 62940.
ISO 9241-12	NOTE	Harmonized as EN ISO 9241-12 ^{Z1} .

^{Z1} Superseded by EN ISO 9241-112 (ISO 9241-112) and EN ISO 9241-125 (ISO 9241-125).

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60945	–	Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results	EN 60945	–
IEC 61162-450	2018	Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection	EN IEC 61162-450	2018
IEC 61924-2	2012	Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results	EN 61924-2	2013
IEC 62288	2014	Maritime navigation and radiocommunication equipment and systems – Presentation of navigation-related information on shipborne navigational displays – General requirements, methods of testing and required test results	EN 62288	2014
IEEE 802.1D	2004	IEEE Standard for local and metropolitan area networks – Media Access Control (MAC) Bridges	–	–
IEEE 802.1Q	–	IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges and Virtual Bridges	–	–
IETF RFC 792	1981	Internet Control Message Protocol (ICMP)	–	–
IETF RFC 1112	1989	Host Extensions for IP Multicasting (SNMP)	–	–
IETF RFC 1157	1990	Simple Network Management Protocol (SNMP)	–	–
IETF RFC 2021	1997	Remote Network Monitoring Management Information Base	–	–
IETF RFC 2236	1997	Internet Group Management Protocol, Version–2	–	–
IETF RFC 2819	2000	Remote Network Monitoring Management Information Base	–	–
IETF RFC 3411	2002	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	–	–
IETF RFC 3577	2003	Introduction to the RMON family of MIB modules	–	–

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IETF RFC 4604	2006	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast	–	–
IETF RFC 5424	2009	The Syslog Protocol	–	–

CONTENTS

European foreword	2
Annex ZA (normative) Normative references to international publications with their corresponding European publications	3
1 Scope	9
2 Normative references	9
3 Terms and definitions	10
4 High-level requirements	16
4.1 Overview	16
4.2 Description	16
4.3 General requirements	17
4.3.1 Equipment and system requirements	17
4.3.2 Physical composition requirements	17
4.3.3 Logical composition requirements	17
4.4 Physical component requirements	18
4.4.1 450-Node	18
4.4.2 460-Node	18
4.4.3 460-Switch	18
4.4.4 460-Forwarder	19
4.4.5 460-Gateway and 460-Wireless gateway	19
4.5 Logical component requirements	19
4.5.1 Network monitoring function	19
4.5.2 System management function	19
4.6 System documentation requirements	19
4.7 Secure area requirements	20
5 Network traffic management requirements	20
5.1 460-Node requirements	20
5.2 460-Switch requirements	20
5.2.1 Resource allocation	20
5.2.2 Loop prevention	21
5.3 460-Forwarder requirements	21
5.3.1 Traffic separation	21
5.3.2 Resource allocation	21
5.3.3 Traffic prioritization	22
5.4 System design requirements	22
5.4.1 Documentation	22
5.4.2 Traffic	23
5.4.3 Connections between secure and non-secure areas	23
6 Security requirements	23
6.1 Security scenarios	23
6.1.1 Threat scenarios	23
6.1.2 Internal threats	23
6.1.3 External threats	24
6.2 Internal security requirements	24
6.2.1 General	24
6.2.2 Denial of service protection	24

6.2.3	REDS security	25
6.2.4	Access control	25
6.3	External security requirements	26
6.3.1	Overview	26
6.3.2	Firewalls	26
6.3.3	Direct communication	27
6.3.4	460-Node	27
6.3.5	460-Gateway	28
6.3.6	460-Wireless gateway	29
6.4	Additional security issues	29
7	Redundancy requirements	29
7.1	General requirements	29
7.1.1	General	29
7.1.2	Interface redundancy	30
7.1.3	Device redundancy	30
7.2	460-Node requirements	31
7.3	460-Switch requirements	31
7.4	460-Forwarder requirements	31
7.5	460-Gateway and 460-Wireless gateway requirements	31
7.6	Network monitoring function requirements	31
7.7	System design requirements	31
8	Network monitoring requirements	31
8.1	Network status monitoring	31
8.1.1	460-Network	31
8.1.2	460-Node	31
8.1.3	460-Switch	32
8.1.4	460-Forwarder	32
8.2	Network monitoring function	33
8.2.1	General	33
8.2.2	Network load monitoring function	33
8.2.3	Redundancy monitoring function	34
8.2.4	Network topology monitoring function	34
8.2.5	Syslog recording function	36
8.2.6	Redundancy of network monitoring function	36
8.2.7	Alert management	36
9	Controlled network requirements	37
10	Methods of testing and required test results	38
10.1	Subject of tests	38
10.2	Test site	38
10.3	General requirements	39
10.4	450-Node	39
10.5	460-Node	39
10.5.1	Network traffic management	39
10.5.2	Security	40
10.5.3	Redundancy	42
10.5.4	Monitoring	42
10.6	460-Switch	42

