

DIN EN 61162-460

ICS 47.020.70

Einsprüche bis 2017-05-03
Vorgesehen als Ersatz für
DIN EN 61162-460:2016-07**Entwurf**

**Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt –
Digitale Schnittstellen –
Teil 460: Mehrerer Datensender und mehrere Datenempfänger –
Ethernet-Verbund – Funktionale und Informationssicherheit
(IEC 80/813/CD:2016);
Text in Englisch**

Maritime navigation and radiocommunication equipment and systems –
Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security
(IEC 80/813/CD:2016);
Text in English

Matériels et systèmes de navigation et de radiocommunication maritimes –
Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet- Sécurité et sécurité
(IEC 80/813/CD:2016);
Text in Anglaise

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-03-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 73 Seiten

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

Nationales Vorwort

Die englische Originalfassung des internationalen Dokuments IEC 80/813/CD:2016 „Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden.

Das internationale Dokument wurde vom TC 80 „Maritime navigation and radiocommunication equipment and systems“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

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.

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 den vorliegenden Normentwurf erfüllt.

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

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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 berichtigt 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 der Norm.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1)}

1 Anwendungsbereich

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 61162-450:2018, 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 aus IEC 80/813/CD: 2016-07-15 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

AES

(en: advanced encryption standard)

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
DMZ**

(en: demilitarized zone)

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

3.16**Dienstverweigerung
DoS**

(en: denial of Service)

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
FMEA/FMECA**

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

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
ICMP**

(en: internet control message protocol)

Protokoll entsprechend ISOC RFC 792

3.20**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)

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, bössartiger 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

sonstige Netzfunktion

ONF

(en: other network function)

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

RSTP

(en: rapid spanning tree protocol)

Protokoll nach IEEE 802.1D

3.30

austauschbare externe Datenquelle

REDS

(en: removable external data source)

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

3.31

Netzfernüberwachung

RMON

(en: remote network monitoring)

standardisierte Überwachungsspezifikation, wie in ISO/IEC RFC 3577 beschrieben

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

3.32

ringförmige Netzstruktur

(en: ring topology)

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

3.33

RSA-Kryptosystem

(en: RSA)

Kryptosystem mit öffentlichem Schlüssel, wie in IEEE 1363 beschrieben

3.34

Systemsicherheit

(en: safety)

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

3.35

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.

3.36

Informationssicherheit

(en: security)

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

3.37

Simple Network Management Protocol

SNMP

(en: simple network management protocol)

Protokoll nach ISOC RFC 3411

3.38

SNMP-Fänger

(en: SNMP-Trap)

Verfahren zur Sammlung von Ereignissen und statistischer Information von vermittelnden Netzknoten gemäß ISOC RFC 1157, ISOC RFC 2021 und ISOC RFC 2819

3.39

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.

3.40

Schnüffeln

(en: sniffing)

Beobachtung und Analyse des Netzverkehrs

3.41

Datenstrom

(en: stream)

Kombination aller Informationsflüsse eines Gerätes, die dasselbe Protokoll benutzen

3.42

Syslog-Protokoll

(en: syslog)

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

3.43

Systemintegrator

(en: system integrator)

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

3.44

Bedrohung

(en: threat)

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

3.45

Datenverkehr

(en: traffic)

Kombination aller Datenströme von einem Gerät

3.46

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.

3.47

virtuelles lokales Netz

VLAN

[en: virtual local area network]

Netz nach IEEE 802.1Q

3.48

virtuelles Privatnetz

VPN

(en: virtual private network)

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

3.49

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.

3.50

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

CONTENTS

CONTENTS	2
FOREWORD	2
1 Scope	4
2 Normative references	4
3 Terms and definitions	5
4 High-level requirements	10
4.1 Overview	10
4.2 Description	10
4.3 General requirements	11
4.3.1 Equipment and system requirements	11
4.3.2 Physical composition requirements	11
4.3.3 Logical composition requirements	11
4.4 Physical component requirements	11
4.4.1 450-Node	11
4.4.2 460-Node	12
4.4.3 460-Switch	12
4.4.4 460-Forwarder	12
4.4.5 460-Gateway and 460-Wireless gateway	13
4.5 Logical component requirements	13
4.5.1 Network monitoring function	13
4.5.2 System management function	13
4.6 System documentation requirements	13
4.7 Secure area requirements	13
5 Network traffic management requirements	14
5.1 460-Node requirements	14
5.2 460-Switch requirements	14
5.2.1 Resource allocation	14
5.2.2 Loop prevention	14
5.3 460-Forwarder requirements	15
5.3.1 Traffic separation	15
5.3.2 Resource allocation	15
5.3.3 Traffic prioritization	15
5.4 System design requirements	16
5.4.1 Documentation	16
5.4.2 Traffic	16
5.4.3 Connections between secure and non-secure areas	17
6 Security requirements	17
6.1 Security scenarios	17
6.1.1 Threat scenarios	17
6.1.2 Internal threats	17
6.1.3 External threats	17
6.2 Internal security requirements	18
6.2.1 General	18
6.2.2 Denial of service protection	18
6.2.3 REDS security	18
6.2.4 Access control	19

