

DIN EN 63154

ICS 35.030; 47.020.70

Einsprüche bis 2018-11-14

Entwurf

Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt – Cyber-Security – Allgemeine Anforderungen, Prüfverfahren und geforderte Prüfergebnisse (IEC 80/883/CD:2018); Text Englisch

Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results (IEC 80/883/CD:2018); Text in English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-09-14 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 29 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die englische Originalfassung des internationalen Dokument IEC 80/883/CD:2018 „Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results“ (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 FprEN nur 6 Wochen 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/vorliegende Norm erfüllt

Da sich die Benutzer des vorliegenden Normentwurfs/der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 63154 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als Nationaler Anhang NA des vorliegenden Normentwurfs/der vorliegenden Norm hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf/Diese Norm 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. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung ^{N1)}

1 Anwendungsbereich

In diesem Dokument werden die Anforderungen, Prüfverfahren und erforderlichen Prüfergebnisse für auf Schiffen mitgeführte Ausrüstungen festgelegt, für die Normen über den Schutz gegen Cyberstörfälle erforderlich sind.

- a) Auf Schiffen mitgeführte Funkausrüstungen, die Bestandteil des Global Maritime Distress and Safety System (weltweites Seenot- und Sicherheitsfunksystem, GMDSS) nach der International Convention for Safety of Life at Sea (Internationales Übereinkommen zum Schutz des menschlichen Lebens auf See, SOLAS) in der ergänzten Fassung und der Torremolinos International Convention for the Safety of Fishing Vessels (Internationales Übereinkommen von Torremolinos über die Sicherheit von Fischereifahrzeugen) in der ergänzten Fassung sowie andere auf Schiffen mitgeführte Funkausrüstungen, sofern zutreffend;
- b) Auf Schiffen mitgeführte Navigationsausrüstungen nach der International Convention for Safety of Life at Sea (Internationales Übereinkommen zum Schutz des menschlichen Lebens auf See, SOLAS) in der ergänzten Fassung und der Torremolinos International Convention for the Safety of Fishing Vessels (Internationales Übereinkommen von Torremolinos über die Sicherheit von Fischereifahrzeugen) in der ergänzten Fassung sowie andere auf Schiffen mitgeführte Navigationshilfen, sofern zutreffend.

Navigations- und Funkkommunikationsausrüstungen werden nach der Festlegung durch den Internationalen Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen (ISPS, en: „International Ship and Port Facility Security Code“) der Internationalen Seeschiffahrts-Organisation (IMO, en: „International Maritime Organization“) im Allgemeinen in gesperrten Bereichen installiert. Dies begründet sich auf der Bedeutung von Navigations- und Funkkommunikationsausrüstungen für die Sicherheit der Navigation. Die gesperrten Bereiche werden im Folgenden als Sicherheitsbereiche mit implementierten Sicherheitsmaßnahmen angesehen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

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

3.1

Konfiguration

Teil der Einrichtungs-, Installations- oder Konfigurationsparameter/-auswahloptionen/-einstellungen, die der Hersteller in seiner Dokumentation als nur im Instandhaltungsmodus verfügbar angegeben hat

3.2

Instandhaltungsmodus

Modus, der qualifizierten und autorisierten Personen vorbehalten ist

Anmerkung 1 zum Begriff: Der Instandhaltungsmodus ist für Vorgänge wie [Flashen von Images][Zurücksetzen auf Werkseinstellungen][Hardwarereparatur] und Konfiguration erforderlich.

^{N1)} Nationale Fußnote: Die Nummerierung des IEC-Schriftstücks 80/883/CD:2018-03 wurde beibehalten.

Anmerkung 2 zum Begriff: Arbeitsverfahren und vorbereitende Tätigkeiten für den Instandhaltungsmodus sind nicht Teil dieser Norm, werden aber üblicherweise im Qualitätssicherungssystem eines Unternehmens abgebildet, das die Erstinstallation oder spätere Instandhaltungsarbeiten übernimmt.

3.3

Normalbetrieb

Nutzung der Funktionalität, die nach der Dokumentation des Herstellers einem Nutzer zur Verfügung steht

Anmerkung 1 zum Begriff: [Absicht. Jeder Abschnitt dieser Norm soll mit „Im Normalbetrieb...“ oder mit „Im Instandhaltungsmodus...“ beginnen.]

3.4

externer Wechseldatenträger

REDS

(en: „removable external data source“)

vom Benutzer wechselbare nicht netzwerkgestützte Datenquelle, einschließlich aber nicht beschränkt auf CDs, Speichersticks und Bluetooth®-Geräte

Anmerkung 1 zum Begriff: Bluetooth ist die Marke eines Produkts der Bluetooth Special Interest Group. Diese Informationen werden als Service für die Nutzer des vorliegenden Dokuments bereitgestellt und stellen keine Empfehlung des genannten Produkts seitens der IEC dar.

