

DIN EN 61162-460



ICS 47.020.70

**Navigations- und Funkkommunikationsgeräte und -systeme
für die Seeschifffahrt –
Digitale Schnittstellen –
Teil 460: Mehrere Datensender und mehrere Datenempfänger –
Ethernet-Verbund – Funktionale und Informationssicherheit
(IEC 61162-460:2015);
Englische Fassung EN 61162-460:2015**

Maritime navigation and radiocommunication equipment and systems –
Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection –
Safety and security
(IEC 61162-460:2015);
English version EN 61162-460:2015

Matériels et systèmes de navigation et de radiocommunication maritimes –
Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet –
Sûreté et sécurité
(IEC 61162-460:2015);
Version anglaise EN 61162-460:2015

Gesamtumfang 71 Seiten

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

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2015-09-22 angenommene Europäische Norm als DIN-Norm ist 2016-07-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61162-460:2015-02.

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 dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- 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 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.

Nationaler Anhang NA (informativ)

Die deutschen Übersetzungen haben Empfehlungscharakter und können nur die ungefähre Begrifflichkeit in Deutsch wiedergeben. Unter Experten wird empfohlen, ausschließlich die englischen Fachbegriffe zu verwenden, um die Gefahr von Missverständnissen zu reduzieren.

1 Anwendungsbereich^{N1)}

Dieser Teil der IEC 61162 ist eine Ergänzung zur Norm IEC 61162-450, wenn höhere Schutz- und Sicherheitsanforderungen geboten sind, z. B. wegen des höheren Gefahrenpotenzials gegenüber externen Angriffen, oder um die Netzwerkintegrität zu verbessern. Diese Norm legt die Leistungsanforderungen 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. Diese Norm enthält auch Anforderungen an ein redundantes IEC 61162-460-konformes Netz.

Diese Norm erweitert die informative Anleitung in IEC 61162-450:2011, Anhang D. Zu den mit IEC 61162-450 festgelegten Anwendungsprotokollanforderungen werden mit dieser Norm keine neuen eingeführt.

3 Begriffe

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

3.1

450er-Netzknoten

(en: 450-Node)

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

Anmerkung 1 zum Begriff: Das 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 dieser Norm 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 dieser Norm vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

^{N1)} Nationale Fußnote: Die Nummerierung der IEC 61162-460:2015 wurde beibehalten.

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 dieser Norm 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 dieser Norm vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.8

Advanced Encryption Standard

(en: advanced encryption standard)

AES

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

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 zu gewährleisten

3.10

Protokollumsetzer in der Anwendungsebene

(en: application level gateway)

Gerät der Netzinfrastruktur, welches ein 460er-Netz mit anderen Netzen verbindet und die mit dieser Norm 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 keine Informationssicherheitsrisiken für angeschlossene Netzknoten darstellt

Anmerkung 1 zum Begriff: DIN EN 61162-450-konformes Netz, das durch eine Klassifizierungsgesellschaft, einen Flaggenstaat oder eine anerkannte Organisation zugelassen ist

3.13

Kategorie-B-Alerts

(en: category B alerts)

Alarmer, bei denen 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**

(en: demilitarized zone)

DMZ

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

3.16**Dienstverweigerung**

(en: denial of Service)

DoS

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

3.17**Informationsfluss**

(en: flow)

Kombination der folgenden Information: Ursprungs- und Ziel-MAC-Adresse, Ursprungs- und Ziel-IP-Adresse, Protokoll, Ursprungs- und Ziel-UDP/TCP-Anschluss-Nummer

3.18**Fehlerart und Einflussanalyse/Fehlerart Einfluss- und Kritikalitätsanalyse**

(en: failure mode and effects analysis/failure mode, effects and criticality analysis)

FMEA/FMECA

analytisches Verfahren nach DIN EN 60812

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.

3.19**Internet Control Message Protocol**

(en: internet control message protocol)

ICMP

Protokoll entsprechend ISOC RFC 792

3.20**Internet Group Management Protocol**

(en: internet group management protocol)

IGMP

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

3.21**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.

3.22**Schadsoftware, böartiger Code**

(en: malware, malicious code)

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

3.23**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.