6.3	External security requirements	20
6.3.1	Overview	20
6.3.2	Firewalls	20
6.3.3	Communication security	21
6.3.4	460-Node	21
6.3.5	460-Gateway	21
6.3.6	460-Wireless gateway	22
6.4	Additional security issues	23
7	Redundancy requirements	23
7.1	General requirements	23
7.1.1	General	23
7.1.2	Interface redundancy	23
7.1.3	Device redundancy	24
7.2	460-Node requirements	24
7.3	460-Switch requirements	24
7.4	460-Forwarder requirements	24
7.5	460-Gateway and 460-Wireless gateway requirements	24
7.6	Network monitoring function requirements	24
7.7	System design requirements	24
8	Network monitoring requirements	25
8.1	Network status monitoring	25
8.1.1	460-Network	25
8.1.2	460-Node	25
8.1.3	460-Switch	25
8.1.4	460-Forwarder	26
8.2	Network monitoring function	26
8.2.1	General	26
8.2.2	Network load monitoring function	27
8.2.3	Redundancy monitoring function	27
8.2.4	Network topology monitoring function	28
8.2.5	Syslog recording function	28
8.2.6	Redundancy of network monitoring function	28
8.2.7	Alert management	29
9	Controlled network requirements	30
10	Methods of testing and required test results	30
10.1	Subject of tests	30
10.2	Test site	30
10.3	General requirements	31
10.4	450-Node	31
10.5	460-Node	32
10.5.1	Network traffic management	32
10.5.2	Security	32
10.5.3	Redundancy	34
10.5.4	Monitoring	34
10.6	460-Switch	34
10.6.1	Resource allocation	34
10.6.2	Loop prevention	35
10.6.3	Security	35

10.6.4	Monitoring	36
10.7	460-Forwarder	37
10.7.1	Traffic separation.....	37
10.7.2	Resource allocation	37
10.7.3	Traffic prioritisation.....	38
10.7.4	Security	38
10.7.5	Monitoring	39
10.8	460-Gateway	40
10.8.1	Denial of service behaviour.....	40
10.8.2	Access control to configuration setup.....	40
10.8.3	Communication security.....	40
10.8.4	Firewall.....	40
10.8.5	Application server	41
10.8.6	Interoperable access to file storage of DMZ	41
10.8.7	Additional security	42
10.9	460-Wireless gateway.....	42
10.9.1	General	42
10.9.2	Security	42
10.10	Controlled network.....	42
10.11	Network monitoring function	43
10.11.1	General	43
10.11.2	Network load monitoring function	43
10.11.3	Redundancy monitoring function	43
10.11.4	Network topology monitoring function	44
10.11.5	Syslog recording function	44
10.11.6	Alert management	44
10.12	System level	45
10.12.1	General	45
10.12.2	System management function	46
10.12.3	System design	46
10.12.4	Network monitoring function	48
10.12.5	Network load monitoring function	48
10.12.6	Redundancy monitoring function	48
10.12.7	Network topology monitoring function	48
Annex A (informative)	Communication scenarios between an IEC 61162-460 network and uncontrolled networks	49
A.1	General.....	49
A.2	Routine off-ship	49
A.3	Routine on-ship.....	50
A.4	460-Gateway usage for direct connection with equipment	50
Annex B (informative)	Summary of redundancy protocols in the IEC 62439 series	51
B.1	Summary of redundancy protocols	51
B.2	RSTP recovery time	51
Annex C (informative)	Guidance for testing	53
C.1	Methods of test	53
C.2	Observation	53
C.3	Inspection of documented evidence	53
C.4	Measurement.....	53
C.5	Analytical evaluation	54

