

DIN EN 61162-460

ICS 47.020.70

Einsprüche bis 2015-03-16

Entwurf

**Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt – Digitale Schnittstellen –
Teil 460: Mehrere Datensender und mehrere Datenempfänger – Ethernet Verbund – Funktionale und Informationssicherheit
(IEC 80/740/CDV:2014);
Englische Fassung FprEN 61162-460:2014**

Maritime navigation and radiocommunication equipment and systems – Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security
(IEC 80/740/CDV:2014);
English version FprEN 61162-460:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-01-16 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de 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/stellungnahme 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 70 Seiten

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

Nationales Vorwort

Die Englische Fassung des europäischen Dokuments FprEN 61162-460:2014 „Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt – Digitale Schnittstellen – Teil 460: Mehrere Datensender und mehrere Datenempfänger – Ethernet Verbund – Funktionale und Informationssicherheit“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (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. Dem entsprechend ist das internationale Dokument IEC 80/740/CDV:2014 „Maritime navigation and radiocommunication equipment and systems – Digital interface – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security“ unverändert in den Entwurf Englische Fassung FprEN 61162-460:2014 übernommen worden.

Das internationale Dokument wurde vom TC 80 „Maritime navigation and radiocommunication equipment and systems“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

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

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

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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 FprEN 61162-460 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und deren 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.

Nationaler Anhang NA ^{N1)} (informativ)

1 Anwendungsbereich

Diese Teilnorm ist eine Ergänzung zur IEC-Norm 61162-450 für integrierte Navigations- und/oder Funkkommunikationssysteme bei denen Normen für höhere funktionale und Informationssicherheit erforderlich sind, z. B. bei verstärkten externen Angriffen oder zur Verbesserung der Netzintegrität. Diese Teilnorm legt Anforderungen und Prüfverfahren für Geräte fest, die in IEC 61162-460 konformen Netzen betrieben werden sollen, sowie Anforderungen an die Netze selbst und Anforderung zur Verbindung des Netzes mit anderen Netzen. Diese Teilnorm enthält auch Anforderungen an ein redundantes IEC 61162-460 konformes Netz.

Diese Teilnorm erweitert die informative Anleitung nach Anhang D der IEC 61162-450. Sie führt keine neuen Anforderungen zu den für die Anwendungsebene nach IEC 61162-450 festgelegten Signalisierungsprotokollen ein.

3 Begriffe

Für das vorliegende Dokument gelten nachfolgend im Einzelnen aufgelistete Synonyme zu den im Abschnitt 3 (*Terms and definitions*) der englischen Sprachfassung dieser Norm aufgelisteten Begriffen.

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.

Alle Definitionen der DIN EN 61162-450 gelten mit, außer wenn neue Definitionen vorhanden sind.

3.1

450er Netzknoten

[en: 450-Node]

Gerät das mit der Norm DIN EN 61162-450 konform ist und der mit dieser 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 Gateway

[en: 460-Gateway]

Gerät der Netzinfrastruktur welches 460er Netze und unkontrollierte Netzen verbindet und die mit dieser Norm vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.4

460er Netz

[en: 460-Network]

Netz das aus 460er Netzknoten, 460er Switches, 460er Netzkoppler, 460er Gateways und drahtlose 460er Gateways sowie 450er Netzknoten besteht

^{N1)} Die Nummerierung aus IEC 80/740/CDV:2014-10 wurde beibehalten.

3.5**460er Netzknoten****[en: 460-Node]**

Gerät welches mit den Anforderungen an einen 450er Netzknoten konform ist und die mit dieser Norm vorgegebenen System- und Informationssicherheitsanforderungen erfüllt

3.6**460er Switch****[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**drahtloses 460er Gateway****[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**erweiterter Verschlüsselungsstandard****[en: Advanced Encryption Standard]****AES**

Blockchiffrialgorithmus mit symmetrischem Schlüssel, der auf einem Substitutions-Permutations-Netzwerk (SPN) basiert und nicht den Verschlüsselungsstandard (DES) nach Feistel anwendet

3.9**Alarmmeldung****[en: alarm]**

Alert höchster Priorität, wie in MSC.252(83) definiert, der eine Situation oder einen Zustand ankündigt, die unmittelbare Aufmerksamkeit, Entscheidung und, falls notwendig, Maßnahmen der Brückenmannschaft erfordert, um die sichere Schiffsführung zu gewährleisten