3.5

externe Datenquelle

EDS

(en: „external data source“)

Netzwerkgestützte oder nicht netzwerkgestützte Datenquelle, einschließlich, aber nicht beschränkt auf REDS, SIM-Karten, Wechselplatten usw.

3.6

Cyberstörfall

Ereignis, aus dem sich tatsächlich oder potentiell negative Konsequenzen für ein an Bord eines Schiffs mitgeführtes System, das Netzwerk und die Ausrüstung oder die damit verarbeiteten, gespeicherten oder übertragenen Daten ergeben

3.7

Nutzer

jede Person, welche die Ausrüstung bestimmungsgemäß nutzt

CONTENTS

CONTENTS	2
FOREWORD	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Module A: Data files	8
4.1 Requirements	8
4.2 Methods of testing and required test results	9
5 Module B: Auto-run of executables	10
5.1 Requirements for executable program file verification	10
5.2 Methods of testing and required test results	10
6 Module C: User authentication	10
6.1 Requirements	10
6.2 Methods of testing and required test results	11
7 Module D: System defence	11
7.1 General	11
7.2 Requirements	11
7.3 Methods of testing and required test results	12
8 Module E: Network access	12
8.1 General	12
8.2 Requirements	12
8.3 Methods of testing and required test results	12
9 Module F: Access to operating system	13
9.1 General	13
9.2 Requirements	13
9.3 Methods of testing and required test results	13
10 Module G: Booting environment	13
10.1 General	13
10.2 Requirements	13
10.3 Methods of testing and required test results	13
11 Module H: Configuration management	14
11.1 Requirements	14
11.2 Methods of testing and required test results	14
12 Module I: Protection against unintentional crash caused by user input	14
12.1 Requirements	14
12.2 Methods of testing and required test results	14
13 Module J: USB interfaces for other than storage purposes	14
13.1 General	14
13.2 Requirements for training option	14
13.3 Methods of testing and required test results for training option	15
13.4 Requirements for technical method option	15
13.5 Methods of testing and required test results for technical method option	15
14 Module K: USB ports and interfaces for REDS	15
14.1 Requirements	15

14.1.1	Physical protection	15
14.1.2	Operational protection	15
14.2	Methods of testing and required test results	16
15	Module L: IEC 61162-1 or IEC 61162-2 as interface	16
16	Module M: IEC 61162-450 as interface	16
16.1	General.....	16
16.2	Requirements related to IEC 61162-1 sentences.....	16
16.3	Requirements related to IEC 61162-450 used for file transfer	17
16.4	Requirements related to Denial of Service (DoS)	17
16.4.1	General	17
16.4.2	Requirement.....	17
16.5	Methods of testing and required test results	17
17	Module N: Other interfaces	18
17.1	General.....	18
17.2	Requirements	18
17.3	Methods of testing and required test results	18
18	Module O: Software maintenance	18
18.1	General.....	18
18.2	Requirements for software maintenance by the authorized persons using maintenance mode.....	18
18.3	Methods of testing and required test results for software maintenance by the authorized person using maintenance mode	18
18.4	Requirements for semi-automatic software maintenance by the crew onboard the vessel.....	18
18.4.1	General	18
18.4.2	Requirement for software update requiring manual transfer into the equipment	19
18.4.3	Requirement for software update readily available for the equipment.....	19
18.5	Methods of testing and required test results for semi-automatic software maintenance by the crew onboard the vessel	19
19	Module P: Remote maintenance	19
20	Documentation	19
20.1	Requirements	19
20.2	Methods of testing and required test results	19
Annex A (informative)	IMO SOLAS regime and practical limitations for equipment	20
Annex B (informative)	Methods of authentication of data files and executables – some examples	21
B.1	General.....	21
B.2	Authentication based on Certificates	21
B.3	Authentication based on Private key and pre-shared Public key	21
B.4	Authentication based on pre-shared key	22
B.5	Authentication based on pre-shared key – Diffie-Hellmann.....	22
Annex C (informative)	Malware protection in type approved systems based on anti- virus software which uses signatures for malware detection	23
C.1	General.....	23
C.2	Issues	23
Annex D (normative)	USB class codes	24
D.1	General.....	24
Annex E (Informative)	Cyber security configuration document for equipment	24

E.1	General for the document	25
E.2	Document parts	25
E.2.1	Hardening of the operating system	25
E.2.2	Upgrade strategy for cyber security reasons	25
E.2.3	Strategies for detecting and reacting to future vulnerabilities	25
Bibliography.....		26

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**MARITIME NAVIGATION
AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS –
CYBERSECURITY –
GENERAL REQUIREMENTS, METHODS OF TESTING
AND REQUIRED TEST RESULTS**

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 63514 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems.

The text of this International 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 International Standard can be found in the report on voting indicated in the above table.

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

52 The committee has decided that the contents of this document will remain unchanged until the
53 stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to
54 the specific document. At this date, the document will be

- 55 • reconfirmed,
56 • withdrawn,
57 • replaced by a revised edition, or
58 • amended.

59

60 The National Committees are requested to note that for this document the stability date
61 is

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

64