3.24

maximale Übertragungsrate

(en: maximum transmission rate)

maximale Anzahl von Bytes je Sekunde, die durch einen Netzknoten oder ein Netzinfrastrukturgerät übertragen werden kann

3.25

Nachbar-MAC-Adresse

(en: neighbour MAC address)

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

3.26

Netzinfrastrukturkomponenten

(en: network infrastructure components)

Geräte, die zumindest zwei Netzknoten in einem 460er-Netz und zwei unterschiedliche Netze verbinden, wie vermittelnde 460er-Netzknoten, 460er-Netzkoppler, 460er-Protokollumsetzer und drahtlose 460er-Protokollumsetzer

3.27

nominelle Netzkapazität

(en: nominal network capacity)

Netzkapazität als eine Bitrate, die auf der Konfiguration basiert

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

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

3.28

andere Netzfunktion

(en: other network function)

ONF

Funktionsblock mit Schnittstellen 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.

3.29

Rapid Spanning Tree Protocol

(en: rapid spanning tree protocol)]

RSTP

Protokoll nach IEEE 802.1D

3.30

austauschbare externe Datenquelle

(en: removable external data source)

REDS

durch den Anwender austauschbare, nicht-netzseitige Datenquelle, einschließlich Compact Disks, Speichersticks oder Bluetooth¹⁾-Geräte, aber nicht darauf beschränkt

3.31

ringförmige Netzstruktur

(en: ring topology)

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

3.32

RSA-Kryptosystem

(en: RSA)

Kryptosystem mit öffentlichem Schlüssel, wie in IEEE 1363 beschrieben

¹⁾ Bluetooth ist die Handelsmarke eines durch die Bluetooth Special Interest Group gelieferten Produkts.

3.33**Systemsicherheit**

(en: safety)

Schutz für Netze gegen ungewollte Bedrohungen wie z. B. Systemfehlfunktion, Falschkonfiguration und Fehlbedienung

3.34**Sicherheitsbereich**

(en: secure area)

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

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

3.35**Informationssicherheit**

(en: security)

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

3.36**Simple Network Management Protocol**

(en: simple network management protocol)

SNMP

Protokoll nach ISOC RFC 3411

3.37**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.

3.38**Schnüffeln**

(en: sniffing)

Beobachtung und Analyse des Netzverkehrs

3.39**Datenstrom**

(en: stream)

Kombination aller Informationsflüsse eines Gerätes, die dasselbe Protokoll benutzen

3.40**Syslog-Protokoll**

(en: syslog)

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

3.41**Systemintegrator**

(en: system integrator)

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

3.42**Bedrohung**

(en: threat)

mögliche Ursache eines Störfalles in der Informationssicherheit eines Computer, der dem System schaden kann

3.43

Datenverkehr

(en: traffic)

Kombination aller Datenströme von einem Gerät

3.44

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.

3.45

virtuelles lokales Netz

[en: virtual local area network]

VLAN

Netz nach IEEE 802.1Q

3.46

virtuelles Privatnetz

(en: virtual private network)

VPN

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

3.47

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.

3.48

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

English Version

**Maritime navigation and radiocommunication equipment and
systems - Digital interfaces - Part 460: Multiple talkers and
multiple listeners - Ethernet interconnection - Safety and security
(IEC 61162-460:2015)**

Matériels et systèmes de navigation et de
radiocommunication maritimes - Interfaces numériques -
Partie 460: Émetteurs multiples et récepteurs multiples -
Interconnexion Ethernet - Sécurité et sécurité
(IEC 61162-460:2015)

Navigations- und Funkkommunikationsgeräte und -systeme
für die Seeschifffahrt - Digitale Schnittstellen - Teil 460:
Mehrere Datensender und mehrere Datenempfänger –
Ethernet-Verbund - Funktionale und Informationssicherheit
(IEC 61162-460:2015)

This European Standard was approved by CENELEC on 2015-09-22. 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, 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: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 80/764/FDIS, future edition 1 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 61162-460:2015.

The following dates are fixed:

- latest date by which the document has (dop) 2016-06-22
to be implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2018-09-22
standards conflicting with the
document have to be withdrawn

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

Endorsement notice

The text of the International Standard IEC 61162-460:2015 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 in EN 60812.
IEC 61162 series	NOTE	Harmonized in EN 61162 series.
IEC 61162-1	NOTE	Harmonized in EN 61162-1.
IEC 61162-2	NOTE	Harmonized in EN 61162-2.
IEC 62439 series	NOTE	Harmonized in EN 62439 series.
IEC 62439-1	NOTE	Harmonized in EN 62439-1.
IEC 62439-2	NOTE	Harmonized in EN 62439-2.
IEC 62439-3	NOTE	Harmonized in EN 62439-3.
IEC 62439-4	NOTE	Harmonized in EN 62439-4.
IEC 62439-5	NOTE	Harmonized in EN 62439-5.
IEC 62439-6	NOTE	Harmonized in EN 62439-6.
ISO 9241-12	NOTE	Harmonized in EN ISO 9241-12.