3.10**Hintertür****[en: backdoor]**

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

3.11**kontrolliertes Netz****[en: controlled network]**

jedes Netz, das in einer Art entwickelt wurde und betrieben wird, dass Behörden gegenüber schriftlich nachgewiesen werden kann, dass sie keine Informationssicherheitsrisiken für angeschlossene Netzknoten darstellen

3.12**Kategorie B Alert****[en: category B alerts]**

Alerts bei denen keine zusätzlichen Informationen als Entscheidungshilfe notwendig sind als die, die am zentralen Alert Management (HMI) angezeigt werden können

3.13**Vorsichtsmeldung****[en: caution]**

niedrigste Priorität eines Alerts. Erregt die Aufmerksamkeit der Brückenmannschaft bezüglich eines Zustandes, der keine Alarmmeldung oder Warnmeldung rechtfertigt aber dennoch Aufmerksamkeit und besondere Beachtung der Situation oder der gegebenen Information erfordert

3.14

entmilitarisierte Zone

[en: Demilitarized Zone]

DMZ

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

3.15

Dienstverweigerung

[en: Denial of Service]

DoS

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

3.16

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

3.17

Fehlermöglichkeits- und Einflussanalyse / Fehlermöglichkeits- 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 Fehlermöglichkeiten gegenüber dem jeweiligen Schweregrad der Folgen darzustellen.

3.18

Internet Kontrollmeldungsprotokoll

[en: Internet Control Message Protocol]

ICMP

Protokoll entsprechend RFC 792

3.19

Internet Gruppenmanagementprotokoll

[en: Internet Group Management Protocol]

IGMP

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

3.20

Verlustrate

[en: loss rate]

Menge der aus einem Informationsfluss am Empfänger verloren gegangenen Daten als Anzahl der verlorenen Pakete gegenüber der am Eingang eines Geräts gemessenen Gesamtanzahl von Paketen, angegeben in Prozent

3.21

Schadsoftware, böartiger Code

[en: malware, malicious code]

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

3.22

Maximale Verlustrate

[en: maximum loss rate]

durch den Hersteller des Gerätes festgelegte Verlustrate für einen Informationsfluss bei dem das Gerät den Normalbetrieb noch fortsetzen kann

3.23**Maximale Netzlast****[en: maximum network load]**

In Bytes pro Sekunde gemessene, kumulierte, maximale Datenverkehrsmenge aller Netzknoten und Netzinfrastrukturkomponenten eines 460er Netzes

3.24**Maximale Übertragungsrate****[en: maximum transmission rate]**

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

3.25**maschenförmige Netzstruktur****[en: mesh topology]**

Netzstruktur bei der jeder Netzknoten mit drei oder mehr Verbindungsleitungen zwischen Switches verbunden ist

3.26**binärer Navigationsbilddatenverkehr****[en: navigational binary image traffic]**

binäre Bilddaten, die nur für Navigationsgeräte bestimmt sind, wie das Radarbild für den VDR

ANMERKUNG 1 zum Begriff: DIN EN 61162-450 legt 2 Arten von Schnittstellen fest: für einfache und für wiederholbare Übertragung.

3.27**Navigationssensorenverkehr****[en: navigational sensor traffic]**

Rundsendungsverkehr, der durch Navigationssensoren erzeugt wird

ANMERKUNG 1 zum Begriff: Die Sensorinformation wird periodisch erzeugt und deren Raten variieren.

ANMERKUNG 2 zum Begriff: Der Sensorverkehr kann klassifiziert sein als MISC, TGTD, SATD usw., wie in DIN EN 61162-450 festgelegt.

3.28**Nachbar-MAC-Adresse****[en: neighbour MAC address]**

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

3.29**Netzinfrastrukturkomponenten****[en: network infrastructure components]**

Geräte, die zumindest zwei Netzknoten in einem 460er Netz und zwei unterschiedliche Netze verbinden, wie 460er Switches, 460er Netzkoppler, 460er Gateways und drahtlose 460er Gateways

3.30**Nominelle Netzkapazität****[en: nominal network capacity]**

Netzkapazität als Bitrate die von der Konfiguration abhängt. Die Kapazität ist die niedrigste Kapazität eines Switches im Netz, um den gesamten Datenverkehr weiter zu leiten

ANMERKUNG 1 zum Begriff: Dies wird zur Festlegung der Leistungsfähigkeit von Geräten benutzt.