Annex D (informative) Some examples to use this standard	55
Annex E (normative) IEC 61162 interfaces for the network monitoring function	59
Bibliography.....	60
Figure 1 – Functional overview of IEC 61162-460 requirement applications	10
Figure 2 – 460-Network with 460-Gateway.....	20
Figure 3 – An example of redundancy	23
Figure 4 – Example of network status recording information	27
Figure A.1 – Usage model for communication between a IEC 61162-450 network and shore networks	49
Figure D.1 – 460-Forwarder used between two networks	55
Figure D.2 – 460-Forwarder used between two networks	55
Figure D.3 – 460-Gateway used for e-Navigation services	56
Figure D.4 – 460-Gateway used for remote maintenance	56
Figure D.5 – 460-Forwarder used to separate an INS system based on its own controlled network from a network of -460 devices	57
Figure D.6 – 460-Forwarder used to separate a Radar system based on its own controlled network from a network of -460 devices	58
Figure E.1 – Network monitoring function logical interfaces	59
Table 1 – Traffic prioritization with CoS and DSCP	16
Table 2 – Summary of alert of Network monitoring	29
Table B.1 – Redundancy protocols and recovery times	51
Table E.1 – Sentences received by the network monitoring function	59
Table E.2 – Sentences transmitted by the network monitoring function	59

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**MARITIME NAVIGATION AND RADIOCOMMUNICATION
EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –****Part 460: Multiple talkers and multiple listeners –
Ethernet interconnection – Safety and security**

FOREWORD

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

International Standard IEC 61162-460 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems.

This second edition of IEC 61162-460 cancels and replaces the first edition published in 2015, of which it constitutes a technical revision.

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

- 460-Switches and 460-Forwarders are required to implement IGMP snooping;
- Dropping of traffic by 460-Forwarder is both amended and clarified;
- Connection between secure and non-secure areas requires a 460-Forwarder as an isolation element;

- Maximum input rate for 460-Nodes is clarified to include all protocol overheads in addition to payloads;
- Clarifications for functionality of the network monitoring;
- 460-Gateway and 460-Wireless gateway are no longer required to report to the network monitoring;
- All alerts from network monitoring have standardized alert identifiers;
- Annex D includes more examples of the use of the standard.

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

This International Standard is to be used in conjunction with IEC 61162-450:2018.

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 publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

Part 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 61162-450:2018. 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 1157, *A Simple Network Management Protocol (SNMP)*

- 118 ISOC RFC 2021, *Remote Network Monitoring Management Information Base*
- 119 ISOC RFC 2236, *Internet Group Management Protocol, Version 2*
- 120 ISOC RFC 2819, *Remote Network Monitoring Management Information Base*
- 121 ISOC RFC 3411, *An Architecture for Describing Simple Network Management Protocol*
122 *(SNMP) Management Frameworks*
- 123 ISOC RFC 3577, *Introduction to the RMON family of MIB modules*
- 124 ISOC RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and*
125 *Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*
- 126 ISOC RFC 5424, *The Syslog Protocol*

127 3 Terms and definitions

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

130 3.1

131 460-Node

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

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

135 3.2

136 460-Forwarder

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

139 3.3

140 460-Gateway

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

143 3.4

144 460-Network

145 network which consists of only 460-Nodes, 460-Switches, 460-Forwarder, 460-Gateway and
146 460-Wireless gateway as well as 450-Nodes

147 3.5

148 460-Node

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

151 3.6

152 460-Switch

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

155 3.7

156 460-Wireless gateway

157 network infrastructure device that connects a 460-Network and wireless networks and which
158 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 larger 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

206 **3.18**
 207 **failure mode and effects analysis**
 208 **FMEA**
 209 **failure mode, effects and criticality analysis**
 210 **FMECA**
 211 analytic method as specified in IEC 60812

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

214 **3.19**
 215 **internet control message protocol**
 216 **ICMP**
 217 protocol according to ISOC RFC 792

218 **3.20**
 219 **internet group management protocol**
 220 **IGMP**
 221 protocol according to ISOC RFC 1112 (version 1), ISOC RFC 2236 (version 2) and
 222 ISOC RFC 4604 (version 3)

223 **3.21**
 224 **loss rate**
 225 amount of lost data by the receiving device of a flow as lost packets per total amount of
 226 packets, measured at the input port of a device

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

228 **3.22**
 229 **malware**
 230 **malicious code**
 231 software used or created to disrupt computer operation

232 **3.23**
 233 **maximum network load**
 234 cumulative maximum amount of all traffic from all network nodes and network infrastructure
 235 components of a single 460-Network

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

237 **3.24**
 238 **maximum transmission rate**
 239 maximum number of bytes per second that can be transmitted by a network node or network
 240 infrastructure equipment

241 **3.25**
 242 **neighbour MAC address**
 243 MAC (media access control) address of connected 450-Node or 460-Node as seen by 460-
 244 Switch and as reported by SNMP (simple network management protocol)