CONTENTS

1	Scope.....	7
2	Normative references	7
3	Terms and definitions	8
4	High-level requirements	13
4.1	Overview	13
4.2	Description	13
4.3	General requirements.....	13
4.3.1	Equipment and system requirements	13
4.3.2	Physical composition requirements.....	14
4.3.3	Logical composition requirements.....	14
4.4	Physical component requirements	14
4.4.1	450-Node.....	14
4.4.2	460-Node.....	15
4.4.3	460-Switch.....	15
4.4.4	460-Forwarder	15
4.4.5	460-Gateway and 460-Wireless gateway	15
4.5	Logical component requirements	16
4.5.1	Network monitoring function	16
4.5.2	System management function.....	16
4.6	System documentation requirements	16
4.7	Secure area requirements	16
5	Network traffic management requirements.....	16
5.1	460-Node requirements	16
5.2	460-Switch requirements	17
5.2.1	Resource allocation	17
5.2.2	Loop prevention	17
5.3	460-Forwarder requirements	18
5.3.1	Traffic separation	18
5.3.2	Resource allocation	18
5.3.3	Traffic prioritization	18
5.4	System design requirements	19
5.4.1	Documentation.....	19
5.4.2	Traffic.....	19
6	Security requirements	19
6.1	Security scenarios.....	19
6.1.1	Threat scenarios	19
6.1.2	Internal threats	19
6.1.3	External threats	20
6.2	Internal security requirements	20
6.2.1	General	20
6.2.2	Denial of service protection	20
6.2.3	REDS security	21
6.2.4	Access control	21
6.3	External security requirements	22
6.3.1	Overview	22

6.3.2	Firewalls	23
6.3.3	Communication security	23
6.3.4	460-Node	23
6.3.5	460-Gateway	24
6.3.6	460-Wireless gateway	25
6.4	Additional security issues	25
7	Redundancy requirements	25
7.1	General requirements	25
7.1.1	General	26
7.1.2	Interface redundancy	26
7.1.3	Device redundancy	27
7.2	460-Node requirements	27
7.3	460-Switch requirements	27
7.4	460-Forwarder requirements	27
7.5	460-Gateway and 460-Wireless gateway requirements	27
7.6	Network monitoring function requirements	27
7.7	System design requirements	27
8	Network monitoring requirements	27
8.1	Network status monitoring	27
8.1.1	460-Network	27
8.1.2	460-Node	28
8.1.3	460-Switch	28
8.1.4	460-Forwarder	28
8.1.5	460-Gateway and 460-Wireless gateway	28
8.2	Network monitoring function	29
8.2.1	General	29
8.2.2	Network load monitoring function	30
8.2.3	Redundancy monitoring function	30
8.2.4	Network topology monitoring function	30
8.2.5	Syslog recording function	31
8.2.6	Redundancy of network monitoring function	31
8.2.7	Alert management	31
9	Controlled network requirements	32
10	Methods of testing and required test results	32
10.1	Subject of tests	32
10.2	Test site	32
10.3	General requirements	33
10.4	450-Node	33
10.5	460-Node	33
10.5.1	Network traffic management	33
10.5.2	Security	34
10.5.3	Redundancy	36
10.5.4	Monitoring	36
10.6	460-Switch	36
10.6.1	Resource allocation	36
10.6.2	Loop prevention	37
10.6.3	Security	37