3.31

Andere Netzfunktion

[en: Other Network Function]

ONF

Funktionsblock mit Schnittstellen zum Netz, der jedoch nicht die in den Abschnitten 5, 6 und 7 der DIN EN 61162-450 festgelegten Protokolle benutzt

3.32

Rapid Spanning Tree Protocol

[en: Rapid spanning tree protocol]

RSTP

Protokoll nach IEEE 802.1D

3.33

austauschbare externe Datenquelle

[en: removable external data source]

REDS

durch den Anwender austauschbare nicht zum Netz gehörende Datenquelle einschließlich Compact Disks, Speicher Sticks oder Bluetooth Geräte aber nicht darauf beschränkt

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 für Netze gegen ungewollte Bedrohungen wie Systemfehlfunktion, Falschkonfiguration und Fehlbedienung

3.37

Informationssicherheit

[en: security]

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

3.38

Simple Network Management Protocol

[en: Simple network management protocol]

SNMP

Protokoll nach ISOC RFC 3411

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****[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 Computers, 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 DIN EN 61162-450 konformes, kein DIN EN 61162-460 konformes oder kein kontrolliertes Netz, z. B. ein drahtloses Netz ist

3.47**virtuelles lokales Netz****[en: Virtual Local Area Network]****VLAN**

Netz nach IEEE 802.1Q

3.48**virtuelles Privatnetz****[en: Virtual Private Network]****VPN**

Erweiterung eines Privaten Netzes mit gekapselten, verschlüsselten und authentifizierten Verbindungen durch mitbenutzte oder öffentliche Netze hindurch

3.49**Warnmeldung****[en: warning]**

ankündigen einer Situation oder Zustand an, die Aufmerksamkeit aber keine unmittelbare Aufmerksamkeit oder Aktivität der Brückenbesetzung erfordert. Warnmeldungen werden vorsorglich angezeigt, um die Brückenbesetzung auf veränderte Zustände 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 Wi-Fi, Bluetooth, verbindet

CONTENTS

1		
2		
3	INTRODUCTION.....	8
4	1 Scope.....	9
5	2 Normative references	9
6	3 Terms and definitions	9
7	4 High-level requirements.....	14
8	4.1 Overview	14
9	4.2 Description	14
10	4.3 General requirements.....	15
11	4.3.1 Equipment and system requirements	15
12	4.3.2 Physical composition requirements.....	15
13	4.3.3 Logical composition requirements.....	16
14	4.4 Physical component requirements	16
15	4.4.1 450-Node	16
16	4.4.2 460-Node	16
17	4.4.3 460-Switch	17
18	4.4.4 460-Forwarder.....	17
19	4.4.5 460-Gateway and 460-Wireless gateway	17
20	4.5 Logical component requirements	17
21	4.5.1 Network monitoring function	17
22	4.5.2 System management function.....	17
23	4.6 System design requirements	18
24	5 Network traffic management requirements.....	18
25	5.1 460-Node requirements	18
26	5.2 460-Switch requirements	18
27	5.2.1 Resource allocation	18
28	5.2.2 Loop prevention.....	19
29	5.3 460-Forwarder requirements	19
30	5.3.1 Traffic separation	19
31	5.3.2 Resource allocation	20
32	5.3.3 Traffic prioritisation.....	20
33	5.4 System design requirements	21
34	5.4.1 Documentation	21
35	5.4.2 Traffic.....	21
36	6 Security requirements.....	21
37	6.1 Security scenarios	21
38	6.1.1 Threat scenarios.....	21
39	6.1.2 Internal threats	21
40	6.1.3 External threats	22
41	6.2 Internal security requirements	22
42	6.2.1 General	22
43	6.2.2 Denial of service protection	22
44	6.2.3 REDS security	23
45	6.2.4 Access control.....	23
46	6.3 Uncontrolled network security requirements	24
47	6.3.1 Overview	24
48	6.3.2 Firewall	24