10.6.1	Resource allocation	42
10.6.2	Loop prevention	43
10.6.3	Security	43
10.6.4	Monitoring.....	44
10.7	460-Forwarder	44
10.7.1	Traffic separation	44
10.7.2	Resource allocation	45
10.7.3	Traffic prioritisation	45
10.7.4	Security	46
10.7.5	Monitoring.....	47
10.8	460-Gateway.....	47
10.8.1	Denial of service behaviour	47
10.8.2	Access control to configuration setup	47
10.8.3	Communication security	48
10.8.4	Firewall.....	48
10.8.5	Application server	49
10.8.6	Interoperable access to file storage of DMZ	49
10.8.7	Additional security.....	49
10.9	460-Wireless gateway	50
10.9.1	General	50
10.9.2	Security	50
10.10	Controlled network	50
10.11	Network monitoring function	50
10.11.1	General	50
10.11.2	Network load monitoring function.....	51
10.11.3	Redundancy monitoring function.....	51
10.11.4	Network topology monitoring function	52
10.11.5	Syslog recording function	52
10.11.6	Alert management.....	52
10.12	System level	54
10.12.1	General	54
10.12.2	System management function.....	54
10.12.3	System design	55
10.12.4	Network monitoring function	56
10.12.5	Network load monitoring function.....	56
10.12.6	Redundancy monitoring function.....	56
10.12.7	Network topology monitoring function	57
Annex A (informative)	Communication scenarios between an IEC 61162-460 network and uncontrolled networks.....	58
A.1	General.....	58
A.2	Routine off-ship.....	58
A.3	Routine on-ship.....	59
A.4	460-Gateway usage for direct connection with equipment	59
Annex B (informative)	Summary of redundancy protocols in IEC 62439 (all parts)	60
Annex C (informative)	Guidance for testing	61
C.1	Methods of test	61
C.2	Observation	61
C.3	Inspection of documented evidence	61

C.4	Measurement	61
C.5	Analytical evaluation	62
Annex D (informative)	Some examples to use this document	63
Annex E (normative)	IEC 61162 interfaces for the network monitoring function	67
Annex F (informative)	Distribution of functions around 460-Network	68
Bibliography		69
Figure 1	– Functional overview of IEC 61162-460 requirement applications	16
Figure 2	– 460-Network with 460-Gateway	26
Figure 3	–Example of redundancy	30
Figure 4	– Example of network status recording information	33
Figure A.1	– Usage model for communication between a IEC 61162-460 network and shore networks	58
Figure D.1	– 460-Forwarder used between two networks	63
Figure D.2	– 460-Forwarder used between two networks	63
Figure D.3	– 460-Gateway used for e-Navigation services	64
Figure D.4	– 460-Gateway used for remote maintenance	64
Figure D.5	– 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices	65
Figure D.6	– 460-Forwarder used to separate a radar system based on its own controlled network from a network of -460 devices	66
Figure E.1	– Network monitoring function logical interfaces	67
Table 1	– Traffic prioritization with CoS and DSCP	22
Table 2	– Summary of alert of network monitoring	36
Table B.1	– Redundancy protocols and recovery times	60
Table E.1	– Sentences received by the network monitoring function	67
Table E.2	– Sentences transmitted by the network monitoring function	67
Table F.1	– Distribution of functions around 460-Network	68
Table F.2	– Equipment standards referencing IEC 61162-460	68