10.6.4	Monitoring.....	38
10.7	460-Forwarder	38
10.7.1	Traffic separation	38
10.7.2	Resource allocation	39
10.7.3	Traffic prioritisation	39
10.7.4	Security	40
10.7.5	Monitoring.....	41
10.8	460-Gateway.....	41
10.8.1	Denial of service behaviour	41
10.8.2	Access control to configuration setup	41
10.8.3	Communication security	41
10.8.4	Firewall.....	42
10.8.5	Application server	42
10.8.6	Interoperable access to file storage of DMZ	43
10.8.7	Additional security.....	43
10.8.8	Monitoring.....	43
10.9	460-Wireless gateway	44
10.9.1	General	44
10.9.2	Security	44
10.9.3	Monitoring.....	44
10.10	Controlled network	44
10.11	Network monitoring function	45
10.11.1	General	45
10.11.2	Network load monitoring function.....	45
10.11.3	Redundancy monitoring function.....	45
10.11.4	Network topology monitoring function	46
10.11.5	Syslog recording function	46
10.11.6	Alert management.....	46
10.12	System level	47
10.12.1	General	47
10.12.2	System management function.....	48
10.12.3	System design	48
10.12.4	Network monitoring function	50
10.12.5	Network load monitoring function.....	50
10.12.6	Redundancy monitoring function.....	50
10.12.7	Network topology monitoring function	50
Annex A (informative)	Communication scenarios between an IEC 61162-460 network and uncontrolled networks	51
A.1	General.....	51
A.2	Routine off-ship.....	51
A.3	Routine on-ship.....	52
A.4	460-Gateway usage for direct connection with equipment	52
Annex B (informative)	Summary of redundancy protocols in the IEC 62439 series	53
B.1	Summary of redundancy protocols.....	53
B.2	RSTP recovery time	53
Annex C (informative)	Guidance for testing	55
C.1	Methods of test	55
C.2	Observation	55

C.3	Inspection of documented evidence	55
C.4	Measurement	55
C.5	Analytical evaluation	56
Annex D (informative)	Some examples to use this standard	57
Annex E (normative)	IEC 61162 interfaces for the network monitoring function	59
Bibliography		60
Annex ZA (normative)	Normative references to international publications with their corresponding European publications.....	62
Figure 1 – Functional overview of IEC 61162-460 requirement applications		13
Figure 2 – 460-Network with 460-Gateway		23
Figure 3 – An example of redundancy		26
Figure 4 – Example of network status recording information		29
Figure A.1 – Usage model for communication between a IEC 61162-450 network and shore networks		51
Figure D.1 – 460-Forwarder used between two networks		57
Figure D.2 – 460-Forwarder used between two networks		57
Figure D.3 – 460-Gateway used for e-Navigation services		58
Figure D.4 – 460-Gateway used for remote maintenance		58
Figure E.1 – Network monitoring function logical interfaces		59
Table 1 – Traffic prioritization with CoS and DSCP		18
Table B.1 – Redundancy protocols and recovery times		53
Table E.1 – Sentences received by the network monitoring function		59
Table E.2 – Sentences transmitted by the network monitoring function		59

IMARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

1 Scope

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

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

2 Normative references

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

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

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

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

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

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

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

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

ISOC RFC 1112, *Host Extensions for IP Multicasting*

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

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

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

ISOC RFC 5424, *The Syslog Protocol*

3 Terms and definitions

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

3.1

450-Node

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

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

3.2

460-Forwarder

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

3.3

460-Gateway

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

3.4

460-Network

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

3.5

460-Node

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

3.6

460-Switch

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

3.7

460-Wireless gateway

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

3.8

advanced encryption standard

AES

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

3.9

alarm

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

3.10

application level gateway

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

3.11

backdoor

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

3.12

controlled network

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

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

3.13

category B alerts

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

3.14

caution

lowest priority of an alert

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

3.15

demilitarized zone

DMZ

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

3.16

denial of service

DoS

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

3.17

flow

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

3.18

failure mode and effects analysis

FMEA

failure mode, effects and criticality analysis

FMECA

analytic method as specified in IEC 60812

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

3.19

internet control message protocol

ICMP

protocol according to ISOC RFC 792

3.20

internet group management protocol

IGMP

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

3.21

loss rate

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

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

3.22

malware

malicious code

software used or created to disrupt computer operation

3.23

maximum network load

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

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

3.24

maximum transmission rate

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

3.25

neighbour MAC address

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

3.26

network infrastructure components

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

3.27

nominal network capacity

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

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

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

3.28

other network function

ONF

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

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

3.29

rapid spanning tree protocol

RSTP

protocol according to IEEE 802.1D

3.30

removable external data source

REDS

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

3.31

ring topology

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

3.32

RSA

public-key cryptosystem as described in IEEE 1363

3.33

safety

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

3.34

secure area

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

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

3.35

security

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

3.36

simple network management protocol

SNMP

protocol according to ISOC RFC 3411

¹ Bluetooth is the trademark of a product supplied by Bluetooth Special Interest Group.