49	6.3.3	Communication security for uncontrolled networks	25
50	6.3.4	460-Node	25
51	6.3.5	460-Gateway	25
52	6.3.6	460-Wireless gateway	27
53	6.4	Additional security issues	27
54	7	Redundancy requirements	27
55	7.1	General requirements	27
56	7.1.1	General	27
57	7.1.2	Interface redundancy	28
58	7.1.3	Device redundancy	28
59	7.2	460-Node requirements	28
60	7.3	460-Switch requirements	29
61	7.4	460-Forwarder requirements	29
62	7.5	460-Gateway and 460-Wireless gateway requirements	29
63	7.6	Network monitoring function requirements	29
64	7.7	System design requirements	29
65	8	Network monitoring requirements	29
66	8.1	Network status monitoring requirements	29
67	8.1.1	460-Network	29
68	8.1.2	460-Node	29
69	8.1.3	460-Switch	30
70	8.1.4	460-Forwarder	30
71	8.1.5	460-Gateway and 460-Wireless gateway	31
72	8.2	Network monitoring function requirements	31
73	8.2.1	General	31
74	8.2.2	Network load monitoring function	32
75	8.2.3	Redundancy monitoring function	32
76	8.2.4	Network topology monitoring function	33
77	8.2.5	Syslog recording function	33
78	8.2.6	Redundancy of network monitoring function	33
79	8.2.7	Alert management	34
80	9	Controlled network requirements	34
81	10	Methods of testing and required test results	35
82	10.1	Subject of tests	35
83	10.2	Test site	35
84	10.3	General requirements	35
85	10.4	450-Node	36
86	10.5	460-Node	36
87	10.5.1	Network traffic management	36
88	10.5.2	Security	37
89	10.5.3	Redundancy	38
90	10.5.4	Monitoring	38
91	10.6	460-Switch	39
92	10.6.1	Resource Allocation	39
93	10.6.2	Loop prevention	39
94	10.6.3	Security	40
95	10.6.4	Monitoring	41
96	10.7	460-Forwarder	41
97	10.7.1	Traffic separation	

98	10.7.2 Resource allocation	41
99	10.7.3 Traffic prioritisation	42
100	10.7.4 Security	42
101	10.7.5 Monitoring	43
102	10.8 460-Gateway	44
103	10.8.1 Denial of service behaviour	44
104	10.8.2 Access control to configuration setup	44
105	10.8.3 Communication security.....	45
106	10.8.4 Firewall	45
107	10.8.5 Application server	45
108	10.8.6 Interoperable access to file storage of DMZ	46
109	10.8.7 Additional security	46
110	10.8.8 Monitoring	46
111	10.9 460-Wireless gateway	47
112	10.9.1 General	47
113	10.9.2 Security	47
114	10.9.3 Monitoring	47
115	10.10 Controlled network	48
116	10.11 Network monitoring function	48
117	10.11.1 General	48
118	10.11.2 Network load monitoring function	48
119	10.11.3 Redundancy monitoring function	49
120	10.11.4 Network topology monitoring function	49
121	10.11.5 Syslog recording function	49
122	10.11.6 Alert management	49
123	10.12 System level	50
124	10.12.1 General	50
125	10.12.2 System management function	51
126	10.12.3 System design	51
127	10.12.4 Network monitoring function	53
128	10.12.5 Network load monitoring function	53
129	10.12.6 Redundancy monitoring function	53
130	10.12.7 Network topology monitoring function	53
131	Annex A (informative) Communication scenarios between a IEC 61162-460 network	
132	and uncontrolled networks	54
133	A.1 Routine off-ship	54
134	A.2 Routine on-ship	55
135	A.3 460-Gateway usage for direct connection with equipment	55
136	Annex B (informative) Summary of redundancy protocols in the IEC 62439 series	56
137	B.1 Summary of redundancy protocols	56
138	B.2 RSTP recovery time	56
139	Annex C (informative) Guidance for testing	58
140	C.2 Observation	58
141	C.3 Inspection of documented evidence	58
142	C.4 Measurement	58
143	C.5 Analytical evaluation	59
144	Annex D (informative) Some examples for usage of this standard	60
145	Annex E (normative) IEC 61162 interfaces for the network monitoring function	62
146	Bibliography	

147		
148	Figure 1 – Functional overview of IEC 61162-460 requirement application	15
149	Figure 2 – 460-Network with 460-Gateway.....	24
150	Figure 3 – An example of redundancy	28
151	Figure 4 – Example of network status recording information (trend curve).....	32
152	Figure A.1 - Usage model for communication between a IEC 61162-450 network and	
153	shore networks	54
154	Figure D.1 – 460-Forwarder used between two networks	60
155	Figure D.2 – 460-Forwarder used between two networks	60
156	Figure D.3 – 460-Gateway used for e-Navigation services	61
157	Figure D.4 – 460-Gateway used for remote maintenance	61
158	Figure E.1 – Network monitoring function logical interfaces.	62
159		
160	Table 1 – Traffic prioritization with CoS and DSCP	20
161	Table B.1 - Redundancy protocols and recovery times	56
162	Table E.1 – IEC 61162-1 sentences received by the network monitoring function	62
163	Table E.2 – IEC 61162-1 sentences transmitted by the network monitoring function	62
164		

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.