245 **3.26**
 246 **network infrastructure components**
 247 devices that connect at least two nodes in a 460-Network and two different networks such as
 248 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway

249 **3.27**
 250 **nominal network capacity**
 251 network capacity as a bit rate which is based on the configuration

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

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

254 **3.28**

255 **other network function**

256 **ONF**

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

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

260 **3.29**

261 **rapid spanning tree protocol**

262 **RSTP**

263 protocol according to IEEE 802.1D

264 **3.30**

265 **removable external data source**

266 **REDS**

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

269 **3.31**

270 **remote network monitoring**

271 **RMON**

272 standard monitoring specification as described in ISOC RFC 3577

273 **3.32**

274 **ring topology**

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

276 **3.33**

277 **RSA**

278 public-key cryptosystem as described in IEEE 1363

279 **3.34**

280 **safety**

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

283 **3.35**

284 **secure area**

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

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

289 **3.36**

290 **security**

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

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

3.37
simple network management protocol
SNMP
protocol according to ISOC RFC 3411

3.38
SNMP-Trap
method to collect events and statistical information from switches according to ISOC RFC 1157, ISOC RFC 2021 and ISOC RFC 2819

3.39
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

3.40
sniffing
monitoring and analysis of the network traffic

3.41
stream
combination of all flows from a device which use same protocol

3.42
syslog
protocol according to ISOC RFC 5424 which is used for an external logging in IEC 61162-450

3.43
system integrator
person or organisation responsible for the functionality of the integrated 460-network

3.44
threat
potential cause of an incident in computer security that may result in harm to the system

3.45
traffic
combination of all streams from a device

3.46
uncontrolled network
data network that is not an IEC 61162-450 compliant, IEC 61162-460 compliant or a controlled network

EXAMPLE: Wireless networks.

3.47
virtual local area network
VLAN
network according to IEEE 802.1Q

3.48
virtual private network
VPN
extension of a private network through encapsulated, encrypted, and authenticated links across shared or public networks

3.49

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.

3.50

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.

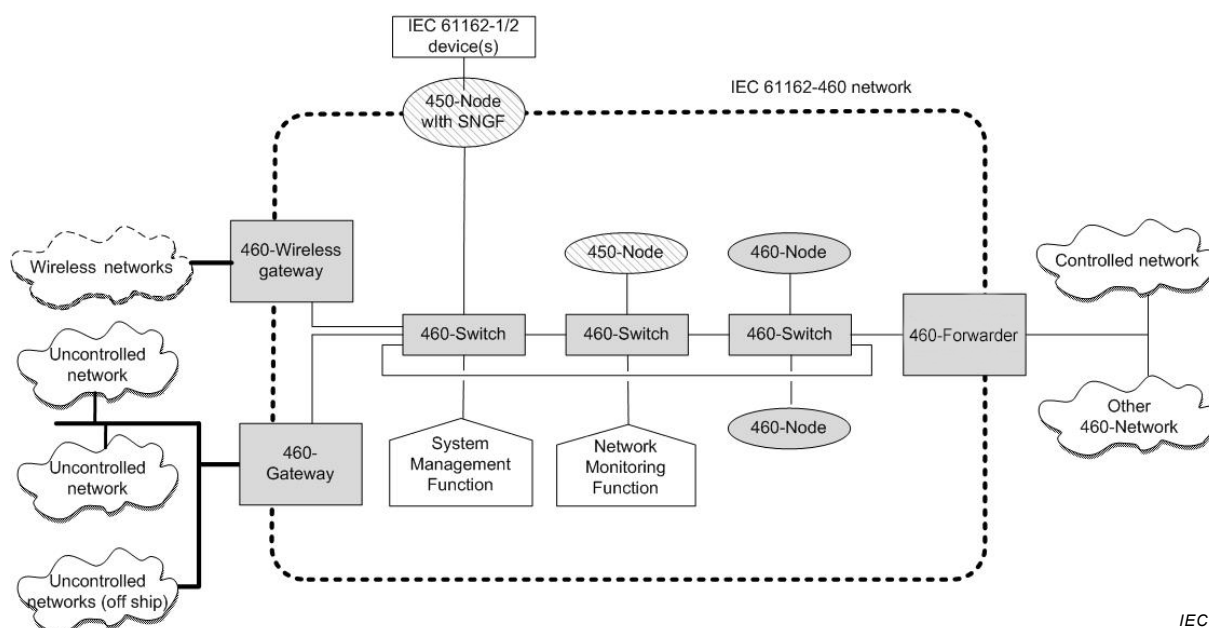


Figure 1 – Functional overview of IEC 61162-460 requirement applications

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.