1 Scope

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

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

2 Normative references

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

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

IEC 61162-450:2018, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection*

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

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

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

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

INTERNET SOCIETY (ISOC). RFC 792, *Internet Control Message Protocol (ICMP), Standard STD0005 (and updates)* [online]. Edited by J. Postel. September 1981 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc792>

INTERNET SOCIETY (ISOC). RFC 1112, *Host Extensions for IP Multicasting* [online]. Edited by S. Deering. August 1989 [viewed 2018-01-08]. Available at <https://www.ietf.org/rfc/rfc1112.txt>

INTERNET SOCIETY (ISOC). RFC 1157, *A Simple Network Management Protocol (SNMP)* [online]. Edited by J. Case et al. May 1990 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc1157>

INTERNET SOCIETY (ISOC). RFC 2021, *Remote Network Monitoring Management Information Base* [online]. Edited by S. Waldbusser. January 1997 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2021>

INTERNET SOCIETY (ISOC). RFC 2236, *Internet Group Management Protocol, Version 2* [online]. Edited by W. Fenner. November 1997 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2236>

INTERNET SOCIETY (ISOC). RFC 2819, *Remote Network Monitoring Management Information Base* [online]. Edited by S. Waldbusser. May 2000 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc2819>

INTERNET SOCIETY (ISOC). RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* [online]. Edited by D. Harrington. December 2002 [viewed 2018-01-08]. Available at <https://www.ietf.org/rfc/rfc3411.txt>

INTERNET SOCIETY (ISOC). RFC 3577, *Introduction to the RMON family of MIB modules* [online]. Edited by S. Waldbusser. August 2003 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc3577>

INTERNET SOCIETY (ISOC). RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast* [online]. Edited by H. Holbrook et al. August 2006 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc4604>

INTERNET SOCIETY (ISOC). RFC 5424, *The Syslog Protocol* [online]. Edited by R. Gerhards. March 2009 [viewed 2018-01-08]. Available at <https://tools.ietf.org/html/rfc5424>

3 Terms and definitions

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

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

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

3.1

450-Node

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

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

3.2

460-Forwarder

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

3.3

460-Gateway

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

3.4

460-Network

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

3.5

460-Node

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

3.6

460-Switch

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

3.7

460-Wireless gateway

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

3.8

advanced encryption standard

AES

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

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

3.9

alarm

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

3.10

application level gateway

network infrastructure device that connects 460-Networks with other networks and which satisfies the safety and security requirements as specified in this document

3.11

backdoor

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

3.12

controlled network

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

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

3.13

category B alert

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

3.14

caution

lowest priority of an alert

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

3.15

demilitarized zone

DMZ

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

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

3.16

denial of service

DoS

attempt to prevent legitimate users from accessing a machine or network resource

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

3.17

flow

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

3.18

failure mode and effects analysis

FMEA

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

3.19

failure mode, effects and criticality analysis

FMECA

analytic method as specified in IEC 60812 that includes a means of ranking the severity of the failure modes

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

3.20

internet control message protocol

ICMP

protocol according to ISOC RFC 792

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

3.21

internet group management protocol

IGMP

protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and ISOC RFC 4604 (version 3)

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

3.22

loss rate

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

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

3.23

malware

malicious code

software used or created to disrupt computer operation

3.24

maximum network load

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

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

3.25

maximum transmission rate

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

3.26

multiple spanning tree protocol

MSTP

protocol, according to IEEE 802.1Q, which is an extension of RSTP for VLANs

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

3.27

neighbour MAC address

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

3.28

network infrastructure component

device that connect at least two nodes in a 460-Network and two different networks, such as 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

3.29

nominal network capacity

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

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

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

3.30

other network function

ONF

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

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

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

3.31

rapid spanning tree protocol **RSTP**

protocol according to IEEE 802.1D for calculating and configuring the active topology of a network

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

3.32

removable external data source **REDS**

user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth¹ devices

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

3.33

remote network monitoring **RMON**

standard monitoring specification as described in ISOC RFC 3577

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

3.34

ring topology

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

3.35

RSA

public-key cryptosystem as described in IEEE 1363

3.36

safety

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

3.37

secure area

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

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

3.38

security

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

3.39

simple network management protocol **SNMP**

protocol according to ISOC RFC 3411 used to convey management information

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

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