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

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

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

218 The committee has decided that the contents of this publication will remain unchanged until
219 the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data
220 related to the specific publication. At this date, the publication will be

- 221 • reconfirmed,
222 • withdrawn,
223 • replaced by a revised edition, or
224 • amended.

225

226 The National Committees are requested to note that for this publication the stability date
227 is 2018

228 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE
229 DELETED AT THE PUBLICATION STAGE.

230

INTRODUCTION

The IEC 61162-450 standard specifies a method by which navigational and radiocommunication equipment can be safely interconnected in a single Ethernet network. This is a "light weight" standard that is intended for use on ships with relatively simple integrated bridge systems and where open integration of several different manufacturers' equipment is a prerequisite.

However, many ships require more complex bridge systems due to complex operational scenarios, heavier use of remote diagnostics and maintenance, tighter integrations with other systems onboard of the ship or offship or for any other reason, e.g.. to support new e- Navigation services.

The IEC 61162-460 standard has been developed as an extension to IEC 61162-450 to allow safe and secure implementation of more complex bridge systems. There are two main reasons to develop this standard:

A.1.1.1 to provide requirements and test specifications for manufacturers that want to provide more functionality in their equipment and systems than IEC 61162-450 caters for or even allows;

A.1.1.2 as a specification and requirement tool for ship owners or yards that want to design more complex bridge systems than IEC 61162-450 allows.

As a consequence of these objectives, the IEC 61162-460 standard allows the use of more complex network infrastructure equipment. This includes support for routing between networks, for interfacing to external systems and for building redundancy and new safety functions into the system. On the other hand, this also requires more stringent design, configuration and operational requirements for equipment and systems which the IEC 61162-450 standard avoids by restricting the use of such equipment.

Thus, the IEC 61162-460 standard should not be construed as a necessary addition to IEC 61162-450, as the latter will provide sufficient and cost-effective specifications for many or even most ships. IEC 61162-460 should be seen as a "high end" addition to IEC 61162-450 for systems that require more complex design and operation requirements. Even though this standard is mainly intended for navigational networks, it may be applied to other Ethernet variant networks.

The main objectives of this standard are to:

- define equipment and system requirements to improve network availability even when some network components or equipment fail to work as specified. These requirements will address safe behaviour of failing devices as well as recovery mechanisms in the network, including redundancy;
- define new requirements and monitoring functions to allow safe design and operation of networks with high network loads in terms of overall bandwidth or message frequency;
- allow safe and secure interconnection to external data sources, including other ship networks, off-ship data sources and removable external data sources by providing more extensive requirements to the components and operation of the system;
- define system monitoring functions to aid in early detection and diagnosis of developing problems related to errors or overload of the system.

This standard allows the limited use of IEC 61162-450 compliant network nodes ("450-Nodes") in IEC 61162-460 networks.

This standard also allows that an IEC 61162-450 compliant network can be interfaced to an IEC 61162-460 network through a 460-Gateway.

MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS – DIGITAL INTERFACES –

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

1 Scope

This standard is an add-on to the IEC 61162-450 standard for integrated navigation and/or radio communication systems 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 to 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. It does not introduce new application level protocol requirement to those that are defined in IEC 61162-450.

2 Normative references

The following referenced documents are indispensable for the application 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 61162-450:2011, *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 – Part 2: Modular structure for INS – Operational and performance 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*.

3 Terms and definitions

For the purposes of this International Standard, the following definitions apply. Unless new definitions are provided, all definitions from IEC 61162-450 also apply.