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

3.37

shipborne network

data network infrastructure on board a ship to exchange data between equipment on board

Note 1 to entry: This may or may not be connected to shore by satellites or other means

3.38

sniffing

monitoring and analysis of the network traffic

3.39

stream

combination of all flows from a device which use same protocol

3.40

syslog

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

3.41

system integrator

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

3.42

threat

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

3.43

traffic

combination of all streams from a device

3.44

uncontrolled network

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

EXAMPLE: Wireless networks.

3.45

virtual local area network

VLAN

network according to IEEE 802.1Q

3.46

virtual private network

VPN

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

3.47

warning

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

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

3.48

wireless access point

wireless AP

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

4 High-level requirements

4.1 Overview

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

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

4.2 Description

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

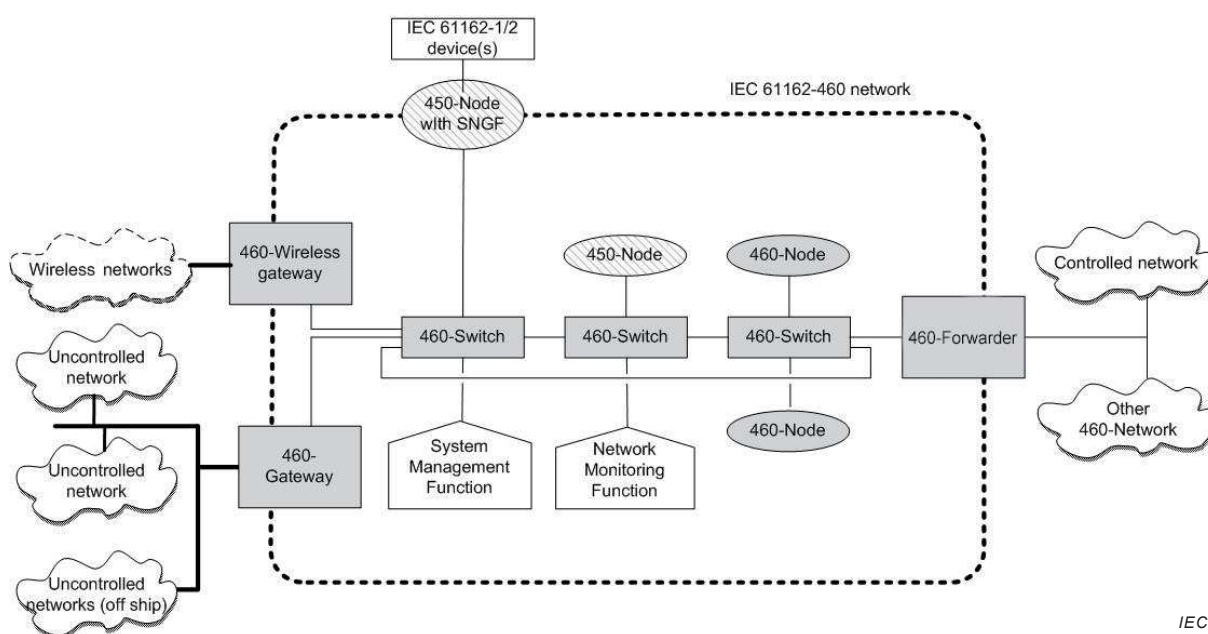


Figure 1 – Functional overview of IEC 61162-460 requirement applications

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

4.3 General requirements

4.3.1 Equipment and system requirements

(See 10.3)

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

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

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

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

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

4.3.2 Physical composition requirements

(See 10.12.3.1)

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

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

4.3.3 Logical composition requirements

(See 10.12.3.1)

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

- network monitoring function, a SF (system function block, see IEC 61162-450) or an ONF (other network function block, see IEC 61162-450) compliant with the requirements in 4.5.1;
- system management function, a SF or an ONF compliant with the requirements in 4.5.2.

4.4 Physical component requirements

4.4.1 450-Node

(See 10.4)

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

- no connection to external networks or REDS;
- syslog implemented as defined IEC 61162-450:2011, 4.3.3.2;
- data output bandwidth documented by the manufacturer as described in 6.2.2.1;