3.1

450-Node

a 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

- 323 **3.3**
324 **460-Gateway**
325 network infrastructure device that connects 460-networks and uncontrolled networks and
326 which satisfies the safety and security requirements as specified in this standard
- 327 **3.4**
328 **460-Network**
329 network which consists of only 460-Nodes, 460-Switches, 460-Forwarder, 460-Gateway and
330 460-Wireless gateway as well as 450-Nodes
- 331 **3.5**
332 **460-Node**
333 device compliant with the requirement of a 450-Node and which satisfies the safety and
334 security requirements as specified in this standard
- 335 **3.6**
336 **460-Switch**
337 network infrastructure device used to interconnect nodes on a 460-Network and which
338 satisfies the safety and security requirements as specified in this standard
- 339 **3.7**
340 **460-Wireless gateway**
341 network infrastructure device that connects a 460-network and wireless networks and which
342 satisfies the safety and security requirements as specified in this standard
- 343 **3.8**
344 **Advanced Encryption Standard**
345 **AES**
346 a symmetric-key block cipher algorithm which is based on a substitution-permutation network
347 (SPN) and does not use the Data Encryption Standard (DES) Feistel network
- 348 **3.9**
349 **alarm**
350 the highest priority of an alert, announcing a situation or condition requiring immediate
351 attention, decision and if necessary action by the bridge team, to maintain the safe navigation
352 of the ship
- 353 **3.10**
354 **backdoor**
355 installed program allowing remote access to a computer by providing a method of bypassing
356 normal authentication
- 357 **3.11**
358 **controlled network**
359 any network that has been designed to operate such that authorities are satisfied by
360 documented evidence that it does not pose any security risks to any connected network nodes
- 361 **3.12**
362 **category B alerts**
363 alerts where no additional information for decision support is necessary besides the
364 information which can be presented at the central alert management HMI
- 365 **3.13**
366 **caution**
367 lowest priority of an alert. Raising bridge team's awareness of a condition which does not
368 warrant an alarm or warning condition, but still requires attention out of the ordinary
369 consideration of the situation or of given information

- 370 **3.14**
371 **Demilitarized Zone**
372 **DMZ**
373 physical or logical sub-network that contains and exposes an organization's external-facing
374 services to a larger and un-trusted network, usually Internet
- 375 **3.15**
376 **Denial of Service**
377 **DoS**
378 attempt to prevent legitimate users from accessing a machine or network resource
- 379 **3.16**
380 **flow**
381 combination of the following information: source and destination MAC address, source and
382 destination IP address, protocol, source and destination UDP/TCP port number
- 383 **3.17**
384 **Failure Mode and Effects Analysis/Failure Mode, Effects and Criticality Analysis**
385 **FMEA/FMECA**
386 an analytic method as specified in IEC 60812
- 387 Note 1 to entry: FMECA extends FMEA by including a criticality analysis, which is used to chart the probability of
388 failure modes against the severity of their consequences.
- 389 **3.18**
390 **Internet Control Message Protocol**
391 **ICMP**
392 protocol according to RFC 792
- 393 **3.19**
394 **Internet Group Management Protocol**
395 **IGMP**
396 protocol according to RFC 1112 (version 1), RFC 2236 (version 2) and RFC 4604(version 3)
- 397 **3.20**
398 **loss rate**
399 amount of lost data by the receiving device of a flow as lost packets per total amount of
400 packets, measured at the input port of a device and expressed in %
- 401 **3.21**
402 **malware, malicious code**
403 software used or created to disrupt computer operation
- 404 **3.22**
405 **maximum loss rate**
406 loss rate for a flow under which the device is still able to continue normal operation, defined
407 by the manufacturer of the device
- 408 **3.23**
409 **maximum network load**
410 cumulative maximum amount of all traffic from all network nodes and network infrastructure
411 components of a single 460-Network measured in bytes per second
- 412 **3.24**
413 **maximum transmission rate**
414 maximum number of bytes per second that can be transmitted by a network node or network
415 infrastructure equipment

- 416 **3.25**
417 **mesh topology**
418 topology where each node is connected with three or more inter-switch links
- 419 **3.26**
420 **navigational binary image traffic**
421 binary image data that is targeted only to the navigational equipment such as the radar image
422 for VDR
- 423 Note 1 to entry: In IEC 61162-450 two types of interfaces are defined: simple and re-transmittable.
- 424 **3.27**
425 **navigational sensor traffic**
426 broadcast traffic that is generated by navigational sensor equipment
- 427 Note 1 to entry: The sensor information is periodically generated and its rates are vary.
- 428 Note 2 to entry: The sensor traffic can be classified as MISC, TGTD, SATD etc, as defined in IEC 61162-450.
- 429 **3.28**
430 **neighbour MAC address**
431 MAC address of connected 450-Node or 460-Node as seen by 460-Switch and as reported by
432 SNMP
- 433 **3.29**
434 **network infrastructure components**
435 devices that connect at least two nodes in a 460-Network and two different networks such as
436 460-Switch, 460-Forwarder, 460-Gateway and 460-Wireless gateway
- 437 **3.30**
438 **nominal network capacity**
439 network capacity as a bit rate which is based on the configuration. The capacity is the lowest
440 capacity of any switch in the network to route all traffic.
- 441 Note 1 to entry: This is used for specifying capabilities of equipment.
- 442 **3.31**
443 **Other Network Function**
444 **ONF**
445 function block that interfaces to the network as specified in IEC 61162-450
- 446 Note 1 to entry: The ONF represents a function that is allowed to share the infrastructure of an IEC 61162-450
447 network but does not use the protocols defined in IEC 61162-450.
- 448 **3.32**
449 **Rapid spanning tree protocol**
450 **RSTP**
451 protocol according to IEEE 802.1D
- 452 **3.33**
453 **removable external data source**
454 **REDS**
455 user removable non-network data source, including, but not limited to compact discs, memory
456 sticks and Bluetooth devices
- 457 **3.34**
458 **ring topology**
459 topology where each node is connected in series to two other nodes

- 460 **3.35**
461 **RSA**
462 public-key cryptosystem as described in IEEE 1363
463
- 464 **3.36**
465 **safety**
466 protection of networks from un-intentional threats such as system mal-functioning, mis-
467 configuration and mis-operation
- 468 **3.37**
469 **security**
470 protection of networks from intentional threats such as virus, worm, denial-of-service attacks,
471 illicit access, etc.
- 472 **3.38**
473 **simple network management protocol**
474 **SNMP**
475 protocol according to ISOC RFC 3411
- 476 **3.39**
477 **shipborne network**
478 data network infrastructure on board a ship to exchange data between equipment on board
- 479 Note 1 to entry: This may or may not be connected to shore by satellites or other means
- 480 **3.40**
481 **sniffing**
482 monitoring and analysis of the network traffic
- 483 **3.41**
484 **stream**
485 combination of all flows from a device which use same protocol
- 486 **3.42**
487 **syslog**
488 protocol according to ISOC RFC 5424 which is used for an external logging in IEC 61162-450
- 489 **3.43**
490 **system integrator**
491 person or organisation responsible for the functionality of the integrated 460-network.
- 492 **3.44**
493 **threat**
494 potential cause of an incident in computer security that may result in harm to the system
- 495 **3.45**
496 **traffic**
497 combination of all streams from a device
- 498 **3.46**
499 **uncontrolled network**
500 any data network that is not an IEC 61162-450 compliant, IEC 61162-460 compliant or a
501 controlled network: for example wireless networks

502 **3.47**
503 **Virtual Local Area Network**
504 **VLAN**
505 network according to IEEE 802.1Q

506 **3.48**
507 **Virtual Private Network**
508 **VPN**
509 extension of a private network through encapsulated, encrypted, and authenticated links
510 across shared or public networks

511 **3.49**
512 **warning**
513 announcing a situation or condition requiring attention but no immediate attention or action by
514 the bridge team
515
516 Note 1 to entry: Warnings are presented for precautionary reasons to make the bridge team aware of changed
517 conditions which are not immediately hazardous, but may become so, if no forward-looking decision is made or
518 action is taken.

519 **3.50**
520 **Wireless Access Point**
521 **Wireless AP**
522 device that connects wireless devices to wired devices through various wireless technologies
523 such as Wi-Fi, Bluetooth

524 **4 High-level requirements**

525 **4.1 Overview**

526 This standard is based on IEC 61162-450 which is a necessary prerequisite for this standard.

527 NOTE This standard relaxes some requirements of IEC 61162-450, in particular with respect to the allowed
528 functionality of switches and to interconnections to other networks. As a consequence of this, this standard
529 specifies more stringent requirements for equipment, system design and operation.

530 All equipment conforming to the IEC 61162-460 standard will also be deemed to satisfy
531 requirements to IEC 61162-450 except the requirements specified in this standard.

532 Clause 4 including sub-clauses does not apply to controlled networks as specified in Clause 9.

533 **4.2 Description**

534 Figure 1 shows a network implementing the requirements of this standard on different parts
535 and components of the network. The grey symbols represent equipment specified in this
536 standard. The pentagons represent logical software functions specified in this standard. The
537 requirements are to some degree independent and for many types of equipment only parts of
538 this standard need to be applied.